

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 □□□□ □□□□□.

Home > Just-in-time VM access >

JIT VM access configuration

VM1

+ Add Save Discard

Configure the ports for which the just-in-time VM access will be applicable

Port	Protocol	Allowed source IPs	IP range	Time range (hours)
3389	Any	CIDR	10.10.0.0/24,192.168.10.0/24	3 hours
8080	Any	Per request	N/A	5 hours

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

Answer Area

Statements	Yes	No
You can establish a Remote Desktop connection from VM1 to VM3 for a maximum of three hours.	<input type="radio"/>	<input type="radio"/>
You can establish a Remote Desktop connection from VM2 to VM1 after requesting access.	<input type="radio"/>	<input type="radio"/>
You can establish a Remote Desktop connection from VM3 to VM1 without requesting access.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
You can establish a Remote Desktop connection from VM1 to VM3 for a maximum of three hours.	<input type="radio"/>	<input checked="" type="radio"/>
You can establish a Remote Desktop connection from VM2 to VM1 after requesting access.	<input checked="" type="radio"/>	<input type="radio"/>
You can establish a Remote Desktop connection from VM3 to VM1 without requesting access.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Answer Area

Statements	Yes	No
You can establish a Remote Desktop connection from VM1 to VM3 for a maximum of three hours.	<input type="radio"/>	<input checked="" type="radio"/>
You can establish a Remote Desktop connection from VM2 to VM1 after requesting access.	<input checked="" type="radio"/>	<input type="radio"/>
You can establish a Remote Desktop connection from VM3 to VM1 without requesting access.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION: 2

contoso.com Azure Active Directory(Azure AD) contains three Azure AD users.
 User1, User2, and User3 are members of the RG1 group.

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

RG1 contains three resources.

RG1 contains three resources. RG1 contains three resources, RG1 contains three resources, RG1 contains three resources? RG1 contains three resources.

□□: □□ 1□□ 1□□□□.

Users who can modify the permissions for RG1:

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

Users who can create virtual networks in RG1:

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

Answer:

Users who can modify the permissions for RG1:


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



Users who can create virtual networks in RG1:

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

Explanation:



Users who can modify the permissions for RG1:

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

Users who can create virtual networks in RG1:

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

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

- A. Active Directory Enterprise Admins
- B. Azure AD Global Admins
- C. Azure AD Global Admins
- D. Azure AD Global Admins
- 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 PIM
- B. contoso.com
- C. contoso.com ID
- D. User2 PIM (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` is a managed group. `RG1` is a resource group. `VM1` is a virtual machine. You want to grant `Role1` to `MG1`. What should you do?

Name	Scoped to
Role1	MG1
Role2	RG1

`Role1` is a role that is scoped to `MG1`.

```
"permissions": [
  {
    "actions": [
      "Microsoft.Compute/virtualMachines/*"
    ],
    "notActions": [
      "Microsoft.Compute/virtualMachines/delete"
    ],
    "dataActions": [],
    "notDataActions": []
  }
]
```

You need to grant `Role1` to `MG1`. What should you do?

Name	Role
User1	Role1
User2	Role1, Role2
User3	Role2

You need to grant `Role1` to `MG1`. What should you do? (Select all that apply.)

Answer Area

Statements	Yes	No
User1 can delete VM1.	<input type="radio"/>	<input type="radio"/>
User2 can delete VM1.	<input type="radio"/>	<input type="radio"/>
User3 can delete VM1.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 can delete VM1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can delete VM1.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can delete VM1.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Answer Area

Statements	Yes	No
User1 can delete VM1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can delete VM1.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can delete VM1.	<input checked="" type="radio"/>	<input type="radio"/>

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 Area

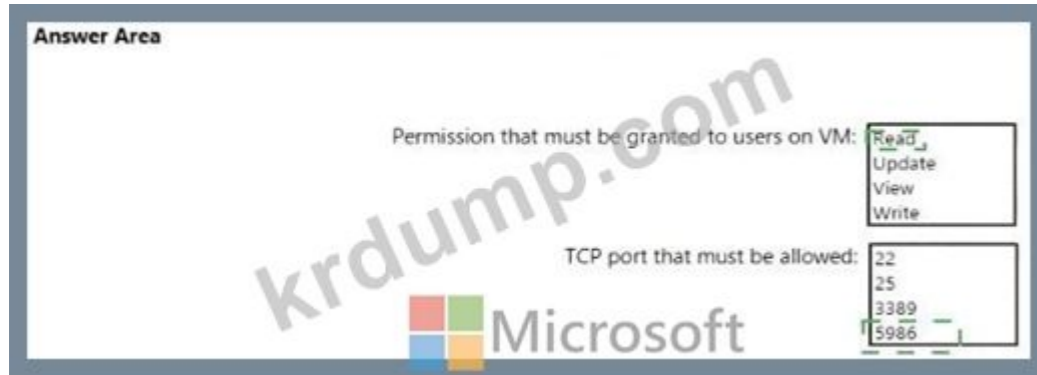
Permission that must be granted to users on VM:

Read	<input type="checkbox"/>
Update	<input type="checkbox"/>
View	<input checked="" type="checkbox"/>
Write	<input type="checkbox"/>

TCP port that must be allowed:

22	<input type="checkbox"/>
25	<input type="checkbox"/>
3389	<input checked="" type="checkbox"/>
5986	<input type="checkbox"/>

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 is an Azure Key Vault. VM1 is a virtual machine. VM1 is connected to Azure Key Vault.

VM1 is connected to VNet1. VNet1 is connected to the Internet.

VM1 is connected to Vault1. Vault1 is connected to the Internet.

Vault1 is connected to the Internet. What is the correct configuration?

- A. VM1 is connected to VNet1. VNet1 is connected to the Internet.
- B. VM1 is connected to VNet1. VNet1 is connected to the Internet.
- C. VM1 is connected to VNet1. VNet1 is connected to the Internet.
- D. VM1 is connected to VNet1. VNet1 is connected to the Internet.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 9

RG1 is a resource group. RG2 is a resource group. ServerAdmins is a security group.

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 is a security group. RG1 is a resource group. RG2 is a resource group.

RG2 is a resource group. ServerAdmins is a security group.

ServerAdmins is a security group. RG1 is a resource group.

ServerAdmins is a security group. RG1 is a resource group. RG2 is a resource group. ServerAdmins is a security group. What is the correct configuration?

RG1: RG1 is a resource group.

- A. RG1 is a resource group.
- B. RG2 is a resource group.
- C. RG1 is a resource group.
- D. RG2 is a resource group.
- E. RG1 is a resource group.
- F. RG2 is a resource group.

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

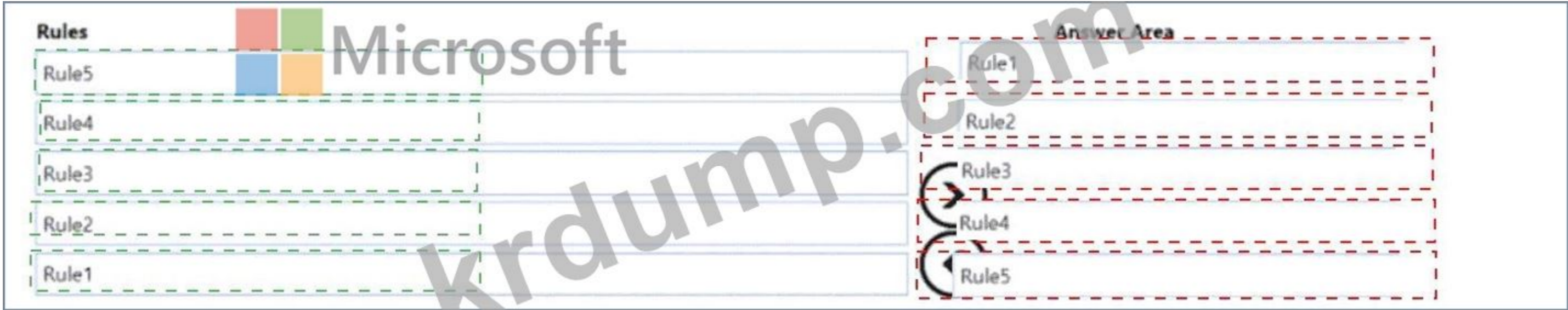
□□□ □□ □□□ □□□□ □□□□ □□□□ □□ □□ □□□ □□ □□ □□□ □□ □□□ □□□□ □□□□□.

Rules

- Rule5
- Rule4
- Rule3
- Rule2
- Rule1

Navigation icons: > and <

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 [redacted] Azure [redacted] [redacted].
 Azure Security Center [redacted] WF1 [redacted] [redacted] [redacted] [redacted]. WF1 [redacted] User1 [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted].
 Alerts [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] WF1 [redacted] [redacted] [redacted].
 WF1 [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]?

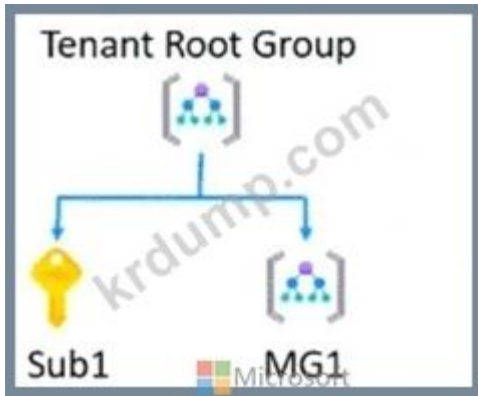
- A. Azure [redacted] [redacted]
- B. Azure [redacted]
- C. Azure Logic Apps [redacted]
- D. Azure DevOps

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 [redacted] Sub1 [redacted] Azure [redacted] [redacted]. [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted].



Which of the following is a valid location for a policy?

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

Which of the following is a valid location for a policy?

- A. Policy1, Initiative1, Initiative2, Initiative3
- B. Policy1, Initiative1
- C. Initiative1, Initiative2, Initiatives
- D. Policy1
- E. Initiative1, Initiative2

Answer: B (LEAVE A REPLY)

NEW QUESTION: 16

contoso.com is a Microsoft Entra ID tenant. You need to configure a policy to review user sign-in activity. Which of the following is a valid location for a policy?

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

Which of the following is a valid location for a policy?

Review name *

Description

Start date *

Frequency

Duration (in days)

End

Number of times

End date *

Users

Scope Everyone

Review role membership (permanent and eligible) *

[Password Administrator](#)

Reviewers

Reviewers

^ Upon completion settings

Auto apply results to resource

Microsoft

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

□□: □□ 1□□ 1□□□□.

Answer Area

User3 can perform Review1 for [answer choice].

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

If User2 fails to complete Review1 by December 12, 2020, [answer choice].

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

Answer:

User3 can perform Review1 for [answer choice].

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

If User2 fails to complete Review1 by December 12, 2020, [answer choice].

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

Explanation:
Answer Area

User3 can perform Review1 for [answer choice].

- User3 only

If User2 fails to complete Review1 by December 12, 2020, [answer choice].

- User3 will receive a confirmation request

AZ-500-KR ☐☐ ☐☐☐ ☐☐☐☐☐ ☐☐ DumpTop ☐☐ ☐☐☐☐ ☐☐☐ AZ-500-KR ☐☐! DumpTop ☐ ☐☐ **AZ-500-KR** ☐☐ ☐☐☐ ☐☐☐☐☐☐, DumpTop AZ-500-KR ☐☐ ☐☐☐ ☐☐☐☐☐☐☐☐. ☐☐☐☐☐ ☐☐☐☐☐☐☐ ☐☐ DumpTop AZ-500-KR ☐☐☐ ☐☐☐☐☐. <https://www.dumptop.com/Microsoft/AZ-500-KR-dump.html> (517 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

NEW QUESTION: 17

☐☐ ☐☐☐☐ ☐☐ ☐☐☐☐☐ ☐☐ ☐☐(NSG)☐☐ ☐☐ 10☐☐☐☐ ☐☐☐☐☐☐☐☐. Azure Storage ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐.

Which of the following is a valid Azure Resource ID for a network security group (NSG)?

Options: 1. /subscriptions/12345678-9010-1111-2222-333333333333

A. /subscriptions/12345678-9010-1111-2222-333333333333/resourceGroups/rg1/providers/Microsoft.Network/networkSecurityGroups/nsg1

B. Azure Network Watcher /subscriptions/12345678-9010-1111-2222-333333333333

C. NSG /subscriptions/12345678-9010-1111-2222-333333333333

D. NSG /subscriptions/12345678-9010-1111-2222-333333333333

E. Azure Log Analytics /subscriptions/12345678-9010-1111-2222-333333333333

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 is a Web Application Firewall (WAF) instance in the West Europe region. It is currently configured to protect a web application in the West Europe region. You need to configure WAF1 to protect a web application in the East US region. What should you do?

Options: 1. Create a new WAF instance in the East US region.

Options: 2. Move WAF1 to the East US region.

A. Azure Bot Manager.

B. Bot Manager 1.1.

C. Azure Bot Framework.

D. Azure Bot Framework SDK.

Answer: [C \(LEAVE A REPLY\)](#)

NEW QUESTION: 19

You have an Azure subscription with the following virtual machines (VMs):

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

You plan to create an Azure Log Analytics workspace in the East US region. Which VMs will be monitored by the workspace?

Options: 1. VM1, VM2, VM3, and VM4

A. VM1

B. VM1, VM2, VM3, and VM4

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 VMs.

VM1 VM2 VM3 VM4 VM5 VM6 VM7 VM8 VM9 VM10 VM11 VM12 VM13 VM14 VM15 VM16 VM17 VM18 VM19 VM20 VM21 VM22 VM23 VM24 VM25 VM26 VM27 VM28 VM29 VM30 VM31 VM32 VM33 VM34 VM35 VM36 VM37 VM38 VM39 VM40 VM41 VM42 VM43 VM44 VM45 VM46 VM47 VM48 VM49 VM50 VM51 VM52 VM53 VM54 VM55 VM56 VM57 VM58 VM59 VM60 VM61 VM62 VM63 VM64 VM65 VM66 VM67 VM68 VM69 VM70 VM71 VM72 VM73 VM74 VM75 VM76 VM77 VM78 VM79 VM80 VM81 VM82 VM83 VM84 VM85 VM86 VM87 VM88 VM89 VM90 VM91 VM92 VM93 VM94 VM95 VM96 VM97 VM98 VM99 VM100.

VM1 VM2 VM3 VM4 VM5 VM6 VM7 VM8 VM9 VM10 VM11 VM12 VM13 VM14 VM15 VM16 VM17 VM18 VM19 VM20 VM21 VM22 VM23 VM24 VM25 VM26 VM27 VM28 VM29 VM30 VM31 VM32 VM33 VM34 VM35 VM36 VM37 VM38 VM39 VM40 VM41 VM42 VM43 VM44 VM45 VM46 VM47 VM48 VM49 VM50 VM51 VM52 VM53 VM54 VM55 VM56 VM57 VM58 VM59 VM60 VM61 VM62 VM63 VM64 VM65 VM66 VM67 VM68 VM69 VM70 VM71 VM72 VM73 VM74 VM75 VM76 VM77 VM78 VM79 VM80 VM81 VM82 VM83 VM84 VM85 VM86 VM87 VM88 VM89 VM90 VM91 VM92 VM93 VM94 VM95 VM96 VM97 VM98 VM99 VM100.

VM1 VM2 VM3 VM4 VM5 VM6 VM7 VM8 VM9 VM10 VM11 VM12 VM13 VM14 VM15 VM16 VM17 VM18 VM19 VM20 VM21 VM22 VM23 VM24 VM25 VM26 VM27 VM28 VM29 VM30 VM31 VM32 VM33 VM34 VM35 VM36 VM37 VM38 VM39 VM40 VM41 VM42 VM43 VM44 VM45 VM46 VM47 VM48 VM49 VM50 VM51 VM52 VM53 VM54 VM55 VM56 VM57 VM58 VM59 VM60 VM61 VM62 VM63 VM64 VM65 VM66 VM67 VM68 VM69 VM70 VM71 VM72 VM73 VM74 VM75 VM76 VM77 VM78 VM79 VM80 VM81 VM82 VM83 VM84 VM85 VM86 VM87 VM88 VM89 VM90 VM91 VM92 VM93 VM94 VM95 VM96 VM97 VM98 VM99 VM100.

VM1 VM2 VM3 VM4 VM5 VM6 VM7 VM8 VM9 VM10 VM11 VM12 VM13 VM14 VM15 VM16 VM17 VM18 VM19 VM20 VM21 VM22 VM23 VM24 VM25 VM26 VM27 VM28 VM29 VM30 VM31 VM32 VM33 VM34 VM35 VM36 VM37 VM38 VM39 VM40 VM41 VM42 VM43 VM44 VM45 VM46 VM47 VM48 VM49 VM50 VM51 VM52 VM53 VM54 VM55 VM56 VM57 VM58 VM59 VM60 VM61 VM62 VM63 VM64 VM65 VM66 VM67 VM68 VM69 VM70 VM71 VM72 VM73 VM74 VM75 VM76 VM77 VM78 VM79 VM80 VM81 VM82 VM83 VM84 VM85 VM86 VM87 VM88 VM89 VM90 VM91 VM92 VM93 VM94 VM95 VM96 VM97 VM98 VM99 VM100.



Answer:
Answer Area



Explanation:



NEW QUESTION: 23

WebApp1 Azure App Services Azure App Services Azure App Services. WebApp1 Azure App Services Azure App Services Azure App Services.

WebApp1 Azure App Services Azure App Services Azure App Services Azure App Services.

* Azure App Services Azure App Services Azure App Services Azure App Services.

* Which Azure service is used to cache content from external sources?

Which Azure service is used to cache content from external sources?

- A. Azure Content Delivery Network
- B. Azure Front Door
- C. Azure Cache for Redis
- D. Azure Front Door Cache

Answer: D (LEAVE A REPLY)

NEW QUESTION: 24

Azure Key Vault Vault1 is an Azure Key Vault. Vault1 key1 is a 2048-bit RSA key.

key1 is 90 days before expiration. How can you extend the expiration date?

How can you extend the expiration date?

- A. Use the Azure Key Vault REST API.
- B. Vault1 Key Vault Premium has an auto-rotate feature.
- C. Vault1 has an auto-rotate feature.
- D. key1 is an EC key and cannot be rotated.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 25

Which Azure service is used to manage privileged identities?

Which Azure service is used to manage privileged identities?

Which Azure service is used to manage privileged identities?

Which Azure service is used to manage privileged identities?

- 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

Answer: C (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 26

Which Azure service is used to manage network security? Which Azure service is used to manage network security?

Which Azure service is used to manage network security? Which Azure service is used to manage network security?

Which Azure service is used to manage network security? Which Azure service is used to manage network security?

Which Azure service is used to manage network security? Which Azure service is used to manage network security?

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

SQL1 is an Azure SQL database. Microsoft Entra ID contains the following objects:

Name	Description
User1	<ul style="list-style-type: none"> Member of Group1 and Group2 Assigned Owner role for App1 and MI1
User2	<ul style="list-style-type: none"> Member of Group1 and Group2 Assigned Owner role for App1 and MI1

SQL1 is an Azure SQL database. Microsoft Entra ID contains the following objects:

User1 and User2 are users in Microsoft Entra ID. SQL1 is an Azure SQL database.

App1 is an application registration in Microsoft Entra ID.

MI1 is a user-assigned managed identity in Microsoft Entra ID.

A. User1

B. User2

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 27

Microsoft Defender for Cloud is configured to monitor the following resources:

Resource 1: Microsoft Entra ID

Resource 2: Microsoft SQL Server

Resource 3: Microsoft 365 Group

Answer Area



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

Answer:



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

```

Explanation:

A screenshot of a computer Description automatically generated

Answer Area

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

NEW QUESTION: 28

Defender for Cloud is a cloud-native security solution that provides protection for Microsoft 365, Azure, and Microsoft Dynamics 365. It is designed to detect and respond to threats in real-time. Defender for Cloud is a cloud-native security solution that provides protection for Microsoft 365, Azure, and Microsoft Dynamics 365. It is designed to detect and respond to threats in real-time.

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

Answer: D (LEAVE A REPLY)

NEW QUESTION: 29

DB1 is an Azure SQL Database instance. Which storage account should be used for backup files?

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 is an Azure SQL Database instance. Which storage account should be used for backup files?

DB1 is an Azure SQL Database instance. Which storage account should be used for backup files?

- A. Storage2 and storage3
- B. storage1 and storage4
- C. storage1
- D. storage1, storage2 and storage3

Answer: A (LEAVE A REPLY)

NEW QUESTION: 30

Which policy should be used to enforce session lifetime?

CAPolicy1 is a Conditional Access policy. Which policy should be used to enforce session lifetime?

- A. CAPolicy1
- B. CAPolicy2
- C. CAPolicy3
- D. CAPolicy4

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 is an Azure AD Premium P2 tenant. Which role should be assigned to User1?

User1 is a user in the contoso.com Azure AD Premium P2 tenant. Which role should be assigned to User1?

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

User1 is a user in the contoso.com Azure AD Premium P2 tenant. Which role should be assigned to User1?

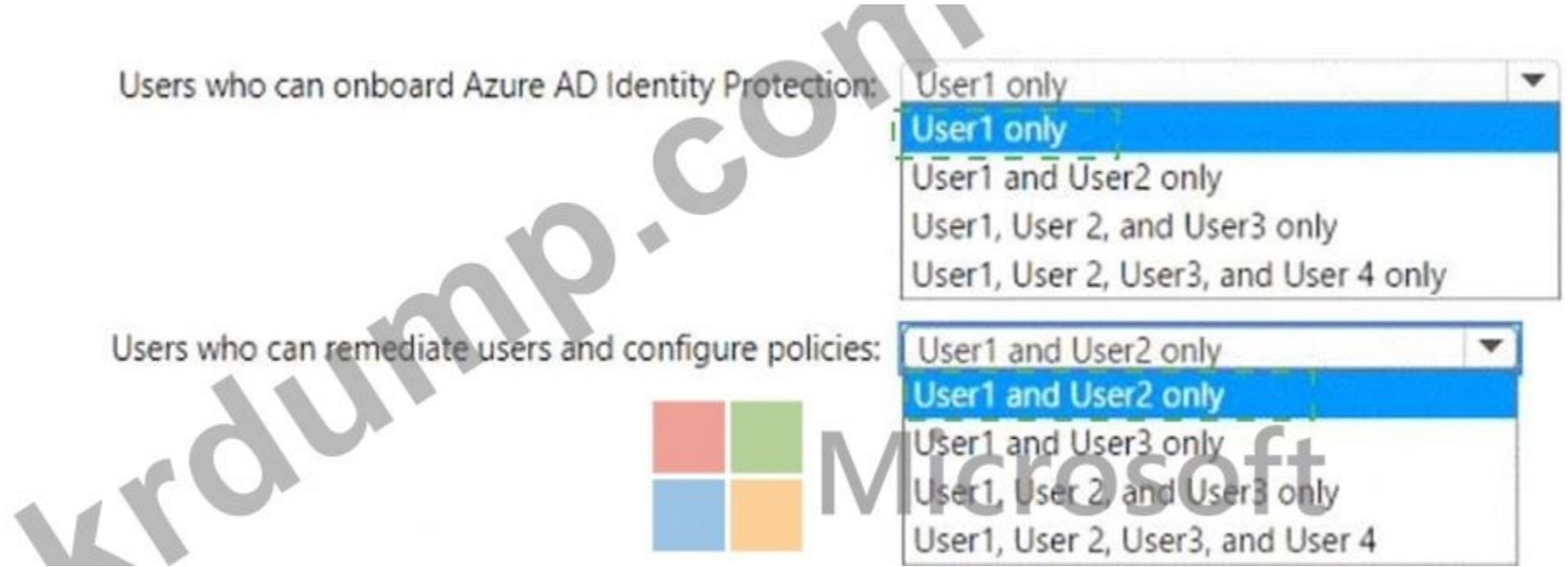
User1 is a user in the contoso.com Azure AD Premium P2 tenant. Which role should be assigned to User1?

User1 is a user in the contoso.com Azure AD Premium P2 tenant. Which role should be assigned to User1?

User1 is a user in the contoso.com Azure AD Premium P2 tenant. Which role should be assigned to User1?



Answer:
User1 only



Explanation:



AZ-500-KR ☐☐ ☐☐☐ ☐☐☐☐☐ ☐☐ DumpTop ☐☐ ☐☐☐☐ ☐☐☐ AZ-500-KR ☐☐! DumpTop ☐ ☐☐ AZ-500-KR ☐☐ ☐☐☐ ☐☐☐☐☐☐, DumpTop AZ-500-KR ☐☐ ☐☐☐ ☐☐☐☐☐☐☐☐☐☐. ☐☐☐☐☐ ☐☐☐☐☐☐☐☐☐☐ ☐☐ DumpTop AZ-500-KR ☐☐☐ ☐☐☐☐☐. <https://www.dumptop.com/Microsoft/AZ-500-KR-dump.html> (517 Q&As Dumps, **30%OFF**)

Special Discount: **KrDump**)

NEW QUESTION: 32

Which Azure SQL Server can be used as the audit log destination?
 Which Azure SQL database can be used as the audit log destination?
 Which Azure SQL database can be used as the audit log destination?

- A. SQL1
- B. SQL1, Analytics1, and Analytics2
- C. Analytics1, Analytics2, and Analytics3
- D. SQL1, Analytics1, and Analytics3

Answer: C (LEAVE A REPLY)

NEW QUESTION: 33

Which Azure Storage account can be used as the audit log destination?

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

Which Azure Storage account can be used as the audit log destination?

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 can be used as the audit log destination.

Which Azure Storage account can be used as the audit log destination? Select all that apply.

Options: Storage1, Storage2, Storage3

Answer Area



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

- Storage1 only
- Storage2 only
- Storage1 and Storage2 only
- Storage1, Storage2, and Storage3

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

- Analytics1 only
- Analytics1 and Analytics2 only
- Analytics1 and Analytics3 only
- Analytics1, Analytics2, and Analytics3

Answer:

Answer Area

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

- Storage1 only
- Storage2 only
- Storage1 and Storage2 only
- Storage1, Storage2, and Storage3

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

- Analytics1 only
- Analytics1 and Analytics2 only
- Analytics1 and Analytics3 only
- Analytics1, Analytics2, and Analytics3

Explanation:

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

- Storage1 only
- Storage2 only
- Storage1 and Storage2 only
- Storage1, Storage2, and Storage3

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

- Analytics1 only
- Analytics1 and Analytics2 only
- Analytics1 and Analytics3 only
- Analytics1, Analytics2, and Analytics3

NEW QUESTION: 34

Contosostorage1 is an Azure Storage account. Contosokeyvault1 is an Azure Key Vault. Sub1 is an Azure subscription. Contosostorage1 is in the same region as Contosokeyvault1. Azure Automation is configured to run a script that uses Contosokeyvault1 to retrieve a secret. The script is run from a virtual machine in Sub1. The script fails with the error: 'The storage account Contosostorage1 is not accessible. The account is not in the same region as the virtual machine.' What should you do to resolve the issue?

Actions

Answer Area

Run Set-AzureRmKeyVaultAccessPolicy

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

Create a user-assigned managed identity.

Create a connection resource in the Azure Automation account.



Answer:

Actions

Answer Area

Run Set-AzureRmKeyVaultAccessPolicy

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

Create a user-assigned managed identity.

Create a connection resource in the Azure Automation account.

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

Create a connection resource in the Azure Automation account.



Explanation:

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.



Create a connection resource in the Azure Automation account.

Step 1: Create an Azure Automation account

Runbooks live within the Azure Automation account and can execute PowerShell scripts.

Step 2: Import PowerShell modules to the Azure Automation account

Under 'Assets' from the Azure Automation account Resources section select 'to add in Modules to the runbook. To execute key vault cmdlets in the runbook, we need to add AzureRM.profile and AzureRM.key vault.

Step 3: Create a connection resource in the Azure Automation account

You can use the sample code below, taken from the AzureAutomationTutorialScript example runbook, to authenticate using the Run As account to manage Resource Manager resources with your runbooks. The AzureRunAsConnection is a connection asset automatically created when we created 'run as accounts' above.

This can be found under Assets - > Connections. After the authentication code, run the same code above to get all the keys from the vault.

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

References:

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

NEW QUESTION: 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 10.1.0.4.

VM5 JIT(Just-in-Time) VM 10.1.0.4.

JIT VM access configuration ✕

VM5

+ Add Save Discard

Configure the ports for which the just-in-time VM access will be applicable

Port	Protocol	Allowed source IPs	IP range	Time range (hours)	
3389	Any	Per request	N/A	3 hours	...

VM5 JIT VM 10.1.0.4.

NSG1 10.1.0.4.

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

10.1.0.4, 10.1.0.4 '10.1.0.4'. 10.1.0.4 '10.1.0.4' 10.1.0.4.

10.1.0.4: 10.1.0.4.

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.	<input type="radio"/>	<input type="radio"/>
Remote Desktop access to VM5 is blocked.	<input type="radio"/>	<input type="radio"/>
An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.	<input type="radio"/>	<input type="radio"/>

Explanation:

Statements	Yes	No
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	<input type="radio"/>	<input type="radio"/>
Remote Desktop access to VM5 is blocked.	<input type="radio"/>	<input type="radio"/>
An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.	<input type="radio"/>	<input type="radio"/>

NEW QUESTION: 36

□□□ □□□ □□□ □□□□ □□□□.

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

□□ □□ □□□ □□ □□□ □□□□ □□□.

* □□ □□□ □□□ □□□

* □□□□□ □□□□ □□□ □□□□□□□.

* □□□□□ □□□ □□ IP □□□□□ □□□

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

□□: □□ 1□□ 1□□□□□.

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

Answer:

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

Explanation:

Medium

High

Medium

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

NEW QUESTION: 37

storage1 is a storage account in a virtual network (VNet) named VNet1 in an Azure subscription. VM1 is a virtual machine in VNet1. VM1 is connected to storage1. VM1 is running a script that attempts to connect to storage1. The script fails with the error message: "Unable to connect to storage1: The IP address of the storage account is not in the allowed IP address range for this virtual network." What should you do to resolve this issue?

- A. storage1 is a storage account in a virtual network (VNet) named VNet1 in an Azure subscription. VM1 is a virtual machine in VNet1. VM1 is connected to storage1. VM1 is running a script that attempts to connect to storage1. The script fails with the error message: "Unable to connect to storage1: The IP address of the storage account is not in the allowed IP address range for this virtual network." What should you do to resolve this issue?
- B. storage1 is a storage account in a virtual network (VNet) named VNet1 in an Azure subscription. VM1 is a virtual machine in VNet1. VM1 is connected to storage1. VM1 is running a script that attempts to connect to storage1. The script fails with the error message: "Unable to connect to storage1: The IP address of the storage account is not in the allowed IP address range for this virtual network." What should you do to resolve this issue?
- C. VNet1 is a virtual network in an Azure subscription. VM1 is a virtual machine in VNet1. VM1 is connected to storage1. VM1 is running a script that attempts to connect to storage1. The script fails with the error message: "Unable to connect to storage1: The IP address of the storage account is not in the allowed IP address range for this virtual network." What should you do to resolve this issue?
- D. Azure is a cloud platform. VM1 is a virtual machine in an Azure subscription. VM1 is connected to storage1. VM1 is running a script that attempts to connect to storage1. The script fails with the error message: "Unable to connect to storage1: The IP address of the storage account is not in the allowed IP address range for this virtual network." What should you do to resolve this issue?

Answer: A (LEAVE A REPLY)

NEW QUESTION: 38

You are a Microsoft Azure administrator. You have a Microsoft Azure subscription that contains a Microsoft Azure Security Center (ASC) resource. You need to ensure that the ASC resource is configured to monitor for security alerts. What should you do?

Options:

- A.
- B.

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 is a Microsoft Entra ID tenant. Admin1 is connected to an Azure Active Directory(Azure AD) tenant. Admin1 is connected to an Azure AD tenant. Admin1 is connected to an Azure AD tenant.

App1 is an application registered in the Azure AD tenant. App1 is an application registered in the Azure AD tenant. App1 is an application registered in the Azure AD tenant.

Admin1 is connected to the Azure AD tenant. Admin1 is connected to the Azure AD tenant. Admin1 is connected to the Azure AD tenant.

Azure Portal is used to manage the Azure AD tenant. Azure Portal is used to manage the Azure AD tenant. Azure Portal is used to manage the Azure AD tenant.

What is the correct configuration?

- A. App1 is added as an enterprise application.
- B. App1 is added as a public application.
- C. App1 is added as a service principal.
- D. Admin1 is added as an enterprise application.

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 is a virtual machine in a virtual network.

VM1 is connected to VNet1. VNet1 is connected to VNet1. VNet1 is connected to VNet1. VNet1 is connected to VNet1. VNet1 is connected to VNet1.

storage1 is a storage account in the same region as VNet1.

storage1 is connected to VNet1. storage1 is connected to VNet1. storage1 is connected to VNet1. storage1 is connected to VNet1. storage1 is connected to VNet1.

* App1 is connected to VNet1. App1 is connected to VNet1. App1 is connected to VNet1. App1 is connected to VNet1. App1 is connected to VNet1.

* VNet1 is connected to storage1. VNet1 is connected to storage1. VNet1 is connected to storage1. VNet1 is connected to storage1. VNet1 is connected to storage1.

* VNet1 is connected to storage1. VNet1 is connected to storage1. VNet1 is connected to storage1. VNet1 is connected to storage1. VNet1 is connected to storage1.

What is the correct configuration? VM1 is connected to VNet1. VM1 is connected to VNet1. VM1 is connected to VNet1. VM1 is connected to VNet1. VM1 is connected to VNet1.

Answer: VM1 is connected to VNet1.

Components

- A private endpoint
- A service endpoint
- An access restriction rule
- Azure Private Link

Answer Area

Microsoft

storage1:

App1:

Answer:

Components

- A private endpoint
- A service endpoint
- An access restriction rule
- Azure Private Link

Answer Area

Microsoft

storage1: A private endpoint

App1: Azure Private Link

Explanation:

Components

- A private endpoint
- A service endpoint
- An access restriction rule
- Azure Private Link

Answer Area

Microsoft

storage1: A private endpoint

App1: Azure Private Link

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) is used to manage Azure resources. User1 is a user who is assigned the role of Administrator. User1 is assigned the role of Administrator for 2 hours. How long does the role last?

- A. 1 hour
- B. 2 hours
- C. 3 hours
- D. 4 hours

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 43

Admin1 is a user who is assigned the role of Administrator for Azure Monitor.

Azure Monitor is used to monitor Azure resources. Admin1 is assigned the role of Administrator for Azure Monitor. Admin1 is assigned the role of Administrator for Azure Monitor. Admin1 is assigned the role of Administrator for 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 is assigned the role of Administrator for Azure Monitor. Admin1 is assigned the role of Administrator for Azure Monitor. Admin1 is assigned the role of Administrator for Azure Monitor.

* VNET1 is a virtual network that is used to connect Azure resources. Admin1 is assigned the role of Administrator for VNET1. Admin1 is assigned the role of Administrator for VNET1. Admin1 is assigned the role of Administrator for VNET1.

* Lock1 is a lock that is used to prevent changes to Azure resources. Admin1 is assigned the role of Administrator for Lock1. Admin1 is assigned the role of Administrator for Lock1. Admin1 is assigned the role of Administrator for Lock1.

Admin1 is assigned the role of Administrator for Azure Monitor. Admin1 is assigned the role of Administrator for Azure Monitor. Admin1 is assigned the role of Administrator for Azure Monitor. Admin1 is assigned the role of Administrator for Azure Monitor.

Admin1 is assigned the role of Administrator for Azure Monitor. Admin1 is assigned the role of Administrator for Azure Monitor. Admin1 is assigned the role of Administrator for Azure Monitor. Admin1 is assigned the role of Administrator for Azure Monitor.

Adding VNET1:

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

Adding Lock1:

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

Answer:

Adding VNET1:

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

Adding Lock1:

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

Explanation:

Adding VNET1:

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

Adding Lock1:



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

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:

Actions

Answer Area

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

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](#))

AZ-500-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ AZ-500-KR □□! DumpTop □ □□ **AZ-500-KR** □□ □□□ □□□□□□, DumpTop AZ-500-KR □□ □□□ □□□□□ □□□ □□□ □□□□□□□□. □□□□ □□□ □□□□ □□ DumpTop AZ-500-KR □□□ □□□□□. <https://www.dumptop.com/Microsoft/AZ-500-KR-dump.html> (517 Q&As Dumps, **30%OFF**

Special Discount: **KrDump**)

NEW QUESTION: 47

□□ □□□ □□□□ □□ Azure Sentinel □□ □□□ □□□□.

* Azure Active Directory ID □□

* □□ □□□ □□(CEF)

* Azure □□□

□ □□□□□ □□□□ □□□□□ □□□□ □□□.

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

□□: □□ 1□□ 1□□□□.

Azure Active Directory Identity Protection:



Microsoft
AzureDiagnostics
CommonSecurityLog
SecurityAlert
SecurityEvent
Syslog


Azure Firewall:

AzureDiagnostics
CommonSecurityLog
SecurityAlert
SecurityEvent
Syslog

CEF:

AzureDiagnostics
CommonSecurityLog
SecurityAlert
SecurityEvent
Syslog

Answer:

Azure Active Directory Identity Protection: 

AzureDiagnostics
CommonSecurityLog
SecurityAlert
SecurityEvent
Syslog

Azure Firewall:

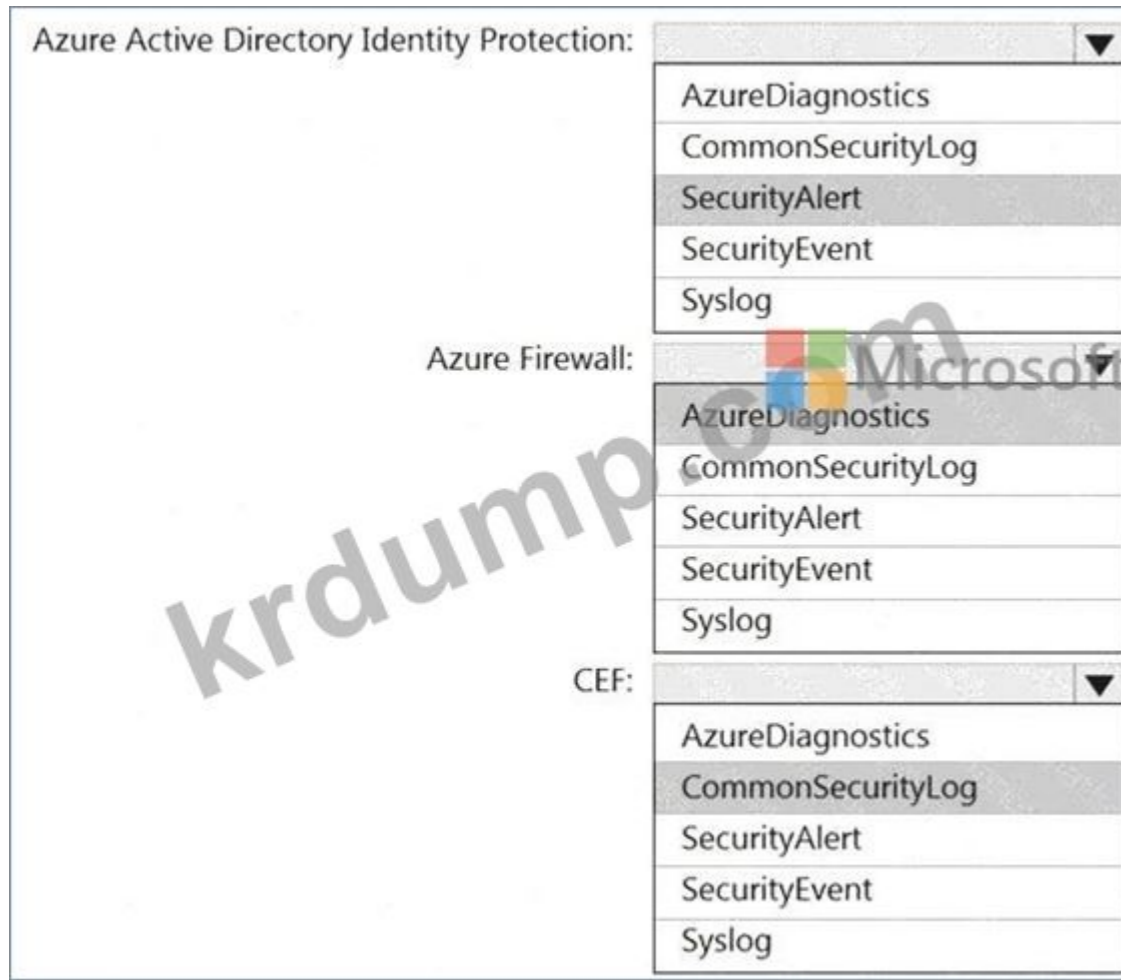
AzureDiagnostics
CommonSecurityLog
SecurityAlert
SecurityEvent
Syslog

CEF:

AzureDiagnostics
CommonSecurityLog
SecurityAlert
SecurityEvent
Syslog

Explanation:

Graphical user interface, application, table Description automatically generated



NEW QUESTION: 48

webapp1 is an Azure App Service.

Azure Repo is a GitHub repository connected to webapp1.

Which tool can you use to monitor the application logs?

- A. Azure DevOps
- B. Azure Storage
- C. Azure Application Insights
- D. Azure DevTest Labs

Answer: [\(SHOW ANSWER\)](#)

NEW QUESTION: 49

KeyVault1 is an Azure Key Vault.

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

Which tool can you use to monitor the application logs?

KeyVault1 is an Azure Key Vault.

Save Discard Microsoft

Allow access from: All networks Selected networks

[Configure network access control for your key vault. Learn More](#)

Virtual networks: [+ Add existing virtual networks](#) [+ Add new virtual network](#)

VIRTUAL NETWORK	SUBNET	RESOURCE GROUP	SUBSCRIPTION
VNET1	default	RG1	...

Firewall: [i](#)

IPv4 ADDRESS OR CIDR

...

Exception:

Allow trusted Microsoft services to bypass this firewall? Yes No

[i](#) This setting is related to firewall only. In order to access this key vault, the trusted service must also be given explicit permissions in the Access policies section.

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

□□: □□ 1□□ 1□□□□.

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

Answer:

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

Explanation:

Answer Area

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

NEW QUESTION: 50

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

Save Discard changes Refresh

Name	sk2311
Skus (Pricing tier)	Standard
Location	eastus
Vault URI	<input type="text" value="https://sk2311.vault.azure.net/"/>
Resource ID	<input type="text" value="/subscriptions/7fed66e-8694-4b54-beae-..."/>
Subscription ID	<input type="text" value="7fed66e-8694-4b54-beae-17fd819d4873"/>
Subscription Name	<input type="text" value="Visual Studio Enterprise Subscription"/>
Directory ID	<input type="text" value="5864e735-7190-4615-b2a0-0b20615b75de"/>
Directory Name	<input type="text" value="Default Directory"/>

Soft-delete **Soft delete has been enabled on this key vault**

Days to retain deleted vaults

- Purge protection
- Disable purge protection (allow key vault and objects to be purged during retention period)
 - Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)

Sk2311

Name	Type
Item1	Key
Item2	Secret
Policy1	Access policy

sk2311

* Item1

* Item2

Item1: sk2311, Item2: sk2311

Item1: sk2311

Answer Area



Statements

Yes

No

You can recover Policy1.

You can add a new key named Item1.

You can recover Item2.

Answer:

Answer Area



Statements

Yes

No

You can recover Policy1.

You can add a new key named Item1.

You can recover Item2.

Explanation:

Answer Area

Statements

You can recover Policy1. Yes No

You can add a new key named Item1. Yes No

You can recover Item2. Yes No

NEW QUESTION: 51

RT1 is connected to an Azure virtual network. RT1 is connected to a virtual network. RT1 is connected to a virtual network.

* RT1 : RouteA

* IP address: 192.168.0.0/24

* RT1 IP: 172.16.10.10

RT1 is connected to a virtual network.

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 is connected to a virtual network?

A. Route2

B. Route1

C. Route1 Route2

D. Route1 Route3

E. Route2 Route3

F. Route3

Answer: D (LEAVE A REPLY)

NEW QUESTION: 52

Azure

The screenshot shows the 'All Alerts' page in the Azure portal. At the top, there are navigation options: 'New alert rule', 'Edit columns', 'Manage alert rules', 'View classic alerts', 'Refresh', and 'Change state'. Below this is a filter section with dropdown menus for 'Subscription' (Azure Pass - Sponsorship), 'Resource group' (Type to start filtering...), 'Resource type' (0 selected), 'Resource' (Type to start filtering...), 'Time range' (Past hour), 'Monitor service' (15 selected), 'Monitor condition' (2 selected), 'Severity' (Sev 4), 'Alert state' (3 selected), and 'Smart group id' (Smart group id). The main area shows a table of alerts with the following data:

NAME	SEVERITY	MONITOR C...	ALERT STATE	AFFECT...	MONITOR SERV...	SIGNAL TYPE	FIRED TIME	SU...
Alert1	Sev4	Fired	New		ActivityLog Ad...	Log	6/6/2019, 11:23:53 ...	Azure ...
Alert1	Sev4	Fired	Acknowledged		ActivityLog Ad...	Log	6/6/2019, 11:23:52 ...	Azure ...
Alert2	Sev4	Fired	Acknowledged		ActivityLog Ad...	Log	6/6/2019, 11:23:25 ...	Azure ...
Alert2	Sev4	Fired	Closed		ActivityLog Ad...	Log	6/6/2019, 11:23:24 ...	Azure ...

Azure

Azure

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

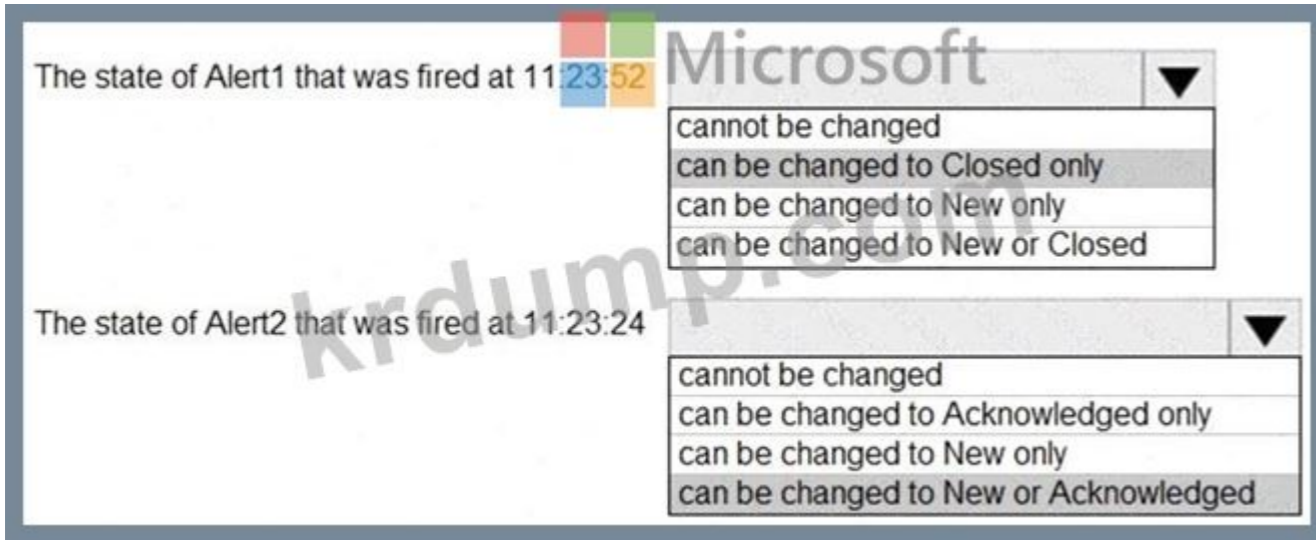
The state of Alert2 that was fired at 11:23:24

Answer:

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

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

Explanation:



References:

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

NEW QUESTION: 53

Which of the following Azure resources are included in the alert rule?

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 is included in the alert rule.

* DB1 is included in the alert rule.

* storage1, Workspace1

DB1 is included in the alert rule.

* DB2 is included in the alert rule.

* storage2

DB2 is included in the alert rule.

DB1, DB2, storage1, storage2, and Workspace1 are included in the alert rule.

Answer Area



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. _____.

* KeyVault1 key1 _____.

* KeyVault2 secret 1 _____.

_____, _____ '_____' _____.

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

Answer:

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

Explanation:

Yes

Yes

No

NEW QUESTION: 57

User1 is a member of the storage1 group in an Azure Active Directory. storage1 is a group in an Azure Active Directory. storage1 is a group in an Azure Active Directory.

Name	Type
container1	Container
folder1	File share
table1	Table

User1 is a member of the storage1 group in an Azure Active Directory.

- * container1 Blob storage
- * folder1 File share
- * table1 Table storage

Statements

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.

Yes

No

Answer:

Statements	Yes	No
On October 1, 2022, if User1 accesses folder1 by using SAS1, he can delete the files in folder1.	<input type="radio"/>	<input checked="" type="radio"/>
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.	<input checked="" type="radio"/>	<input type="radio"/>
On October 1, 2022, User1 can delete the rows in table1 by using SAS1.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

No, Yes, No

NEW QUESTION: 58

Company1 is a member of the storage1 group in an Azure Active Directory.

Company1 is a member of the storage1 group in an Azure Active Directory. storage1 is a group in an Azure Active Directory. storage1 is a group in an Azure Active Directory.

* Any; Any

* Any : Any

* Any: 100

* Any: Any

* Any: Any

* Any: Any

Company1 storage1 is a member of the storage1 group in an Azure Active Directory.

Company1 storage1 is a member of the storage1 group in an Azure Active Directory.

* Any: Microsoft.Storage/storageAccounts

* storage1

* blob

* VNet1

* Subnet1

From VM2, you can create a container in storage1.

From VM1, you can upload data to the blob storage of storage1.

Answer Area

Statements	Yes	No
From VM2, you can create a container in storage1.	<input type="radio"/>	<input type="radio"/>
From VM1, you can upload data to the blob storage of storage1.	<input type="radio"/>	<input type="radio"/>
From VM2, you can upload data to the blob storage of storage1.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
From VM2, you can create a container in storage1.	<input type="radio"/>	<input checked="" type="radio"/>
From VM1, you can upload data to the blob storage of storage1.	<input checked="" type="radio"/>	<input type="radio"/>
From VM2, you can upload data to the blob storage of storage1.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Statements	Yes	No
From VM2, you can create a container in storage1.	<input type="radio"/>	<input checked="" type="radio"/>
From VM1, you can upload data to the blob storage of storage1.	<input checked="" type="radio"/>	<input type="radio"/>
From VM2, you can upload data to the blob storage of storage1.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION: 59

storage1

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

Azure □□□ □□: User1 -28681041@ExamUsers.com

Azure □□□□: GpOAe4@IDg

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>

AZ-500-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ AZ-500-KR □□! DumpTop □ □□ **AZ-500-KR** □□ □□□ □□□□□□, DumpTop AZ-500-KR □□ □□□ □□□□□□
□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop AZ-500-KR □□□ □□□□□. <https://www.dumptop.com/Microsoft/AZ-500-KR-dump.html> (517 Q&As Dumps, **30%OFF**
Special Discount: KrDump)

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 is an Azure subscription with a management group named MG1. Sub1 contains the following resources:

Sub1 contains the following resources:

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: <ul style="list-style-type: none">• Source: Any• Source port ranges: *• Destination: Any• Destination port ranges: *• Action: Allow• Priority: 500



Sub1 contains the following resources:

* Management scope: MG1

* Network groups:

o Name: Group1

Group members: VNet1

* Security admin configuration:

o Name: SAT

o Rule collections:

Name: SACollection1

Target network groups: Group1

Security admin rules:

Name: SARule1

Priority: 500

Action: Deny

Direction: Inbound

Source type: Any

Source port *

SA1 is deployed to all Azure regions.

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

* Management scope: Sub1

* Network groups:

o Name: Group2

Group members: VNet1

* Security admin configuration:

o Name: SA2

o Rule collections:

Name: SACollection2
 # Target network groups: Group2
 # Security admin rules:
 # Name: SARule2
 # Priority: 500
 # Action: Always allow
 # Direction: Inbound
 # Source type: Any
 # Source port: *

SA2 is an Azure Security Rule.
 SA2 is associated with the public IP address of VM1.
 SA2: 100 10000.

Statements	Yes	No
If you change Priority for NSGRule1 to 100 , NSG1 will be processed before SA1 and SA2.	<input type="radio"/>	<input type="radio"/>
Internet traffic is blocked to the public IP address of VM1.	<input type="radio"/>	<input type="radio"/>
If you change Action for SARule1 to Allow , internet traffic to the public IP address of VM1 will be enabled automatically.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
If you change Priority for NSGRule1 to 100 , NSG1 will be processed before SA1 and SA2.	<input type="radio"/>	<input checked="" type="radio"/>
Internet traffic is blocked to the public IP address of VM1.	<input type="radio"/>	<input checked="" type="radio"/>
If you change Action for SARule1 to Allow , internet traffic to the public IP address of VM1 will be enabled automatically.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Answer Area



Statements

If you change Priority for NSGRule1 to **100**, NSG1 will be processed before SA1 and SA2.

Yes

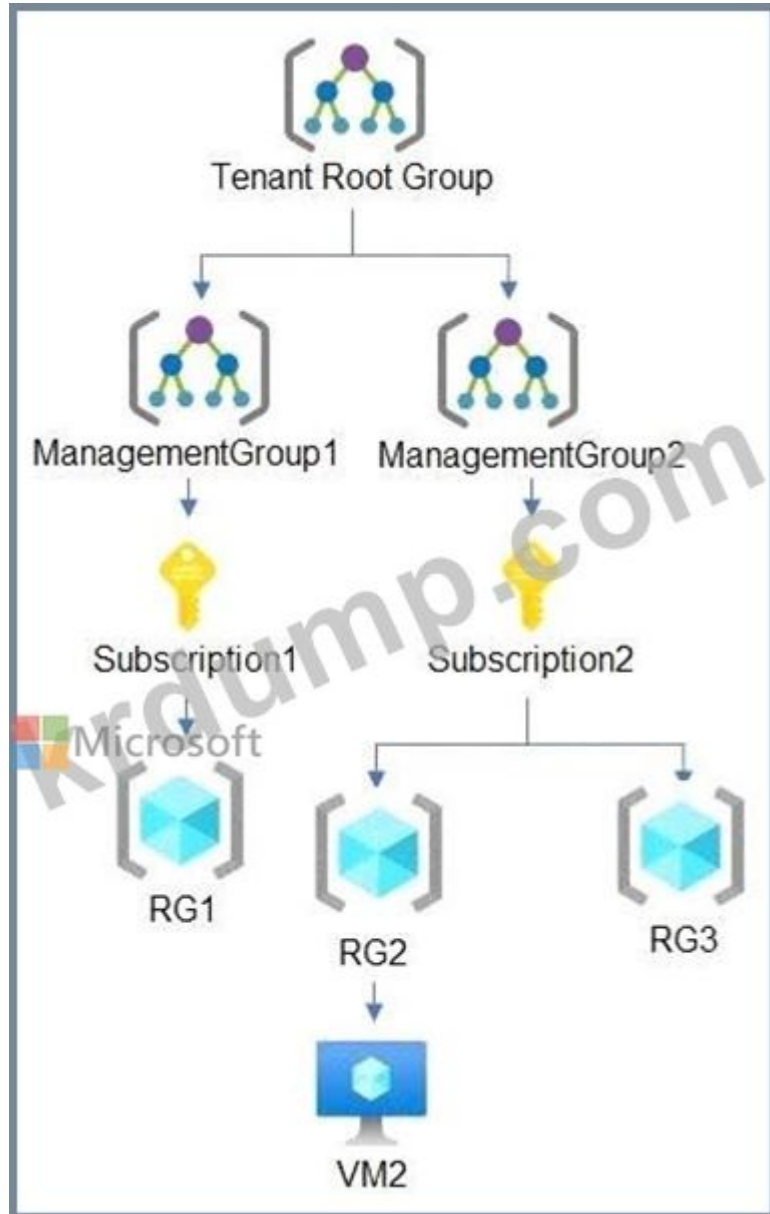
No

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 □□□ □□ □□□ □□□□ □□□□.

Which of the following statements are true regarding RBAC permissions?

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

Which of the following statements are true regarding RBAC permissions?
 Select all that apply.
 100 100000.

Statements	Yes	No
User1 can deploy virtual machines to RG1.	<input type="radio"/>	<input type="radio"/>
User2 can delete VM2.	<input type="radio"/>	<input type="radio"/>
User3 can reset the password of the built-in Administrator account of VM2.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 can deploy virtual machines to RG1.	<input type="radio"/>	<input type="radio"/>
User2 can delete VM2.	<input type="radio"/>	<input type="radio"/>
User3 can reset the password of the built-in Administrator account of VM2.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Statements	Yes	No
User1 can deploy virtual machines to RG1.	<input type="radio"/>	<input type="radio"/>
User2 can delete VM2.	<input type="radio"/>	<input type="radio"/>
User3 can reset the password of the built-in Administrator account of VM2.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION: 66

Which of the following Azure resource providers are supported?

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

Which of the following Azure resource providers are supported?
 Select all that apply.

Which of the following service endpoint policies can be used to access the storage1 and WebApp1 endpoints?
Options: VM1, storage1, and WebApp1 only.

Microsoft
Can be accessed by using a service endpoint: storage1 and WebApp1 only

- storage1 and WebApp1 only
- VM1 and storage1 only
- VM1 and WebApp1 only
- VM1, storage1, and WebApp1 only

Support service endpoint policies: storage1 only

- storage1 only
- VM1 only
- WebApp1 only
- VM1 and storage1 only
- Storage1 and WebApp1 only

Answer:
Answer Area

Microsoft
Can be accessed by using a service endpoint: storage1 and WebApp1 only

- storage1 and WebApp1 only
- VM1 and storage1 only
- VM1 and WebApp1 only
- VM1, storage1, and WebApp1 only

Support service endpoint policies: storage1 only

- storage1 only
- VM1 only
- WebApp1 only
- VM1 and storage1 only
- Storage1 and WebApp1 only

Explanation:

Microsoft
Can be accessed by using a service endpoint: storage1 and WebApp1 only

Support service endpoint policies: storage1 only

NEW QUESTION: 67

Microsoft Sentinel uses the Common Event Format (CEF) to ingest data from various sources. Which of the following is a valid CEF header?
Options: 100 100000.

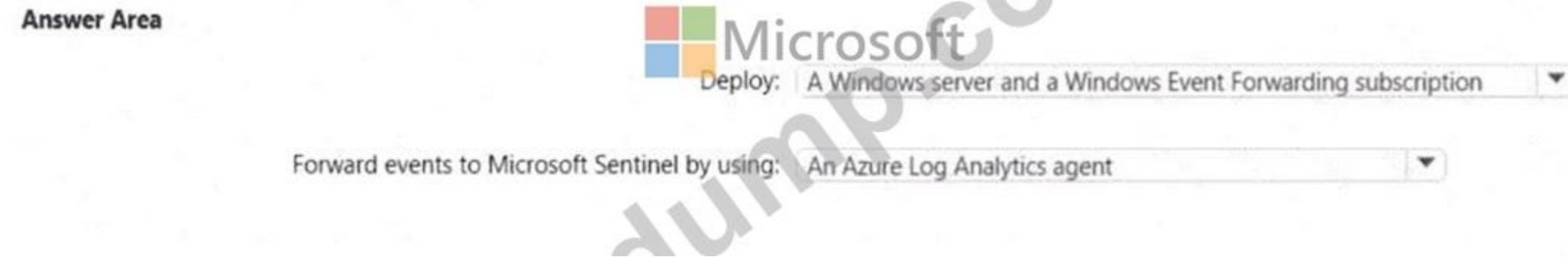


Answer:

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 2012R2	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: A, B, C


The screenshot shows the Microsoft Azure portal interface. On the left, there is a large watermark 'krdump.com'. In the center, the Microsoft logo is visible. On the right, there are two dropdown menus for selecting VMs. The top dropdown is labeled 'Windows:' and has a list of options: 'VM1 only', 'VM3 only', 'VM1 and VM2 only', 'VM1 and VM3 only', and 'VM1, VM2 and VM3'. The 'VM1 only' option is selected and highlighted in blue. The bottom dropdown is labeled 'Linux:' and has a list of options: 'VM4, VM5 and VM6', 'VM5 only', 'VM6 only', 'VM4 and VM6 only', 'VM5 and VM6 only', and 'VM4, VM5 and VM6'. The 'VM4, VM5 and VM6' option is selected and highlighted in blue.

Answer:

Actions

- ⋮ Add a managed certificate.
- ⋮ Configure the Inbound traffic configuration settings and the Outbound traffic configuration settings.
- ⋮ Add a custom domain to WebApp1.
- ⋮ Add a public key certificate (.cer).
- ⋮ Change the App Service plan to Basic.
- ⋮ Change the App Service plan to Shared.
- ⋮ Add a deployment slot to WebApp1.

Answer Area



Microsoft


Answer:

Actions

- ⋮ Add a managed certificate.
- ⋮ Configure the Inbound traffic configuration settings and the Outbound traffic configuration settings.
- ⋮ Add a custom domain to WebApp1.
- ⋮ Add a public key certificate (.cer).
- ⋮ Change the App Service plan to Basic.
- ⋮ Change the App Service plan to Shared.
- ⋮ Add a deployment slot to WebApp1.

Answer Area

- ⋮ Change the App Service plan to Basic.
- ⋮ Change the App Service plan to Shared.
- ⋮ Add a deployment slot to WebApp1.



Microsoft

Explanation:

Actions



Microsoft

- ⋮ Add a managed certificate.
- ⋮ Configure the Inbound traffic configuration settings and the Outbound traffic configuration settings.
- ⋮ Add a custom domain to WebApp1.
- ⋮ Add a public key certificate (.cer).

Answer Area

- 1 ⋮ Change the App Service plan to Basic.
- 2 ⋮ Change the App Service plan to Shared.
- 3 ⋮ Add a deployment slot to WebApp1.

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 □□□ □□: User1 -28681041@ExamUsers.com

Azure □□□□: GpOAe4@IDg

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>

Answer Area		
Statements	Yes	No
Connections from VM1 to storage1 always use IP address 10.1.1.5.	<input type="radio"/>	<input type="radio"/>
Connections from VM2 to Vault1 always use IP address 20.224.219.230.	<input type="radio"/>	<input type="radio"/>
Authentication from VM3 to the tenant uses either IP address 10.11.1.5 or 40.122.155.212.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area		
Statements	Yes	No
Connections from VM1 to storage1 always use IP address 10.1.1.5.	<input checked="" type="radio"/>	<input type="radio"/>
Connections from VM2 to Vault1 always use IP address 20.224.219.230.	<input type="radio"/>	<input checked="" type="radio"/>
Authentication from VM3 to the tenant uses either IP address 10.11.1.5 or 40.122.155.212.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

ANSWER AREA		
Statements	Yes	No
Connections from VM1 to storage1 always use IP address 10.1.1.5.	<input type="radio"/>	<input checked="" type="radio"/>
Connections from VM2 to Vault1 always use IP address 20.224.219.230.	<input type="radio"/>	<input checked="" type="radio"/>
Authentication from VM3 to the tenant uses either IP address 10.11.1.5 or 40.122.155.212.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION: 79

You are configuring a new Azure Kubernetes Service (AKS) cluster. You need to ensure that the cluster can connect to the Azure Key Vault service. What should you do?

A. Enable the Azure Key Vault service on the AKS cluster.

B. Configure the AKS cluster to use the Azure Key Vault service.

C. Configure the AKS cluster to use the Azure Key Vault service.

D. Configure the AKS cluster to use the Azure Key Vault service.

Actions

- Deploy an AKS cluster.
- Create a client application.
- Create a server application.
- Create an RBAC binding.
- Create a custom RBAC role.

Answer Area

Microsoft

-
-
-
-
-

Answer:

Actions

- Deploy an AKS cluster.
- Create a client application.
- Create a server application.
- Create an RBAC binding.
- Create a custom RBAC role.

Answer Area

Microsoft

- Create a server application.
- Create a client application.
- Deploy an AKS cluster.
- Create an RBAC binding.
-

Explanation:



Scenario: Azure AD users must be able 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](#).

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

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](#).

00 0 000 00, 000 000 '0'0 00000. 000 000 '000'0 00000.
00: 00 100 10000.

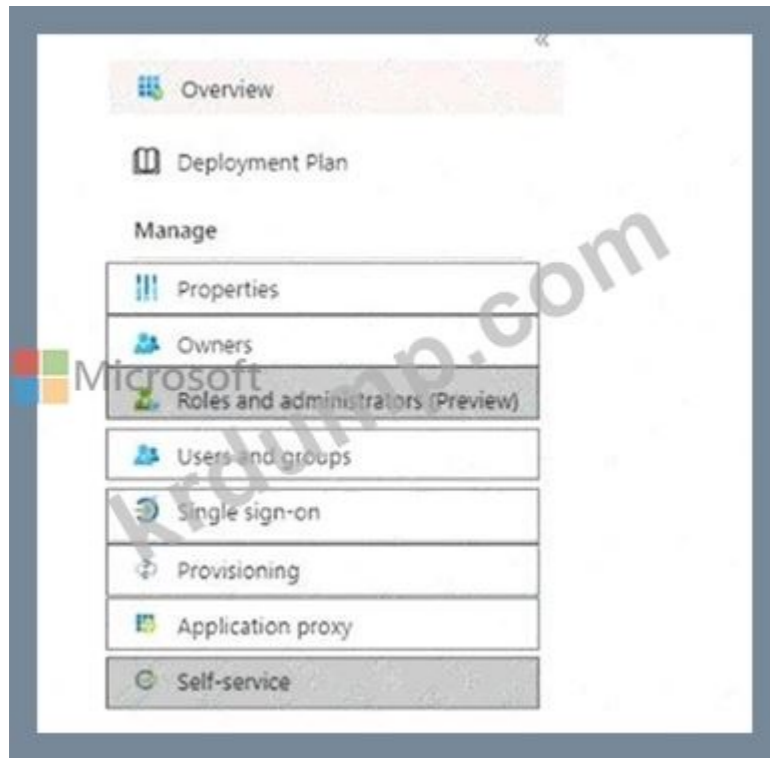


Answer:



Explanation:

Graphical user interface, application Description automatically generated



NEW QUESTION: 82

contoso.onmicrosoft.com is an Azure Active Directory (Azure AD) tenant.

Admin1 is a user in the tenant.

user1@outlook.com is a user in the Microsoft tenant.

Admin1 is assigned the Azure AD role of "user1@outlook.com" in the tenant. Admin1 is assigned the Azure AD role of "user1@outlook.com" in the tenant. Admin1 is assigned the Azure AD role of "user1@outlook.com" in the tenant. Admin1 is assigned the Azure AD role of "user1@outlook.com" in the tenant.

- A. Admin1 is assigned the role of "user1@outlook.com" in the tenant.
- B. Admin1 is assigned the role of "user1@outlook.com" in the tenant.
- C. Admin1 is assigned the role of "user1@outlook.com" in the tenant.
- D. Admin1 is assigned the role of "user1@outlook.com" in the tenant.

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 83

Microsoft 365 E5 is licensed.

Microsoft Defender for Cloud is installed on Azure servers.

Microsoft Defender for Cloud is installed on Azure servers.

Microsoft Defender for Cloud is installed on Azure servers.

Microsoft Defender for Cloud is installed on Azure servers.

- A. Server2
- B. Server2 Server3
- C. Server3
- D. Server1

E. 001, 002, 003

F. 0010 003

Answer: (SHOW ANSWER)

NEW QUESTION: 84

00 00 000 000 00 000 000 Azure 000 0000.

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

Azure Portal 00 000 0000 0 000 00 000 00 000000. 0 000 00 00 00 000000.

Name	Type
Role3	Azure AD
Role4	Azure subscription

00 000 0000 000 000 00 0 000? 000000 00 0000 000 000 000000.

00: 00 100 10000.

Role3:

- Role1 only
- Built-in Azure AD roles only
- Role1 and built-in Azure AD roles only
- Role1, built-in Azure AD roles, and built-in Azure subscription roles

Role4:

- Role2 only
- Built-in Azure AD roles only
- Role2 and built-in Azure subscription roles only
- Role2, built-in Azure subscription roles, and built-in Azure AD roles

Answer:

Role3:

- Role1 only
- Built-in Azure AD roles only
- Role1 and built-in Azure AD roles only
- Role1, built-in Azure AD roles, and built-in Azure subscription roles

Role4:

- Role2 only
- Built-in Azure AD roles only
- Role2 and built-in Azure subscription roles only
- Role2, built-in Azure subscription roles, and built-in Azure AD roles

Explanation:

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

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

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



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□ □□ □□ □□□ □□ □□□ □□□□□.

Total number of Microsoft Defender for Cloud email notifications about an RDP brute force attack on Tuesday:

4

1

2

3

4

7

3

4

7

9

11



Total number of Microsoft Defender for Cloud email notifications on Tuesday:

Explanation:

Answer Area

Total number of Microsoft Defender for Cloud email notifications about an RDP brute force attack on Tuesday: 4

Total number of Microsoft Defender for Cloud email notifications on Tuesday: 7



NEW QUESTION: 88

App1 Azure App Service

Virtual Network Integration

ASP-demoapp8789577567336group-84d2

App Service Plan	ASP-demoapp8789577567336group-84d2
App Service Plan Location	East US
Regional VNet integrations	1/2
Gateway required VNet integrations	0/5
VNet NAME ↑	GATEWAY STATUS ↑↓
vnet1/subnet2	N/A


2 VM1

100

Answer Area

To deny outbound access, configure [answer choice] on Subnet2.

To connect to a virtual network in a different region, configure [answer choice].



a network security group (NSG)
 a network security group (NSG)
 a service endpoint
 an application security group


Gateway-required VNet integrations
 an Azure NAT Gateway integration
 Gateway-required VNet integrations
 Regional VNet integrations

Answer:

Answer Area

To deny outbound access, configure [answer choice] on Subnet2.

To connect to a virtual network in a different region, configure [answer choice].



a network security group (NSG)
 a network security group (NSG)
 a service endpoint
 an application security group

Gateway-required VNet integrations
 an Azure NAT Gateway integration
 Gateway-required VNet integrations
 Regional VNet integrations

Explanation:

Answer Area



To deny outbound access, configure [answer choice] on Subnet2. a network security group (NSG)

To connect to a virtual network in a different region, configure [answer choice]. Gateway-required VNet integrations

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 is an Azure Key Vault. You need to ensure that the application can access the secrets in Vault1. The application is running on an Azure VM. The application needs to access the secrets in Vault1. What should you do?

- A. Azure AD. Add the application as a user in Azure AD.
- B. Azure Key Vault. Add the application as a secret in Azure Key Vault.
- C. Azure Key Vault. Add the application as a secret in Azure Key Vault.
- D. Azure AD. Add the application as a user in 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 Resource Manager (ARM) templates are used to create and manage Azure resources. You have an ARM template that defines a storage account. The storage account is named storage1. The storage account is located in the resource group RG1. The storage account is created with the role assignments shown in the following table. What is the result of the role assignments?

```

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

```

Role2 is assigned to the storage account. What is the result of the role assignments?

Name	Role
User1	Role1
User2	Role2
User3	Role1, Role2

What is the result of the role assignments? Select the correct answer.

Role1: User1, User2, User3. Role2: User2, User3.

App registrations

Users can register applications ⓘ



App1 is registered in the tenant.

User1 is assigned the Azure AD App1 role. The role is assigned to the user.

User1 is assigned the role. What is the result?

- A. User1 can register applications.
- B. User1 can register applications in the tenant.
- C. Azure AD App1 role is assigned to the user.
- D. Azure AD App1 role is not assigned to the user.

Answer: D ([LEAVE A REPLY](#))

Reference:

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

NEW QUESTION: 93

Azure AD is used to manage the identities of users and devices.

Users can be assigned roles in Azure AD. What is the result of assigning a role?

Users can be assigned roles in Azure AD. What is the result of assigning a role?

Users can be assigned roles in Azure AD. What is the result of assigning a role?

- A. Azure AD role is assigned to the user.
- B. Azure AD role is not assigned to the user.
- C. Azure AD role is assigned to the user.
- D. Azure AD role is not assigned to the user.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 94

Company1 has an Azure AD tenant named company1.com. The tenant is connected to an on-premises Active Directory forest named company1.com. The tenant is connected to an on-premises Active Directory forest named company1.com.

Company1 has an Azure AD tenant named company1.com. The tenant is connected to an on-premises Active Directory forest named company1.com. The tenant is connected to an on-premises Active Directory forest named company1.com.

Company1 has an Azure AD tenant named company1.com. The tenant is connected to an on-premises Active Directory forest named company1.com. The tenant is connected to an on-premises Active Directory forest named company1.com.

- A. The tenant is connected to an on-premises Active Directory forest named company1.com.
- B. The tenant is connected to an on-premises Active Directory forest named company1.com.
- C. The tenant is connected to an on-premises Active Directory forest named company1.com.
- D. Active Directory is connected to the tenant.

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

Q: Which of the following is a feature of Microsoft Antimalware on Windows Server 2012 R2? (Select two.)

A. It is installed as a feature.

B. It is installed as an extension.

C. It is installed as a service.

D. It is installed as a role.

- 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

Q: You are configuring storage1 for an Azure Storage VM1. Which of the following actions should you perform? (Select three.)


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

Answer Area



Answer:


Actions	Answer Area
Run the <code>Set-AzVMDiskEncryptionExtension</code> cmdlet.	Create an Azure key vault.
Set the Key Vault access policy to Enable access to Azure Virtual Machines for deployment .	Set the Key Vault access policy to Enable access to Azure Disk Encryption for volume encryption .
Set the Key Vault access policy to Enable access to Azure Disk Encryption for volume encryption .	Run the <code>Set-AzVMDiskEncryptionExtension</code> cmdlet.
Generate a key vault certificate.	
Create an Azure key vault.	
Configure storage1 to use a customer-managed key.	



Explanation:

Graphical user interface, text, application Description automatically generated

Create an Azure key vault.
Set the Key Vault access policy to Enable access to Azure Disk Encryption for volume encryption .
Run the <code>Set-AzVMDiskEncryptionExtension</code> cmdlet.



Reference:

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

NEW QUESTION: 97

Sub1 Azure Application Insights WebApp1 Azure OAuth 2.0

Sub1 Azure Application Insights WebApp1 Azure OAuth 2.0

Sub1 Azure Application Insights WebApp1 Azure OAuth 2.0

Sub1 Azure Application Insights WebApp1 Azure OAuth 2.0

Sub1 Azure Application Insights WebApp1 Azure OAuth 2.0

Sub1 Azure Application Insights WebApp1 Azure OAuth 2.0

Sub1 Azure Application Insights WebApp1 Azure OAuth 2.0

Sub1 Azure Application Insights WebApp1 Azure OAuth 2.0

Sub1 Azure Application Insights WebApp1 Azure OAuth 2.0

- A. Microsoft Visual Studio .webtest Application Insights
- B. .webtest Application Insights
- C. Azure AD

- D.
- E.
- F.

Answer: F (LEAVE A REPLY)

NEW QUESTION: 101

SQL11 is an Azure SQL Managed Instance. You need to configure auditing for SQL11. The audit log destination must be storage1. The audit log must include all database events. Which two actions should you perform? (Select two.)

- * :
- * : storage1

Azure SQL Managed Instance is a fully managed database service that provides the same SQL Server engine as on-premises but with the benefits of cloud. It is designed to be a drop-in replacement for on-premises SQL Server.

Answer Area

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

Answer:
Answer Area

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

Explanation:

Answer Area

Audit events for DB1 are written to storage1.	<input checked="" type="radio"/>	<input type="radio"/>
Audit events for DB2 are written to storage1 and storage2.	<input checked="" type="radio"/>	<input type="radio"/>
Storage3 can be used as an audit log destination for DB3.	<input type="radio"/>	<input checked="" type="radio"/>

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 is a managed network security service. AzFW1 is an Azure Firewall Standard instance. You need to configure AzFW1 to protect the network. Which three actions should you perform? (Select three.)

- * TLS
- *
- * (IDPS)

Which of the following is a security protocol?

- A. TLS
- B. IDPS
- C. IDPS
- D. TLS, IDPS
- E. IDPS

Answer: A (LEAVE A REPLY)

NEW QUESTION: 103

You are configuring a new Azure Active Directory (Azure AD) tenant. You need to ensure that the tenant can connect to an on-premises Active Directory (AD) forest. Which of the following is a requirement for connecting to an on-premises AD forest?

Options:

- A. The on-premises AD forest must be running Windows Server 2012 R2 or later.
- B. The on-premises AD forest must be running Windows Server 2008 R2 or later.
- C. The on-premises AD forest must be running Windows Server 2008 or later.
- D. The on-premises AD forest must be running Windows Server 2003 or later.

- A. A
- B. B

Answer: A (LEAVE A REPLY)

NEW QUESTION: 104

You are configuring a new Azure Active Directory (Azure AD) tenant. You need to ensure that the tenant can connect to an on-premises Active Directory (AD) forest. Which of the following is a requirement for connecting to an on-premises AD forest?

Options:

- A. The on-premises AD forest must be running Windows Server 2012 R2 or later.
- B. The on-premises AD forest must be running Windows Server 2008 R2 or later.
- C. The on-premises AD forest must be running Windows Server 2008 or later.
- D. The on-premises AD forest must be running Windows Server 2003 or later.

Azure AD Connect: User1 -28681041@ExamUsers.com
Azure AD Connect: GpOAe4@IDg
Azure Portal: CTRL-K
Azure AD Connect: 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

VM1, VM2, VM3, and VM4 are virtual machines in an Azure subscription. The configuration is as follows:

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

VM1, VM2, VM3, and VM4 are connected to VNET1.

Azure Bastion is connected to VNET2.

Which virtual machines can be accessed from Azure Bastion?

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

Answer: A (LEAVE A REPLY)

<https://docs.microsoft.com/en-us/azure/bastion/vnet-peering>

NEW QUESTION: 106

App1 is an application in an Azure subscription. App1 uses the Microsoft Graph API to access user calendars. The configuration is as follows:

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

App1 is configured to use the Microsoft Graph API to access user calendars. Which permissions are required for App1 to access user calendars?

- A. Microsoft.Graph Calendars.ReadWrite and Microsoft.Graph User.Read
- B. Microsoft.Graph Calendars.ReadWrite and Microsoft.Graph Calendars.Read
- C. Microsoft.Graph Calendars.Read
- D. Microsoft.Graph Calendars.ReadWrite.Shared and Microsoft.Graph User.Read

Answer: A (LEAVE A REPLY)

Reference:

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

AZ-500-KR ... DumpTop ... AZ-500-KR ... DumpTop AZ-500-KR ... <https://www.dumptop.com/Microsoft/AZ-500-KR-dump.html> (517 Q&As Dumps, 30%OFF

Special Discount: KrDump)

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 ...

Operating systems:

- SLES only
- Windows Server only
- SLES and Windows Server



Platforms:

- Azure virtual machines only
- Azure virtual machines and Hyper-V virtual machines only
- Azure Arc-enabled servers and Azure virtual machines only
- Azure virtual machines, Hyper-V virtual machines, and Azure Arc-enabled servers

Answer:

Operating systems:

- SLES only
- Windows Server only
- SLES and Windows Server

Platforms:

- Azure virtual machines only
- Azure virtual machines and Hyper-V virtual machines only
- Azure Arc-enabled servers and Azure virtual machines only
- Azure virtual machines, Hyper-V virtual machines, and Azure Arc-enabled servers

NEW QUESTION: 109

Microsoft Defender for Cloud is a cloud-native security solution that provides comprehensive protection for your Azure resources. It offers a unified view of your security posture, including alerts, recommendations, and incident response capabilities. Defender for Cloud is designed to help you identify and remediate security risks across your Azure environment, ensuring your data and applications are protected from threats. It integrates with other Microsoft security products, such as Microsoft Defender for Endpoint and Microsoft Defender for Office 365, to provide a holistic security strategy. Defender for Cloud is available as a managed service, so you can focus on your core business while Microsoft handles the security management. For more information, visit the Microsoft Defender for Cloud documentation.

Settings | Continuous export

Visual Studio Enterprise Subscription

Save

Continuous export

Configure streaming export setting of Defender for Cloud data to multiple export targets. Exporting Defender for Cloud's data also enables you to use experiences such as integration with 3rd-party SIEM and Azure Data Explorer. [Learn More >](#)

Event hub Log Analytics workspace

Export enabled On Off

Exported data types

<input type="checkbox"/> Security recommendations	No selected recommendation
<input checked="" type="checkbox"/> Secure score ⓘ	Overall score.Control score
Controls	All controls selected
<input type="checkbox"/> Security alerts	No selected severities
<input type="checkbox"/> Regulatory compliance	No selected standards

Export frequency

<input checked="" type="checkbox"/> Streaming updates ⓘ
<input type="checkbox"/> Snapshots (Preview) ⓘ

Answer:

Settings | Continuous export

Visual Studio Enterprise Subscription

Save

Continuous export

Configure streaming export setting of Defender for Cloud data to multiple export targets. Exporting Defender for Cloud's data also enables you to use experiences such as integration with 3rd-party SIEM and Azure Data Explorer. [Learn More >](#)

Event hub Log Analytics workspace

Export enabled On Off

Exported data types

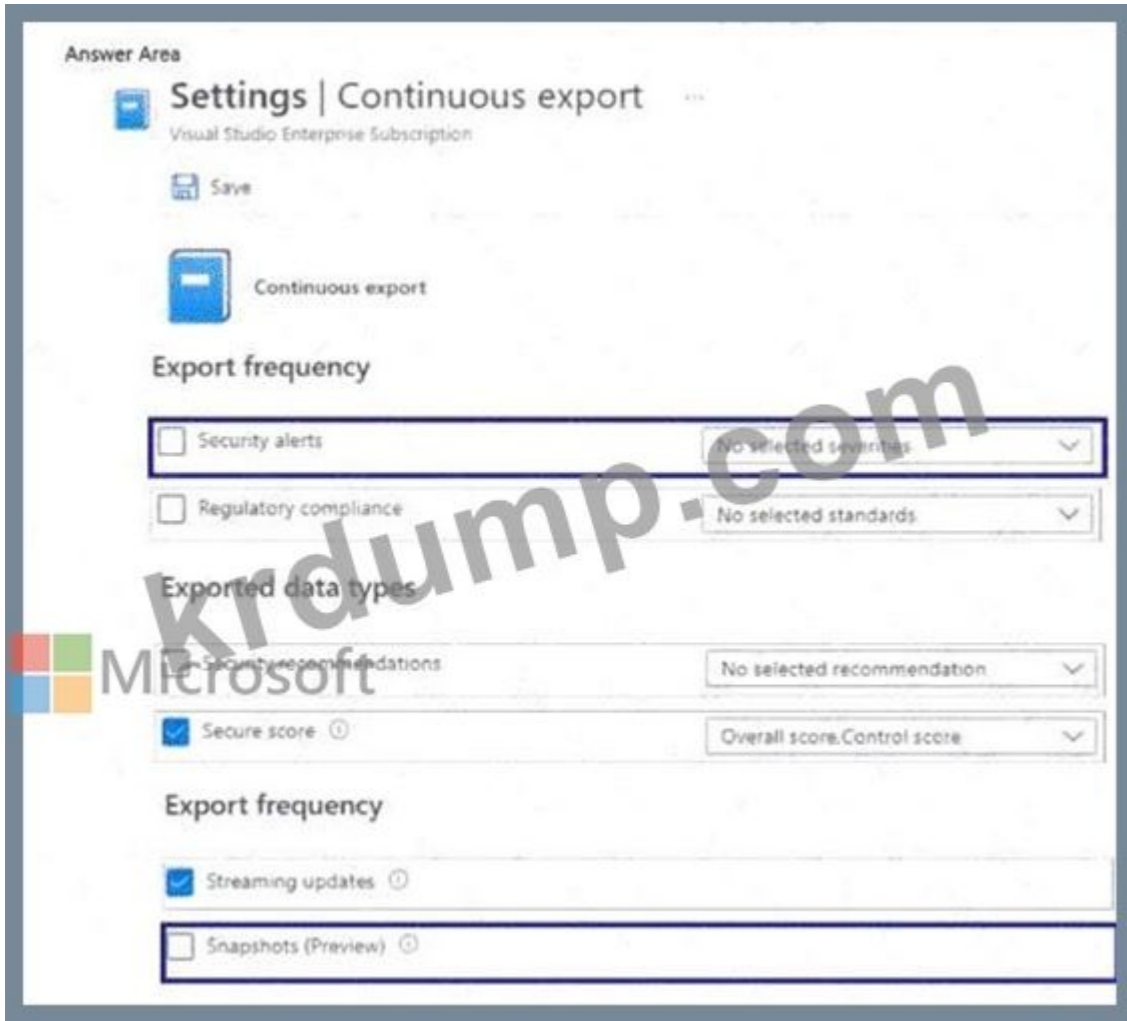
<input type="checkbox"/> Security recommendations	No selected recommendation
<input checked="" type="checkbox"/> Secure score ⓘ	Overall score, Control score
Controls	All controls selected
<input type="checkbox"/> Security alerts	No selected severities
<input type="checkbox"/> Regulatory compliance	No selected standards

Export frequency

<input checked="" type="checkbox"/> Streaming updates ⓘ
<input type="checkbox"/> Snapshots (Preview) ⓘ



Explanation:



NEW QUESTION: 110

Contoso.com is a Microsoft Entra ID tenant. The tenant contains the following users:

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

The tenant contains the following applications:

Name	Owner	Users and groups
App1	User3	User4
App2	User4	User3

App1 and App2 are registered in the tenant. The tenant contains the following groups:

Answer Area

App1:

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

App2:

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

Answer:

Answer Area

App1:

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

App2:

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

Explanation:

Answer Area

App1:

App2:

NEW QUESTION: 111

Sub1 is an Azure virtual network. Sub1 has VNet1 with two subnets, Subnet1 and Subnet2.

Subnet1 has an Ubuntu Server 20.04 VM1. VM1 is connected to Subnet1.

Microsoft Docker is installed on VM1. Subnet1 has a storage account.

Docker is configured to connect to the storage account. Azure Storage is used to store Docker images.

VM1 is unable to pull Docker images from the storage account.

- A. The storage account is not configured for CNI.
- B. The storage account is not configured for NSG.
- C. docker-compose.yml is not configured.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 112

Sub1 is an Azure virtual network.

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	VNET3/Subnet1	NSG4

VNET1, VNET2, VNET3 are all in the same region. VM1, VM2, VM3, and VM4 are all in the same region.

* VM1, VM2, VM3, and VM4 are all connected to the same VNET.

* VM1 is connected to VNET1, VM2 to VNET1, VM3 to VNET2, and VM4 to VNET3.

Answer Area

Microsoft

ASG1:

ASG2:

Answer:

see the answer below in explanation.

Explanation:

Answer as below.

Answer Area

Microsoft

ASG1:

ASG2:

NEW QUESTION: 113

contoso.com is an Azure Active Directory (Azure AD) tenant. Sub1 is an Azure AD group.

Azure Security Center is configured to monitor the security of the Azure AD tenant.

Which of the following is a built-in sensitive information type?

A. Microsoft Cloud App Security

B. Azure AD

C. Azure AD Connect

D. Microsoft Cloud App Security

E. 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:

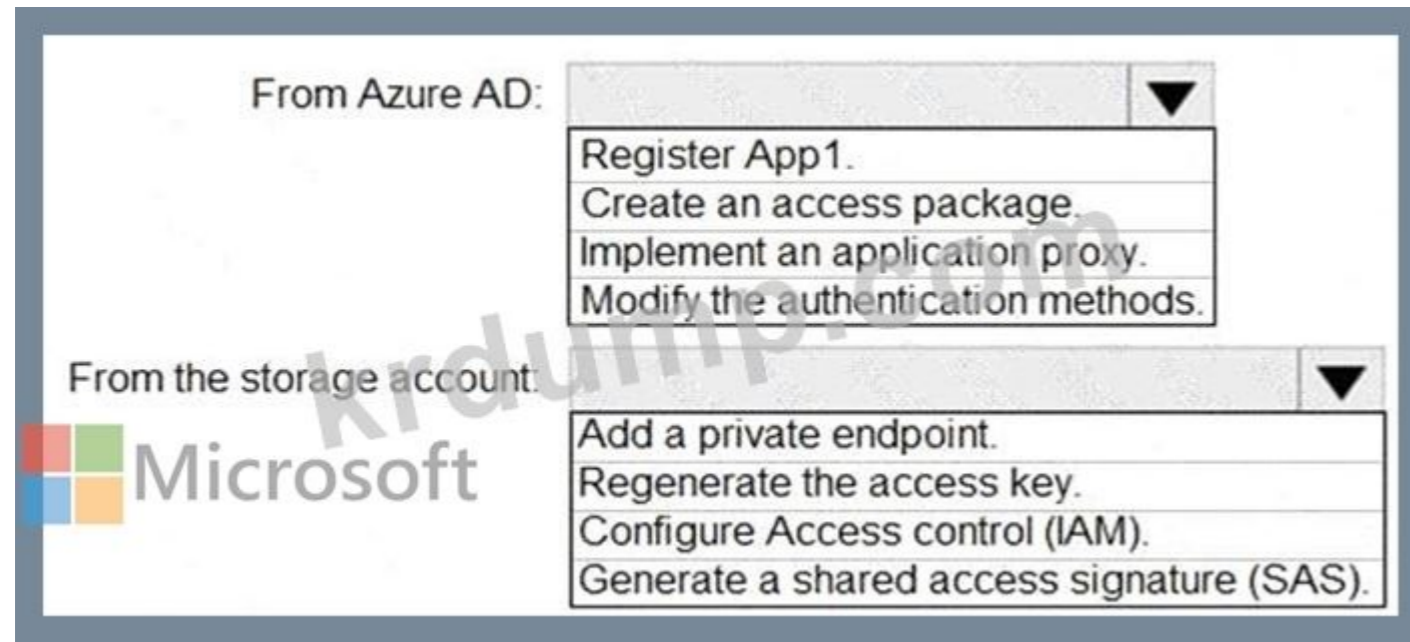
<https://docs.microsoft.com/en-us/office365/securitycompliance/customize-a-built-in-sensitive-information-type>

NEW QUESTION: 114

container1 is a storage container in Blob storage. App1 is an application that stores data in Azure Storage.

Azure Active Directory (Azure AD) is configured to use App1 as a federated identity provider for container1.

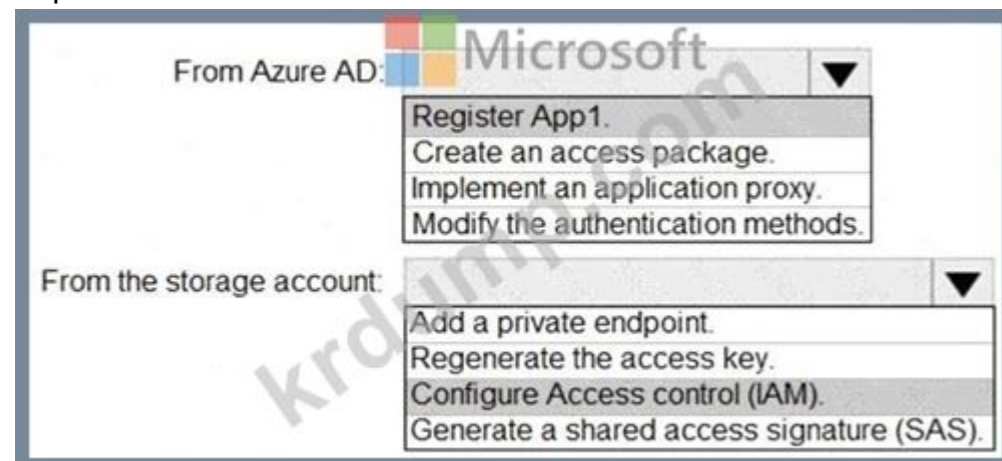
□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□□□ □□□□□.
□□: □□ 1□□ 1□□□□.



Answer:



Explanation:



Reference:

<https://azure.microsoft.com/en-in/blog/announcing-the-preview-of-aad-authentication-for-storage/>

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

Azure □□□ □□: User1 -28681041@ExamUsers.com

Azure □□□□: GpOAe4@IDg

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 □□□ □□□□.

□□□□□ □□□□ □-□□□□ □□□ 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



The custom role grants a user permission to delete Azure SQL Database resources.

Yes

No

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

The custom role grants a user permission to delete Azure SQL Database resources.

Yes

No

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:

The screenshot shows the 'Answer Area' with the following correct selections:

- Statement 1: The custom role grants a user permission to delete Azure SQL Database resources. **Yes** (selected).
- Statement 2: The custom role grants a user permission to manage the Microsoft Entra admin settings for an Azure SQL Database server. **No** (selected).
- Statement 3: The custom role grants a user permission to reset the administrator password for instances of Azure Database for MariaDB. **No** (selected).

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□ □□□□ □ □□□ □□□□ □□□.

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

Actions

Answer Area

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

Answer:

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

Explanation:

- Implement Azure AD Connect.
- Enable Active Directory Domain Services (AD DS) authentication on storage1.
- Assign share-level permissions for share1.

Reference:

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

□□□ □□ □□□□ rle □□□□ 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 Area

Statements	Yes	No
You can start VM1.	<input type="radio"/>	<input type="radio"/>
You can start VM2.	<input type="radio"/>	<input type="radio"/>
You can create a virtual machine in RG2.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
You can start VM1.	<input type="radio"/>	<input checked="" type="radio"/>
You can start VM2.	<input checked="" type="radio"/>	<input type="radio"/>
You can create a virtual machine in RG2.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Answer Area

Statements	Yes	No
You can start VM1.	<input type="radio"/>	<input checked="" type="radio"/>
You can start VM2.	<input checked="" type="radio"/>	<input type="radio"/>
You can create a virtual machine in RG2.	<input type="radio"/>	<input type="radio"/>

References:

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

NEW QUESTION: 126

Sub2 is a virtual network with the following configuration:

Sub2 has three subnets: Sub1 (10.0.0.0/24), Sub3 (10.0.1.0/24), and Sub4 (10.0.2.0/24).

Sub1 contains VM1 and VM2. Sub3 contains VM3. Sub4 contains VM5.

Answer Area

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

Answer:

Answer Area

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

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) is configured with the following roles and members.

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

Vault1 is an Azure Key Vault. The following permissions are assigned to the groups.

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


The following roles are assigned to the users.

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

Which of the following statements are true? Select all that apply.

Options: 1. User1 can set Purge protection to Enable for Vault1. 2. User2 can configure firewalls and virtual networks for Vault1. 3. User3 can add access policies to Vault1.

Answer Area



Statements	Yes	No
User1 can set Purge protection to Enable for Vault1.	<input type="radio"/>	<input type="radio"/>
User2 can configure firewalls and virtual networks for Vault1.	<input type="radio"/>	<input type="radio"/>
User3 can add access policies to Vault1.	<input type="radio"/>	<input type="radio"/>

Answer:


Answer Area



Statements	Yes	No
User1 can set Purge protection to Enable for Vault1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can configure firewalls and virtual networks for Vault1.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can add access policies to Vault1.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Answer Area



Statements	Yes	No
User1 can set Purge protection to Enable for Vault1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can configure firewalls and virtual networks for Vault1.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can add access policies to Vault1.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION: 128

Azure Key Vault is configured with the following roles and members.

Options: 1. User1 can set Purge protection to Enable for Vault1. 2. User2 can configure firewalls and virtual networks for Vault1. 3. User3 can add access policies to Vault1.

□□: □□ 1□□ 1□□□□.

```
New-AzureRmKeyVault -VaultName 'KeyVault1' -ResourceGroupName 'RG1'
```

```
-Location 'East US'
```

-EnabledForDeployment
-EnablePurgeProtection
-Tag

-Confirm
-DefaultProfile
-EnableSoftDelete
-SKU

Answer:

```
New-AzureRmKeyVault -VaultName 'KeyVault1' -ResourceGroupName 'RG1'
```

```
-Location 'East US'
```

-EnabledForDeployment
-EnablePurgeProtection
-Tag

-Confirm
-DefaultProfile
-EnableSoftDelete
-SKU

Explanation:

```
New-AzureRmKeyVault -VaultName 'KeyVault1' -ResourceGroupName 'RG1'
```

```
-Location 'East US'
```

-EnabledForDeployment
-EnablePurgeProtection
-Tag

-Confirm
-DefaultProfile
-EnableSoftDelete
-SKU

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

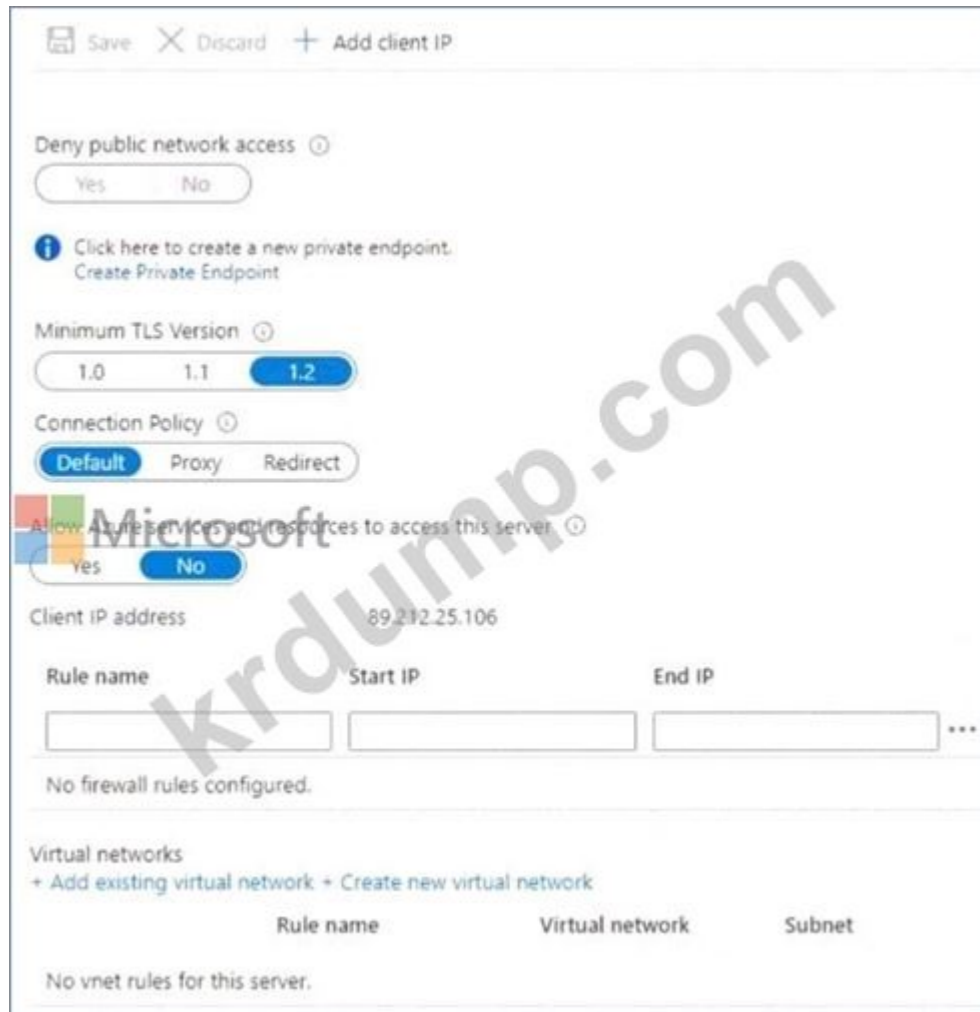
Specifies that the soft-delete functionality is enabled for this key vault. When soft-delete is enabled, for a grace period, you can recover this key vault and its contents after it is deleted.

References:

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

NEW QUESTION: 129

SQL1 is an Azure SQL Database VM1 is an Azure VM. VM1 IP is 89.212.25.106. SQL1 is in a virtual network. What is the best way to connect VM1 to SQL1?



VM1 SQL1 is in a virtual network. What is the best way to connect VM1 to SQL1?

- A. Create a firewall rule to allow traffic from VM1 to SQL1.
- B. Create a virtual network rule to allow traffic from VM1 to SQL1.
- C. Azure Firewall is required to connect VM1 to SQL1.
- D. Create a virtual network rule to allow traffic from VM1 to SQL1.

Answer: (SHOW ANSWER)

NEW QUESTION: 130

WAF1 is an Azure Application Gateway (WAF) in a virtual network. Bicep is used to create the resources. What is the best way to connect WAF1 to 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'
            negationCondition: true
            matchValues: [
              '10.10.10.0/24'
            ]
          }
        ]
      }
    ]
    policySettings: {
      requestBodyCheck: true
      maxRequestBodySizeInKb: 128
      state: 'Enabled'
      mode: 'Detection'
    }
    managedRules: {
      managedRuleSets: [
        {
          ruleSetType: 'OWASP'
          ruleSetVersion: '3.2'
        }
      ]
    }
  }
}
```

00 0 000 00, 000 00000 '0'0 00000. 000 000 '000'0 00000.
00: 00 100 10000.



Answer Area



Statements

	Yes	No
A request to the backend pool from IP address 10.1.1.5 is allowed.	<input type="radio"/>	<input type="radio"/>
Incoming requests attempting file path attacks are blocked.	<input type="radio"/>	<input type="radio"/>
WAF1 allows a 50-MB file to be uploaded.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements

	Yes	No
A request to the backend pool from IP address 10.1.1.5 is allowed.	<input type="radio"/>	<input checked="" type="radio"/>
Incoming requests attempting file path attacks are blocked.	<input checked="" type="radio"/>	<input type="radio"/>
WAF1 allows a 50-MB file to be uploaded.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Answer Area

Statements

	Yes	No
A request to the backend pool from IP address 10.1.1.5 is allowed.	<input type="radio"/>	<input checked="" type="radio"/>
Incoming requests attempting file path attacks are blocked.	<input checked="" type="radio"/>	<input type="radio"/>
WAF1 allows a 50-MB file to be uploaded.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION: 131

Microsoft Defender for Cloud is integrated with Azure Monitor. Which Azure Monitor component is used to collect and analyze logs from Microsoft Defender for Cloud? (Select two.)

- A. Azure Monitor Alerts
- B. Azure Monitor Diagnostics
- C. Azure Monitor Log Analytics
- D. Microsoft Defender

D. PostgreSQL Audit (pgAudit)

Answer: (SHOW ANSWER)

NEW QUESTION: 132

500 users are connected to AU1. You need to ensure that Azure AD Connect can connect to Azure Active Directory. What should you do?

- A. Configure the Connect To Cloud Directory option to (UPN)
- B. Configure the Connect To Cloud Directory option to
- C. Configure the UPN (User Principal Name) option to
- D. Configure the Connect To Cloud Directory option to
- E. Configure the Connect To Cloud Directory option to (UPN)

Answer: C (LEAVE A REPLY)

NEW QUESTION: 133

You have a virtual network (VNET) in Azure. The VNET has three subnets.

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 is connected to Subnet2. You need to ensure that VM1 can access storageacc1 in Azure Storage.

Allow access from
 All networks Selected networks

Configure network security for your storage accounts. [Learn more.](#)

Virtual networks

Secure your storage account with virtual networks. [+ Add existing virtual network](#)
[+ Add new virtual network](#)

VIRTUAL NETWORK	SUBNET	ADDRESS RANGE	ENDPOINT STATUS	RESOURCE GROUP	SUBSCRIPTION
-----------------	--------	---------------	-----------------	----------------	--------------

No network selected.



Firewall

Add IP ranges to allow access from the internet on your on-premises networks. [Learn more.](#)

Address Range

13.80.73.87

IP address or CIDR

Exceptions

- Allow trusted Microsoft services to access this storage account
- Allow read access to storage logging from any network

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

Statements	Yes	No
From VM1, you can upload a blob to storageacc1.	<input type="radio"/>	<input type="radio"/>
From VM2, you can upload a blob to storageacc1.	<input type="radio"/>	<input type="radio"/>
From VM3 , you can upload a blob to storageacc1.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
From VM1, you can upload a blob to storageacc1.	<input checked="" type="radio"/>	<input type="radio"/>
From VM2, you can upload a blob to storageacc1.	<input type="radio"/>	<input checked="" type="radio"/>
From VM3 , you can upload a blob to storageacc1.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Statements Yes No

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

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☐ ☐☐☐☐☐☐☐☐ ☐☐ ☐☐ ☐☐

☐☐ ☐☐☐☐ ☐☐, ☐☐☐☐☐☐☐☐ '☐'☐ ☐☐☐☐☐☐. ☐☐☐☐☐☐☐ '☐☐☐☐'☐☐☐☐☐☐.

☐☐: ☐☐ 10☐ 10☐☐☐☐.

Answer Area

	Yes	No
Statements		
WebApp2 can be integrated with Subnet11.	<input type="radio"/>	<input type="radio"/>
WebApp2 can be integrated with Subnet12.	<input type="radio"/>	<input type="radio"/>
WebApp2 can be integrated with Subnet21.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements

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

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	<i>Not applicable</i>	Locally-redundant storage (LRS)	Two Azure Files shares
storage2	Premium	Page blobs	Locally-redundant storage (LRS)	Three containers

☐☐☐ ☐☐☐ ☐☐ ☐☐ ☐☐☐☐ ☐☐ ☐☐☐☐ ☐☐☐☐☐☐ ☐☐☐☐ ☐☐☐. ☐☐☐☐ ☐☐☐☐ ☐☐☐☐☐☐ ☐☐☐☐ ☐☐ ☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐.

☐☐☐☐☐ ☐☐☐☐ ☐☐☐☐☐ ☐☐☐☐ ☐☐☐☐☐☐ ☐☐☐☐☐☐? ☐☐☐☐☐☐ ☐☐☐☐☐☐ ☐☐☐☐☐☐☐.

☐☐: ☐☐ 1☐☐ 1☐☐☐☐.

Answer Area

storage1:
 1
 2
 3
 6

storage2:
 1
 2
 3
 6
 8

☐☐

Answer:

Answer Area

storage1: ▼

- 1
- 2
- 3
- 6

storage2: ▼

- 1
- 2
- 3
- 6
- 8



Explanation:

Answer Area

storage1: ▼

storage2: ▼

NEW QUESTION: 144

Scenario: You are configuring an Azure Kubernetes Service (AKS) cluster. The cluster configuration includes the following storage settings:

storage1: 1
storage2: 1

AKS1 is an Azure Kubernetes Service (AKS) cluster. AZCR1 is an Azure Container Registry (ACR) instance. Azure Storage is configured with the following settings:

AKS1 is connected to AZCR1. The storage settings are as follows:

storage1: 1
storage2: 1

What is the result of this configuration?

A. The cluster can access the storage account.

B. The cluster cannot access the storage account.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 145

Scenario: You are configuring Microsoft Antimalware on a Windows Server. The configuration includes the following settings:

Microsoft Antimalware is installed. The configuration is as follows:

1. The Microsoft Antimalware service is set to start automatically.

Create a custom policy definition that has effect set to:

Create a policy assignment and modify:

Answer:

Create a custom policy definition that has effect set to:

Create a policy assignment and modify:

- Explanation:
1. DeployifNotExists
 2. Scope

NEW QUESTION: 146

AD DS(Active Directory Domain Services) is a Microsoft Windows Server service that provides a central location for storing user accounts, groups, computer accounts, and other objects. It is used to manage and secure network resources. Azure Active Directory (AAD) is a cloud-based identity and access management service that integrates with AD DS. AAD provides a secure and scalable way to manage user identities and access to cloud and on-premises resources. AAD is used to manage user identities and access to cloud and on-premises resources. AAD is used to manage user identities and access to cloud and on-premises resources.

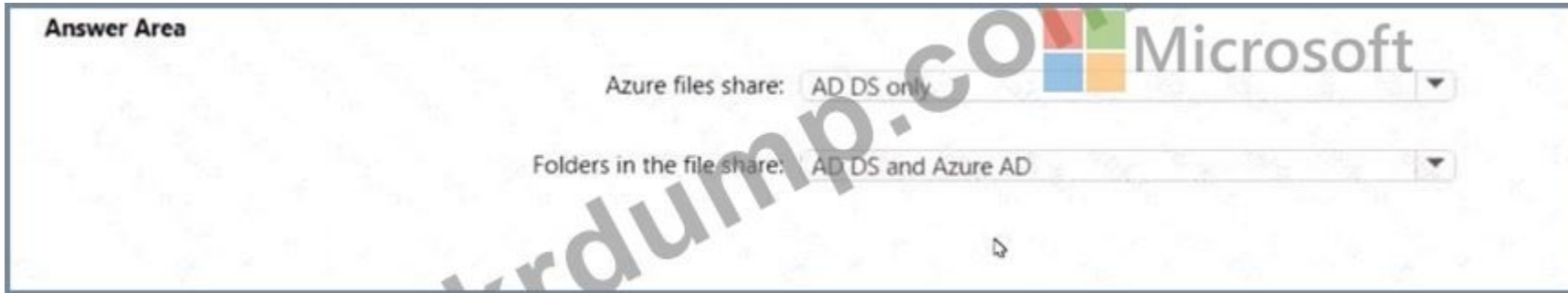


Answer:

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>

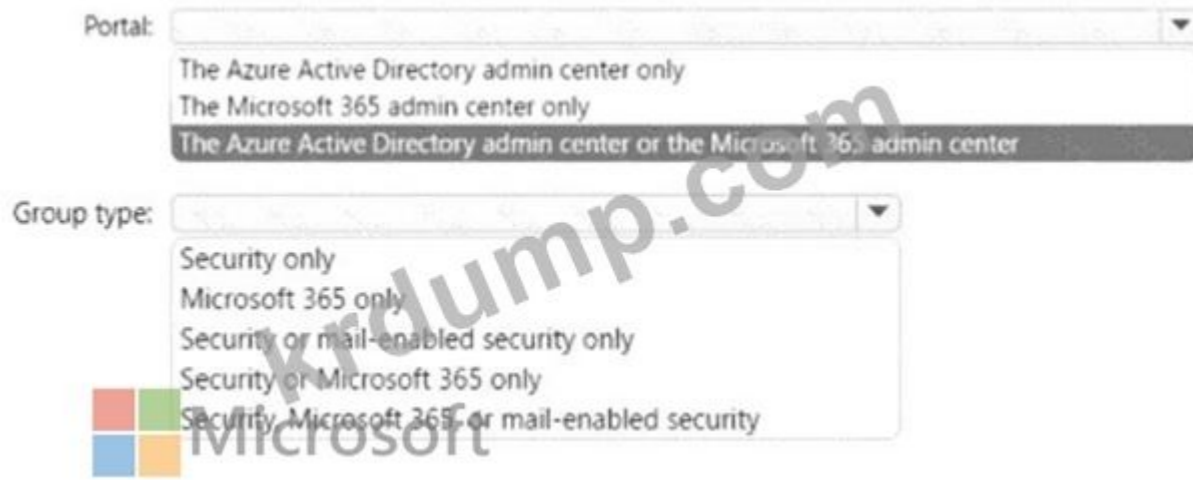
NEW QUESTION: 149

contoso.com Azure AD Azure AD Premium P1 .

Group1 .

1 ? .


: 1 .



Answer:

Portal:

Group type:



Explanation:

Portal:

Group type:



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

NEW QUESTION: 150

Sub1 is an Azure subscription. The following table shows the configuration of the resource groups in Sub1.

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



Sub1 contains a virtual machine (VM) named VM1.

* VM1

* VM1: DS2v2

* Resource Group: RG1

* VMs: VM1, VM2

* Scenario: Azure Security 2022

VM1 has Azure Disk Encryption enabled. The encryption keys are stored in Key Vault.

VM1 is in the same region as the Key Vault. What Key Vault is used for encryption?

- A. Vault1 and Vault3
- B. Vault1, Vault2, Vault3 and Vault4
- C. Vault1
- D. Vault1 and 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

VM1 is in the same region as the Key Vault. What Key Vault is used for encryption?

Name	Type
VM1	Virtual machine
VNet1	Virtual network
AFW1	Azure firewall

VM1 is in the same region as the Key Vault. What Key Vault is used for encryption?

What type of rule is used to allow traffic from VM1 to the Key Vault?

- A. Inbound NAT rule
- B. Outbound NAT rule
- C. DNAT rule
- D. SNAT rule

Answer: B (LEAVE A REPLY)

AZ-500-KR is a collection of questions and answers for the AZ-500-KR exam. DumpTop is the best source for AZ-500-KR questions and answers. **AZ-500-KR** is a collection of questions and answers for the AZ-500-KR exam. DumpTop is the best source for AZ-500-KR questions and answers. <https://www.dumptop.com/Microsoft/AZ-500-KR-dump.html> (517 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

NEW QUESTION: 152

Azure Firewall is used to protect the network resources in the Azure cloud.

VM1 is in the same region as the Key Vault. What Key Vault is used for encryption?

What type of rule is used to allow traffic from VM1 to the Key Vault?

What type of rule is used to allow traffic from VM1 to the Key Vault?

Which of the following is a valid Azure Container Instance (ACI) configuration?

- A. ContainerGroup { VMSize: 'Standard_D1', Containers: [{ Name: 'my-container', Image: 'my-image' }] }
- B. ContainerGroup { VMSize: 'Standard_D1', Containers: [{ Name: 'my-container', Image: 'my-image', Ports: [{ Port: 80, Protocol: 'TCP' }] }] }
- C. ContainerGroup { VMSize: 'Standard_D1', Containers: [{ Name: 'my-container', Image: 'my-image', Ports: [{ Port: 80, Protocol: 'TCP', Name: 'my-container' }] }] }
- D. ContainerGroup { VMSize: 'Standard_D1', Containers: [{ Name: 'my-container', Image: 'my-image', Ports: [{ Port: 80, Protocol: 'TCP', Name: 'my-container' }] }] }

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 SQL Database supports which of the following security protocols?

AzSQL1 supports Azure SQL Database security protocols.

AzSQL1 supports Azure SQL Database security protocols.

AzSQL1 supports Azure SQL Database security protocols.

* AzSQL1 supports Azure SQL Database security protocols, including TLS, TDE, and Microsoft Azure SQL Database security protocols.

* AzSQL1 supports Azure SQL Database security protocols, including TLS, TDE, and Microsoft Azure SQL Database security protocols.

AzSQL1 supports Azure SQL Database security protocols?

- A. TLS
- B. TLS and TDE
- C. Microsoft Azure SQL Database security protocols (TDE)
- D. Azure SQL Database security protocols
- E. TLS and TDE

Answer: B (LEAVE A REPLY)

NEW QUESTION: 154

LAW1 supports Azure Log Analytics Sub1 supports Azure Log Analytics.

Windows Server 2012 R2 and Windows Server 2016 support Log Analytics agents. LAW1 supports Log Analytics agents. LAW1 supports Log Analytics agents.

LAW1 supports Log Analytics agents. LAW1 supports Log Analytics agents.

* LAW1 supports Log Analytics agents.

* LAW1 supports Log Analytics agents.

* LAW1 supports Log Analytics agents.

* LAW1.

LAW1 supports Log Analytics agents?

- A. Yes
- B. Yes (Log Analytics agents)
- C. No
- D. No

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>

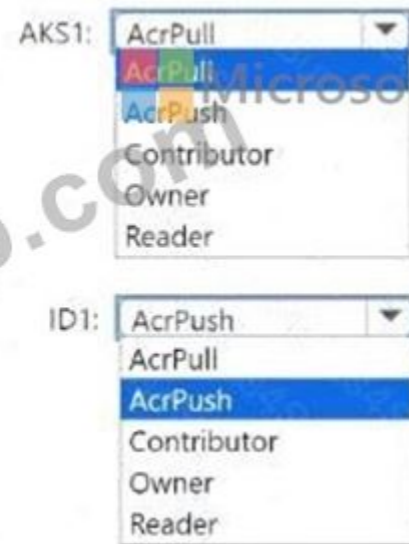
NEW QUESTION: 155

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

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

□□: □□ 1□□ 1□□□□.

Answer Area



Answer:



Explanation:

Answer Area

AKS1: AcrPull

ID1: AcrPush



NEW QUESTION: 156

User1 is a member of the Azure Active Directory (Azure AD) group. User1 is assigned the role of Contributor. User1 is assigned the role of Contributor. User1 is assigned the role of Contributor?

- A. Contributor
- B. Contributor
- C. Contributor
- D. Contributor

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 157

Sub1 is a subscription in Azure. Sub1 is a subscription in Azure.

Name	Location
RG1	West US
RG2	East US

Sub1 is a subscription in Azure Policy. Sub1 is a subscription in Azure Policy.

```

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

```

Sub1 is a subscription in Azure Policy.

00 00 0000 0000 00 000000.

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

00 0 0000 00, 0000 000000 '0'0 000000. 0000 0000 '0000'0 000000.

00: 00 100 100000.

Answer Area

Statements	Yes	No
You can create IPobject1.	<input type="radio"/>	<input type="radio"/>
You can create obj1.	<input type="radio"/>	<input type="radio"/>
You can create OBJ3.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area Microsoft

Statements	Yes	No
You can create IPobject1.	<input type="radio"/>	<input checked="" type="radio"/>
You can create obj1.	<input type="radio"/>	<input checked="" type="radio"/>
You can create OBJ3.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Answer Area

Statements	Yes	No
You can create IPobject1.	<input type="radio"/>	<input checked="" type="radio"/>
You can create obj1.	<input type="radio"/>	<input checked="" type="radio"/>
You can create OBJ3.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION: 158

00: 0 0000 0000 000000 00000 0000 00 0 000000. 0 0000 0000 0000 0 00 0000 0000 00000 00000. 00 00 00000 0000 0 0 000 000 0 00, 00 00 00000 0000 00 0 00000.


0 0000 0000 0000 0000 00 000000 0000 0 000000. 0000 00 0000 00 0000 000000 00000.

AKS10000 Azure Kubernetes Service(AKS) 000000 AZCR10000 Azure 00000 00000000 000000 Azure 0000 000000.

AKS10 AZCR10 0000 000000 000000 0000 0 0000 000000 0000.

00 00: AKS10 000000 00 00 000000 0000 00 ID0 Kubernetes Agentless Operator 0000 0000000.

0000 00 0000 0000000?

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

Which of the following is a valid configuration for an AKS cluster? HTTP application routing is enabled. IP address is 10.0.0.1. AKS cluster is in the East US region. TLS termination is enabled. Network configuration is Basic.

- A. AKS Ingress controller is enabled.
- B. Network configuration is Basic (CNI) and HTTP application routing is disabled.
- C. Azure container monitoring is enabled.
- D. Azure container monitoring is disabled.

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 Resource Manager (ARM) templates are used to create and manage Azure resources. Which of the following is a valid configuration for an ARM template? The template is a JSON file. The template is a YAML file. The template is a PowerShell script. The template is a Windows batch file.

- A. Microsoft Intune
- B. Azure Automation
- C. Azure Resource Manager
- D. Azure PowerShell

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

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.

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) is a cloud-based directory service. It is a part of Azure AD Premium Plan 2. It is used to manage users and groups in a cloud-based environment. The domain is fabrikam.com. The user is user@fabrikam.com. The user is user@fabrikam.com.

User1 is a user in the fabrikam.com domain. The user is user1@fabrikam.com.

* user1 is user1@fabrikam.com. The user is user1@fabrikam.com.

* User1 is a user in the fabrikam.com domain. The user is user1@fabrikam.com.

* The user is user1@fabrikam.com.

Which of the following is correct?

- A. user1 is a user in the fabrikam.com domain.
- B. The user is user1@fabrikam.com.
- C. The user is user1@fabrikam.com.
- D. User1 is a user in the fabrikam.com domain.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 165

Sub2 is a virtual machine in the fabrikam.com domain. It is used to manage users and groups in a cloud-based environment. The domain is fabrikam.com. The user is user@fabrikam.com. The user is user@fabrikam.com. The user is user@fabrikam.com.

Statements	Yes	No
From VM1, you can successfully ping the private IP address of VM4.	<input type="radio"/>	<input type="radio"/>
From VM2, you can successfully ping the private IP address of VM4.	<input type="radio"/>	<input type="radio"/>
From VM1, you can connect to the web server on VM4.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
From VM1, you can successfully ping the private IP address of VM4.	<input type="radio"/>	<input checked="" type="radio"/>
From VM2, you can successfully ping the private IP address of VM4.	<input checked="" type="radio"/>	<input type="radio"/>
From VM1, you can connect to the web server on VM4.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Statements	Yes	No
From VM1, you can successfully ping the private IP address of VM4.	<input type="radio"/>	<input checked="" type="radio"/>
From VM2, you can successfully ping the private IP address of VM4.	<input checked="" type="radio"/>	<input type="radio"/>
From VM1, you can connect to the web server on VM4.	<input checked="" type="radio"/>	<input type="radio"/>


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

Scenario: A company has a virtual network with two subnets. Sub1 is a Windows Server 2016 VM. Sub2 is an Azure Disk Encryption VM. The company wants to ensure that the VMs can communicate with each other and with the internet. The company has a key vault and wants to use it to store secrets for the VMs. The company has a storage account and wants to use it to store data for the VMs. The company has a virtual network and wants to use it to connect the VMs to the internet. The company has a virtual network and wants to use it to connect the VMs to the internet.

Actions	Answer Area
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.	

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](#).

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

Statements	Yes	No
User1 can map share1 to Server1 by using the access key of storage1.	<input type="radio"/>	<input type="radio"/>
User1 can map share1 to Server1 by using the user's credentials.	<input type="radio"/>	<input type="radio"/>
User1 can map share1 to Server2 by using the access key of storage1.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 can map share1 to Server1 by using the access key of storage1.	<input type="radio"/>	<input checked="" type="radio"/>
User1 can map share1 to Server1 by using the user's credentials.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can map share1 to Server2 by using the access key of storage1.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Statements	Yes	No
User1 can map share1 to Server1 by using the access key of storage1.	<input type="radio"/>	<input checked="" type="radio"/>
User1 can map share1 to Server1 by using the user's credentials.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can map share1 to Server2 by using the access key of storage1.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION: 168

User8 is a member of RG4, RG5, and RG6. What can User8 do?

User8 can create virtual networks in RG4, RG5, and RG6. User8 can create NSGs in RG4, RG5, and RG6.

What are the correct answers?

User8 can create virtual networks in:	<ul style="list-style-type: none">RG4 onlyRG6 onlyRG4 and RG6 onlyRG4, RG5, and RG6
User8 can create NSGs in:	<ul style="list-style-type: none">RG4 onlyRG4 and RG5 onlyRG4 and RG6 onlyRG4, RG5, and RG6

Answer:

User8 can create virtual networks in:



- RG4 only
- RG6 only
- RG4 and RG6 only
- RG4, RG5, and RG6

User8 can create NSGs in:

- RG4 only
- RG4 and RG5 only
- RG4 and RG6 only
- RG4, RG5, and RG6

Explanation:

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

Box2: RG4 & RG6

NEW QUESTION: 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

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□□□□□.

```
let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AccountType == 'User' and
    [dropdown menu: ActivityID, DataType, EventID, QuantityUnit] ==4625

| Summarize failed_login_attempts=
    [dropdown menu: Count(), Countif(), Makeset(), Split()]

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

Answer:

```
let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AccountType == 'User' and
    [dropdown menu: ActivityID, DataType, EventID, QuantityUnit] ==4625

Summarize failed_login_attempts=
    [dropdown menu: Count(), Countif(), Makeset(), Split()]

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

Explanation:

```

let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AccountType == 'User' and EventID == 4625

| Summarize failed_login_attempts=
    Count(),
    latest_failed_login=arg_max(TimeGenerated, Account)
    by Account
| where failed_login_attempts > 5

```

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

```

let timeframe = 1d;
SecurityEvent
| where TimeGenerated > ago(1d)
| where AccountType == 'User' and EventID == 4625 // 4625 - failed log in
| summarize failed_login_attempts=count(), latest_failed_login=arg_max(TimeGenerated, Account) by Account
| where failed_login_attempts > 5
| project-away Account1

```

References:

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

NEW QUESTION: 173

Scenario: A company has two virtual networks (VNet1 and VNet2) in Azure. Each VNet has a subnet (Subnet1 and Subnet2) and a network security group (NSG1 and NSG2). The NSGs are associated with the subnets. The subnets are connected to each other via a virtual network gateway.

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

NSG1 and NSG2 are configured to allow traffic between the subnets.

VM1 and VM2 are virtual machines that are connected to Subnet1 and Subnet2, respectively.

Name	Connected to
VM1	Subnet1
VM2	Subnet2

Question: What is the result of the configuration? (Select all that apply.)

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

Two virtual machines, VM1 and VM2, are deployed to Subnet1. VM1 is connected to VNet1 and VM2 is connected to VNet2. VM1 has a public IP address of 10.0.0.1 and VM2 has a public IP address of 10.0.0.2.

Answer Area



Statements

WebApp1 can connect to VM2.

Yes

No

NSG1 controls inbound traffic to WebApp1.

WebApp2 can connect to VM1.

Answer:

Answer Area

Statements

WebApp1 can connect to VM2.

Yes

No

NSG1 controls inbound traffic to WebApp1.

WebApp2 can connect to VM1.



Microsoft

Explanation:

ANSWER AREA

 **Statements** Microsoft
WebApp1 can connect to VM2.

Yes

No

NSG1 controls inbound traffic to WebApp1.

WebApp2 can connect to VM1.

NEW QUESTION: 174

contoso.com is a Microsoft Entra ID tenant.

fabrikam.com is a Microsoft Entra ID tenant with a conditional access policy.

contoso.com is configured to require MFA for all users.

Contoso.com is configured to require MFA for all users. (contoso.com is configured to require MFA for all users.)

□□ □□□ □□□□ □□□ □□□ □□□ □□□□.

* □□: CAPolicy1

* □□

o □□□ □□ □□ □□□: B2B □□ □□□ □□□

o □□ □□

□□: □□ □□□□ □ o □□□ □□

□□ □□ □□

□□□ □□□ □□□□ □□□ □□□□□ □

□□ □□ □□ □□

□□ □□□: □□

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

□□: □□□ □□ □□ □□□ 1□□□□□.

Answer Area

Statements

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.

Yes

No

Answer:

Answer Area

Statements

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.

Yes

No

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.	<input checked="" type="radio"/>	<input type="radio"/>
To minimize the number of MFA authentication prompts for the users in fabrikam.com, you must configure the Trust settings.	<input type="radio"/>	<input checked="" type="radio"/>
Users with devices that have a compliant device claim from fabrikam.com can review the user properties of the users in contoso.com.	<input type="radio"/>	<input checked="" type="radio"/>

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.	<input type="radio"/>	<input type="radio"/>
VM2 can ping VM4 successfully.	<input type="radio"/>	<input type="radio"/>
VM3 can be accessed by using Remote Desktop from the internet.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
VM1 can ping VM3 successfully.	<input checked="" type="radio"/>	<input type="radio"/>
VM2 can ping VM4 successfully.	<input type="radio"/>	<input checked="" type="radio"/>
VM3 can be accessed by using Remote Desktop from the internet.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Statements	Yes	No
VM1 can ping VM3 successfully.	<input checked="" type="radio"/>	<input type="radio"/>
VM2 can ping VM4 successfully.	<input type="radio"/>	<input checked="" type="radio"/>
VM3 can be accessed by using Remote Desktop from the internet.	<input checked="" type="radio"/>	<input type="radio"/>

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 ☐☐☐☐ ☐☐☐☐☐☐ ☐☐☐☐☐☐.

Answer: (SHOW ANSWER)

NEW QUESTION: 179

□□ □□□□ □□ □□□ □□ □□□.

```
Microsoft  
{"RoleAssignmentId": "13ae6e22-b93a-412f-9dc5-fc92b1726bde",  
"Scope": "/subscriptions/0a1baf97-0be4-424a-92fa-873c5a45fbbc/resourceGroups/RG1",  
"DisplayName": "Admin1",  
"SignInName": "Admin1@contoso.com",  
"RoleDefinitionName": "Owner",  
"RoleDefinitionId": "/subscriptions/0a1baf97-0be4-424a-92fa-873c5a45fbbc/providers/
```

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

□□: □□ 1□□ 1□□□□.

[answer choice] can delete VM1.

- Only Admin1
- Only Admin1 and Admin2
- Only Admin1 and Admin3
- Only Admin1 and Admin4
- Admin1, Admin2, Admin3, and Admin4

[answer choice] can create new resource groups.

Admin1 on These are the selections for the statement [answer choice] ca

- Admin2 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, Admin3, and Admin4

Answer:

[answer choice] can delete VM1.

- Only Admin1
- Only Admin1 and Admin2
- Only Admin1 and Admin3
- Only Admin1 and Admin4
- Admin1, Admin2, Admin3, and Admin4

[answer choice] can create new resource groups.

Admin1 on These are the selections for the statement [answer choice] ca

- Admin2 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, Admin3, and Admin4

NEW QUESTION: 180

Which of the following statements are true?

Name	Assigned server admin	Database
sqlsvr1	User1	DB1
sqlsvr2	Group1	DB2

Microsoft Entra ID is used to manage user identities and access to resources. In this scenario, you have two SQL Server instances, sqlsvr1 and sqlsvr2, and two databases, DB1 and DB2. The following table shows the server administrators assigned to each instance.

Answer Area

Statements	Yes	No
User1 can alter the schema of DB1.	<input type="radio"/>	<input type="radio"/>
User1 can alter the schema of DB2.	<input type="radio"/>	<input type="radio"/>
User2 can alter the schema of DB2.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 can alter the schema of DB1.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can alter the schema of DB2.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can alter the schema of DB2.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Answer Area

Statements	Yes	No
User1 can alter the schema of DB1.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can alter the schema of DB2.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can alter the schema of DB2.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION: 183

Which of the following statements are true?

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

Microsoft Entra ID is used to manage user identities and access to resources. In this scenario, you have two users, User1 and User2, and their user devices are listed in the following table.

□□: □□ 1□□ 1□□□□.

Authentication methods

- FIDO2 security key only
- Microsoft Authenticator app only
- Windows Hello for Business only
- Microsoft Authenticator app and Windows Hello for Business only
- Windows Hello for Business and FIDO2 security key only
- Microsoft Authenticator app, Windows Hello for Business, and FIDO2 security key

Answer Area

User1: _____

User2: _____

Answer:

Authentication methods

- FIDO2 security key only
- Microsoft Authenticator app only
- Windows Hello for Business only
- Microsoft Authenticator app and Windows Hello for Business only
- Windows Hello for Business and FIDO2 security key only
- Microsoft Authenticator app, Windows Hello for Business, and FIDO2 security key

Answer Area

User1: Microsoft Authenticator app only

User2: Windows Hello for Business only

Explanation:


Authentication methods

- FIDO2 security key only
- Microsoft Authenticator app only
- Windows Hello for Business only
- Microsoft Authenticator app and Windows Hello for Business only
- Windows Hello for Business and FIDO2 security key only
- Microsoft Authenticator app, Windows Hello for Business, and FIDO2 security key

Answer Area

User1: Microsoft Authenticator app only

User2: Windows Hello for Business only



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:

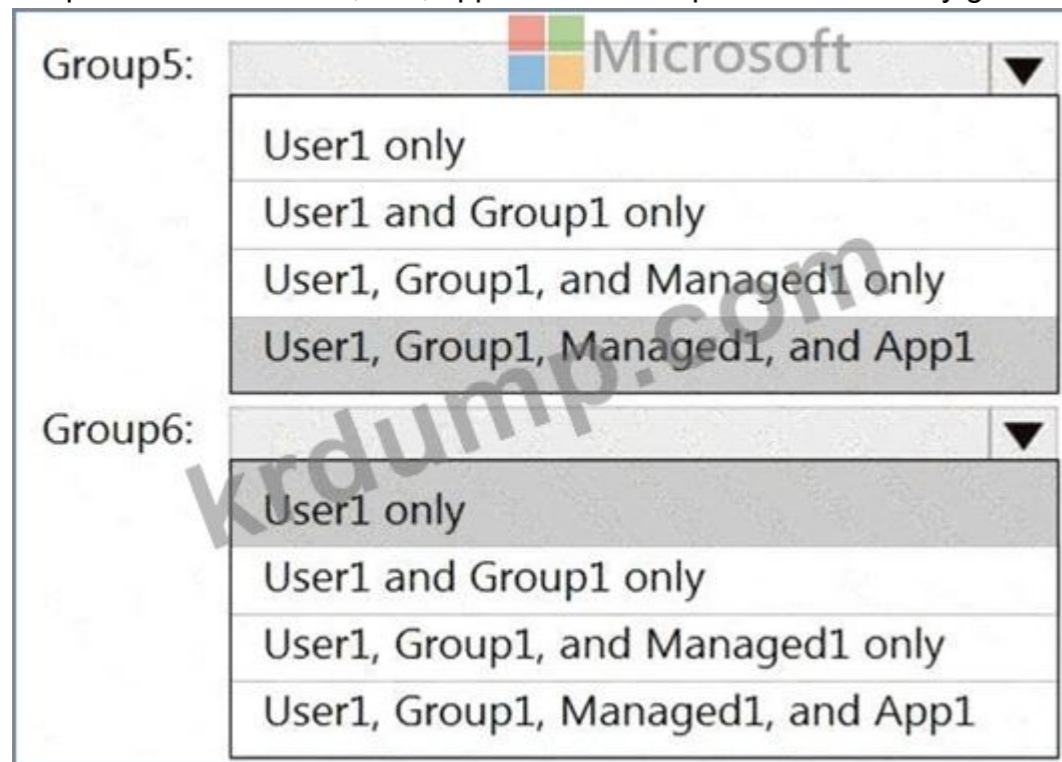
- User1 only
- User1 and Group1 only
- User1, Group1, and Managed1 only
- User1, Group1, Managed1, and App1

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

VM1 and VM2 are virtual machines in an Azure virtual network.

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

VM1 and VM2 are connected to VNET1. NSG1 is associated with VNET1.

VM1 and VM2 are connected to DB1. DB1 is connected to the Internet.

Which of the following is true?

- A. NSG1 blocks traffic from VM1 to DB1.
- B. VNET1 blocks traffic from VM1 to DB1.
- C. VNET1 blocks traffic from VM2 to DB1.
- D. NSG1 blocks traffic from VM2 to DB1.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 187

VM1 is a virtual machine in an Azure virtual network.

VM1 is connected to VNET1. NSG1 is associated with VNET1. NSG1 has the following rules:

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	AllowAzureLoadBalancerInBound	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 is configured with Just-in-Time (JIT) VM access. Which of the following is true?

- * Port: 3389, 22
- * Port: 3389
- * Port: 3389, 22
- * Port: 3389, 22

JIT rule priority over SSH rule for VM1.
 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 Area

Statements	Microsoft	Yes	No
The RDP rule has priority over the NSG rule created by JIT.		<input type="radio"/>	<input type="radio"/>
If you disconnect from VM1 within the three-hour time range, you must reactivate the JIT rule to reconnect to VM1.		<input type="radio"/>	<input type="radio"/>
The SSH connection to VM1 disconnects automatically after three hours.		<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Microsoft	Yes	No
The RDP rule has priority over the NSG rule created by JIT.		<input type="radio"/>	<input type="radio"/>
If you disconnect from VM1 within the three-hour time range, you must reactivate the JIT rule to reconnect to VM1.		<input type="radio"/>	<input type="radio"/>
The SSH connection to VM1 disconnects automatically after three hours.		<input type="radio"/>	<input type="radio"/>

Explanation:

Statements	Microsoft	Yes	No
The RDP rule has priority over the NSG rule created by JIT.		<input type="radio"/>	<input checked="" type="radio"/>
If you disconnect from VM1 within the three-hour time range, you must reactivate the JIT rule to reconnect to VM1.		<input type="radio"/>	<input checked="" type="radio"/>
The SSH connection to VM1 disconnects automatically after three hours.		<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION: 188

contoso.com is a Microsoft Enterprise managed domain. contoso.com has an App1 application that runs on an Android device. App1 is installed on the device. Azure Active Directory (AAD) is configured for the domain. What is the correct configuration for App1?

- A. AAD
- B. AAD
- C. AAD

D.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 189

Three ExpressRoute circuits are configured in a Microsoft Azure virtual network. The circuits are named ER1, ER2, and ER4. The virtual network is connected to a Microsoft Azure virtual network.

Which of the following ExpressRoute circuits are used for Layer 2 encryption?

Options: ER1, ER2, ER3, and ER4

Answer Area

Layer 2 encryption: ER3 and ER4 only

Layer 3 encryption: ER1, ER2, ER3, and ER4

Answer:

Answer Area

Layer 2 encryption: ER3 and ER4 only

Layer 3 encryption: ER1, ER2, ER3, and ER4

Explanation:

Answer Area

Layer 2 encryption: ER3 and ER4 only

Layer 3 encryption: ER1, ER2, ER3, and ER4

NEW QUESTION: 190

100 virtual machines are configured in a Microsoft Azure virtual network. The virtual machines are named VM1, VM2, and VM3. The virtual network is connected to a Microsoft Azure virtual network.

Which of the following Azure virtual network configurations are used for Layer 2 encryption?

Options: Initiative1, Initiative2, and Initiative3

Options: Initiative1, Initiative2, and Initiative3

- 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

Which Azure AD user role can be assigned the Owner subscription role?

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

Which Azure AD Privileged Identity Management (PIM) user roles can be assigned the Owner subscription role?

- 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

Which Azure Storage service can be used to store data in a secure and compliant manner?

storage1 is a storage account in the East US region. Which Azure Storage service can be used to store data in a secure and compliant manner?

storage1 is a storage account in the East US region. Which Azure Storage service can be used to store data in a secure and compliant manner?

- A. TLS
- B. Azure Key Vault
- C. Azure Storage
- D. Azure Key Vault

Answer: (SHOW ANSWER)

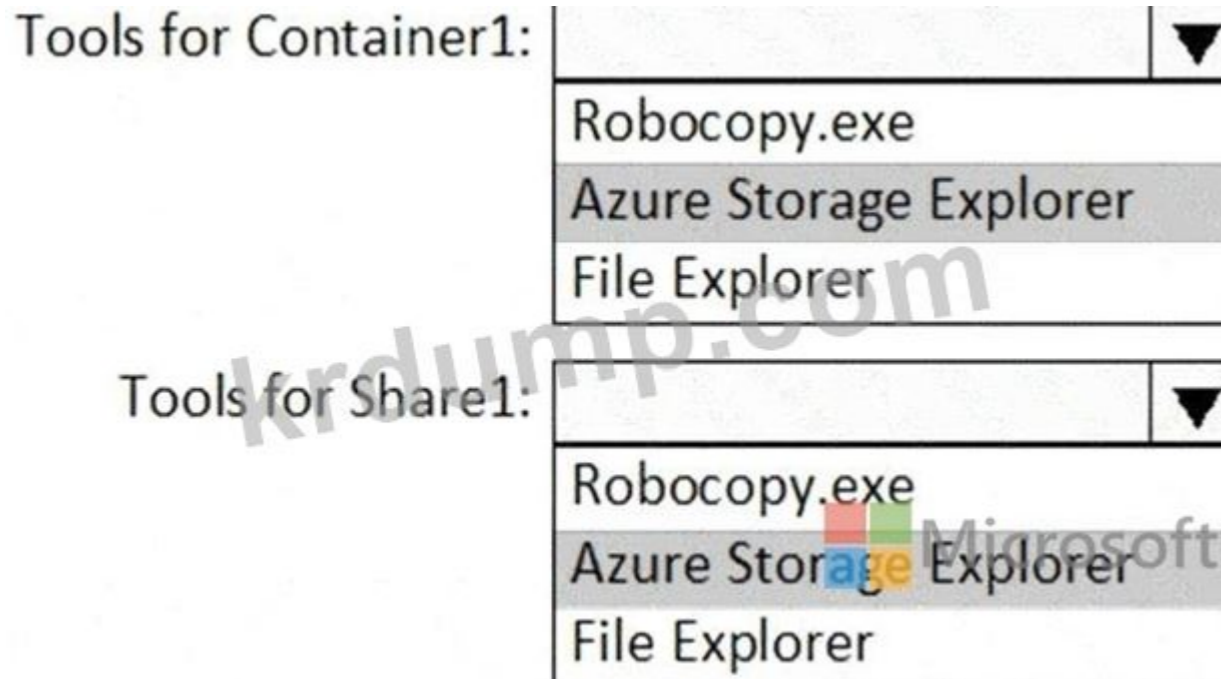
NEW QUESTION: 193

Which Azure Security Center tool can be used to monitor and manage security alerts?

Which Azure Security Center tool can be used to monitor and manage security alerts?

Which Azure Security Center tool can be used to monitor and manage security alerts?

- A. Azure Monitor



NEW QUESTION: 195

OU2 User1. You need to ensure that the tools are available to the users in the OU2. What should you do?

A. Assign the tools to the users in the OU2.

B. Assign the tools to the container in the OU2.

C. Assign the tools to the share in the OU2.

D. Assign the tools to the container in the share in the OU2.

Tools

- The Azure portal
- Azure AD Connect
- The Active Directory admin center
- Active Directory Sites and Services
- Active Directory Users and Computers

Answer Area

OU2:	Tool
User1:	Tool

Answer:

Tools

- The Azure portal
- Azure AD Connect
- The Active Directory admin center
- Active Directory Sites and Services
- Active Directory Users and Computers

Answer Area

OU2: Azure AD Connect

User1: The Azure portal

Explanation:

Table Description automatically generated

OU2: Azure AD Connect

User1: The Azure portal

NEW QUESTION: 196

Scenario: You are configuring a domain-joined Apache server to connect to an Azure Active Directory (Azure AD) domain. The server is located in a virtual machine (VM) in an Azure subscription. The VM is running Windows Server 2016. The Azure AD domain is named contoso.com. The Azure AD domain is connected to an on-premises Active Directory (AD) domain. The on-premises AD domain is named contoso.com. The on-premises AD domain is connected to an on-premises Active Directory (AD) domain. The on-premises AD domain is named contoso.com. The on-premises AD domain is connected to an on-premises Active Directory (AD) domain. The on-premises AD domain is named contoso.com.

What should you do to configure the Apache server to connect to the Azure AD domain?

- 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>

AZ-500-KR [www.dump.com](https://www.dump.com/Microsoft/AZ-500-KR-dump.html) DumpTop [www.dump.com](https://www.dump.com/Microsoft/AZ-500-KR-dump.html) AZ-500-KR [www.dump.com](https://www.dump.com/Microsoft/AZ-500-KR-dump.html)! DumpTop [www.dump.com](https://www.dump.com/Microsoft/AZ-500-KR-dump.html) **AZ-500-KR** [www.dump.com](https://www.dump.com/Microsoft/AZ-500-KR-dump.html) [www.dump.com](https://www.dump.com/Microsoft/AZ-500-KR-dump.html), DumpTop AZ-500-KR [www.dump.com](https://www.dump.com/Microsoft/AZ-500-KR-dump.html) [www.dump.com](https://www.dump.com/Microsoft/AZ-500-KR-dump.html) [www.dump.com](https://www.dump.com/Microsoft/AZ-500-KR-dump.html). [www.dump.com](https://www.dump.com/Microsoft/AZ-500-KR-dump.html) DumpTop AZ-500-KR [www.dump.com](https://www.dump.com/Microsoft/AZ-500-KR-dump.html) [www.dump.com](https://www.dump.com/Microsoft/AZ-500-KR-dump.html). <https://www.dump.com/Microsoft/AZ-500-KR-dump.html> (517 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

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

Which of the following statements are true? Select all that apply.

Answer Area

Statements

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.

Yes No

Answer:

Answer Area

Statements

You can create additional Microsoft Entra diagnostic settings. Yes No

You can configure retention for locations where Setting4 stores logs. Yes No

You can configure Setting2 to have Analytics1 and Analytics2 as destinations. Yes No

Explanation:

Answer Area

Statements	Yes	No
You can create additional Microsoft Entra diagnostic settings.	<input checked="" type="radio"/>	<input type="radio"/>
You can configure retention for locations where Setting4 stores logs.	<input checked="" type="radio"/>	<input type="radio"/>
You can configure Setting2 to use Analytics1 and Analytics2 as destinations.	<input type="radio"/>	<input checked="" type="radio"/>

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□□□□□.

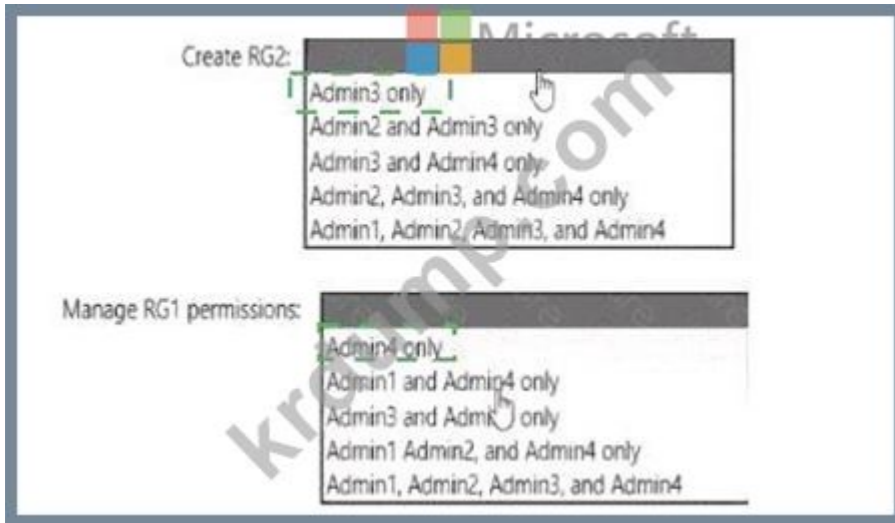
Create RG2:

- Admin3 only
- Admin2 and Admin3 only
- Admin3 and Admin4 only
- Admin2, Admin3, and Admin4 only
- Admin1, Admin2, Admin3, and Admin4

Manage RG1 permissions:

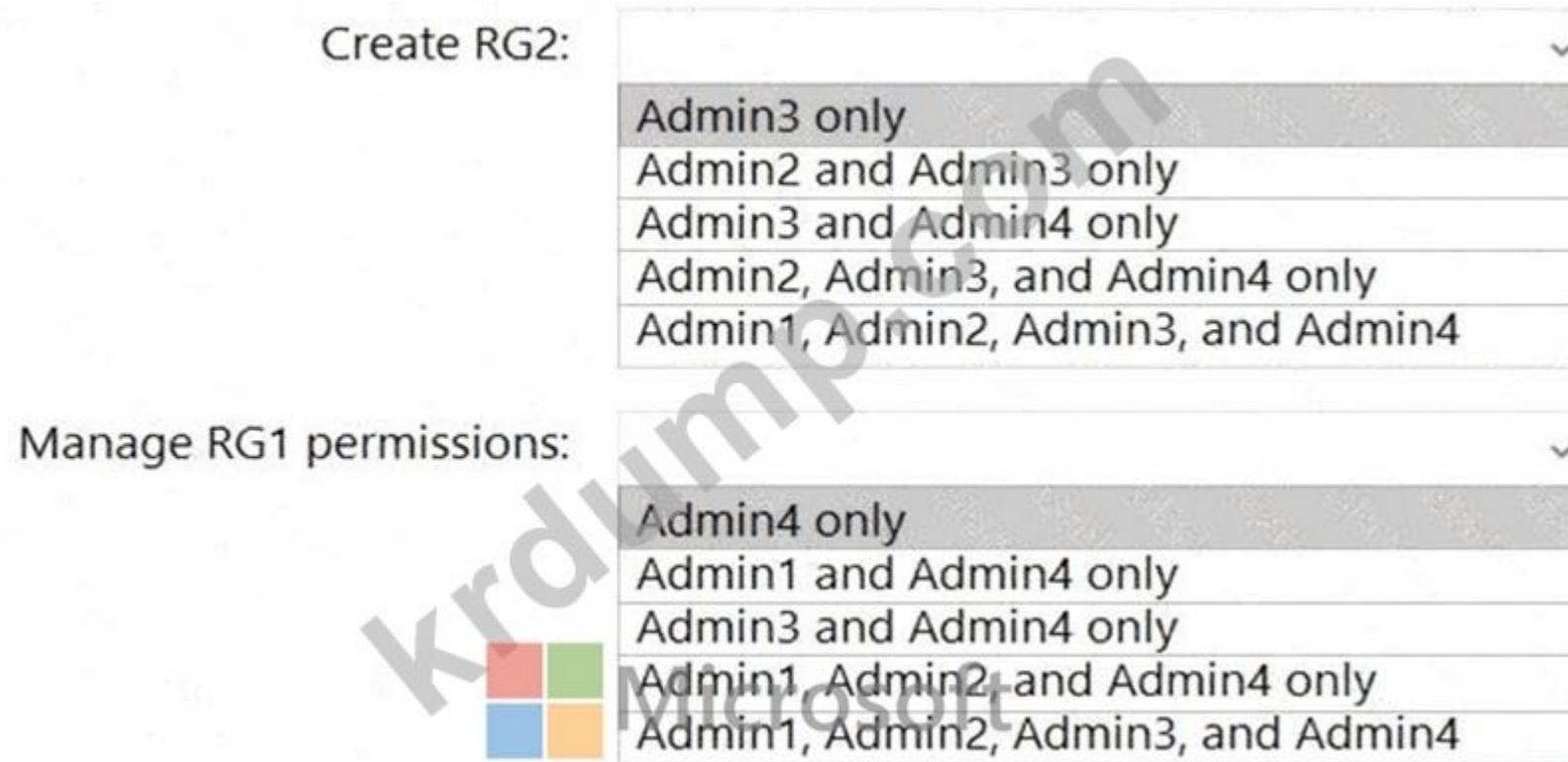
- Admin4 only
- Admin1 and Admin4 only
- Admin3 and Admin4 only
- Admin1, Admin2, and Admin4 only
- Admin1, Admin2, Admin3, and Admin4

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 .

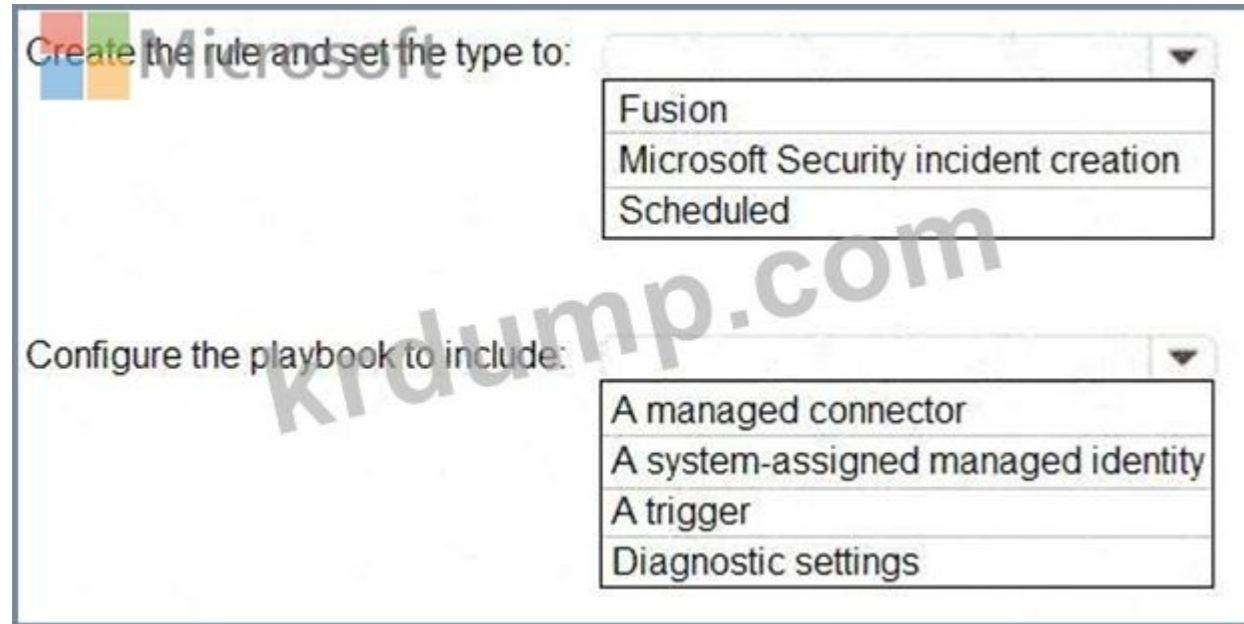
Query1 Azure AD .

Query1 Playbook1 Azure Sentinel .

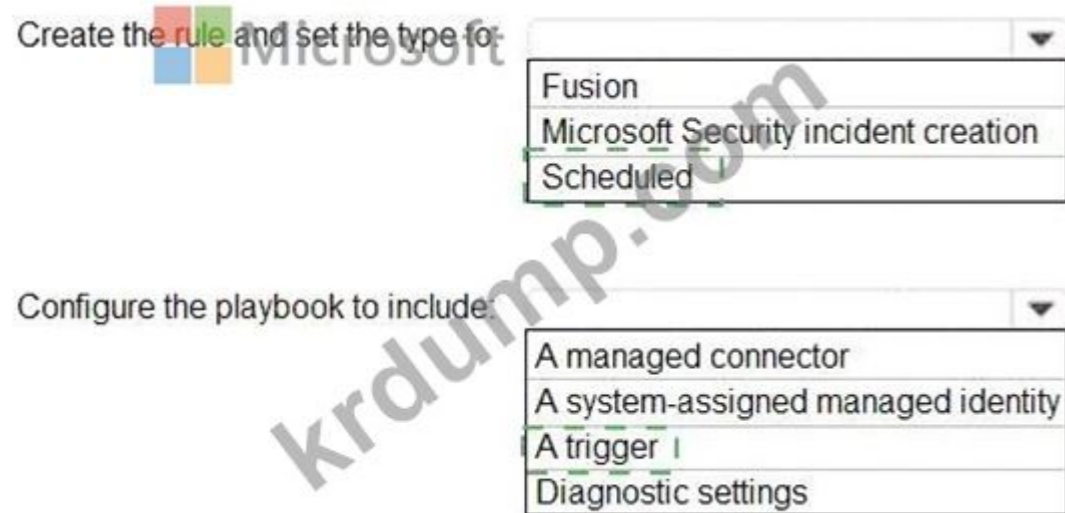
Playbook1 .

? .

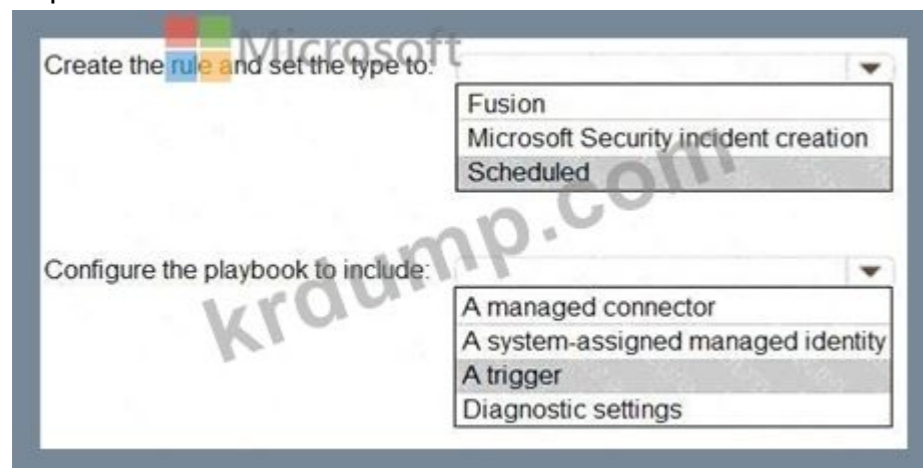
□□: □□ 1□□ 1□□□□.



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 □□□ □□□ □ □□□ □□□.

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

Actions

Answer Area

Add the query to Favorites.

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

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

Add a bookmark and assign a tag.

Add a bookmark and map an entity.

From Azure Monitor, run an Azure Log Analytics query.


Select a query result



Answer:



Actions	Answer Area
Add the query to Favorites.	From the Azure Sentinel workspace, run an Azure Log Analytics query.
From the Azure Sentinel workspace, run an Azure Log Analytics query.	Select a query result.
In a Jupyter notebook, create a reference to the IP address.	Add a bookmark and map an entity.
Add a bookmark and assign a tag.	
Add a bookmark and map an entity.	
From Azure Monitor, run an Azure Log Analytics query.	
Select a query result.	



Explanation:

From the Azure Sentinel workspace, run an Azure Log Analytics query.
Select a query result.
Add a bookmark and map an entity.

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 Area

Statements	Yes	No
You can associate RT1 with Subnet3.	<input type="radio"/>	<input type="radio"/>
You can delete RT1.	<input type="radio"/>	<input type="radio"/>
When you attempt to ping VM2 from VM1, traffic is routed to 172.16.10.10.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
You can associate RT1 with Subnet3.	<input checked="" type="radio"/>	<input type="radio"/>
You can delete RT1.	<input type="radio"/>	<input checked="" type="radio"/>
When you attempt to ping VM2 from VM1, traffic is routed to 172.16.10.10.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Answer Area

Statements	Yes	No
You can associate RT1 with Subnet3.	<input checked="" type="radio"/>	<input type="radio"/>
You can delete RT1.	<input type="radio"/>	<input checked="" type="radio"/>
When you attempt to ping VM2 from VM1, traffic is routed to 172.16.10.10.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION: 203

contoso.com Microsoft Entra User1 App1 Role1 Enterprise App1 Enterprise

- A. API
- B.
- C.
- D.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 204

storage1 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.	<input type="radio"/>	<input type="radio"/>
VM2 can connect to storage1.	<input type="radio"/>	<input type="radio"/>
VM3 can connect to storage1.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
VM1 can connect to storage1.	<input type="radio"/>	<input checked="" type="radio"/>
VM2 can connect to storage1.	<input checked="" type="radio"/>	<input type="radio"/>
VM3 can connect to storage1.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Statements	Yes	No
VM1 can connect to storage1.	<input type="radio"/>	<input checked="" type="radio"/>
VM2 can connect to storage1.	<input checked="" type="radio"/>	<input type="radio"/>
VM3 can connect to storage1.	<input type="radio"/>	<input checked="" type="radio"/>

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 Area

Service Principals:

- Managed1, VM1, and App1 only
- App1 only
- Managed1 and VM1 only
- Managed1, VM1, and App1 only**
- Managed1, VM1, App1, and Group1

Identities:

- Managed1 and VM1 only
- App1 only
- Managed1 and VM1 only**
- Managed1, VM1, and App1 only
- Managed1, VM1, App1, and Group1

Answer:



Explanation:



NEW QUESTION: 206

☐☐ ☐☐ ☐☐ ☐☐ Azure Firewall ☐☐☐ ☐☐☐ Azure ☐☐☐ ☐☐☐☐.

Name	Type
Policy1	Standard
Policy2	Premium

☐☐☐☐ ☐☐ ☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐.

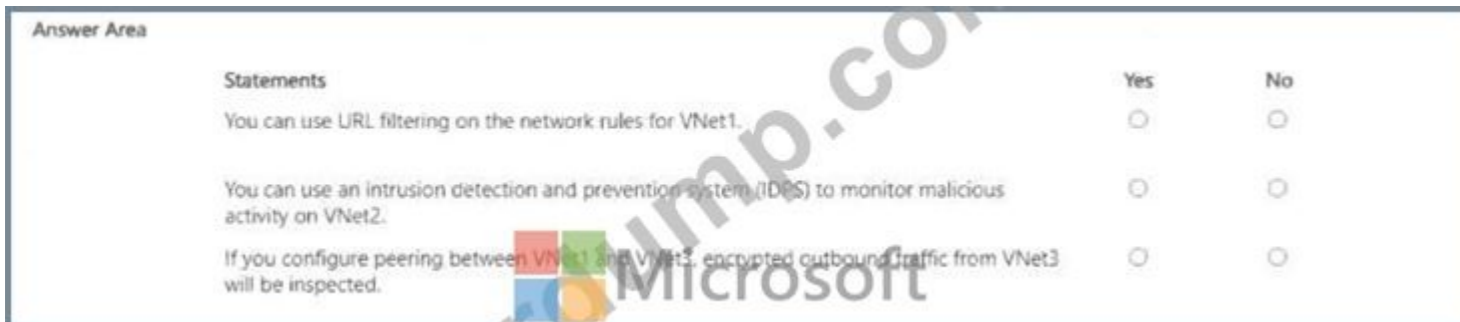
Name	Tier	Policy
FW1	Premium	Policy2
FW2	Premium	Policy1

☐☐☐☐ ☐☐ ☐☐ ☐☐☐☐ ☐☐☐☐☐☐ ☐☐☐☐☐☐☐.

Name	Firewall
VNet1	FW1
VNet2	FW2
VNet3	None

☐☐ ☐☐☐☐ ☐☐, ☐☐☐☐☐☐☐☐ '☐'☐☐☐☐☐☐. ☐☐☐☐☐☐☐☐ '☐☐☐☐'☐☐☐☐☐☐.

☐☐: ☐☐ 1☐☐ 1☐☐☐☐.



Answer:

NEW QUESTION: 209

Azure .

Azure AD(Azure Active Directory) PIM(Privileged Identity Management) Azure AD .

? .

Actions

Answer Area

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

Consent to PIM.

 Microsoft
Sign up PIM for Azure AD roles.


Discover privileged roles.

Discover resources.

Answer:



Actions	Answer Area
Verify your identity by using multi-factor authentication (MFA).	Consent to PIM.
Consent to PIM.	Verify your identity by using multi-factor authentication (MFA).
Sign up PIM for Azure AD roles.	Sign up PIM for Azure AD roles.
Discover privileged roles.	
Discover resources.	

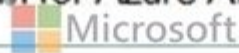


Explanation:

Consent to PIM.

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

Sign up PIM for Azure AD roles.



Step 1: Consent to PIM

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 .

Upload images: ▼

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

Download images: ▼

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

Answer:

Upload images: ▼

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

Download images: ▼

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

Explanation:

Upload images:

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

Download images:

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

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>

AZ-500-KR 00 000 000000 00 DumpTop 00 0000 000 AZ-500-KR 00! DumpTop 0 00 AZ-500-KR 00 000 000000, DumpTop AZ-500-KR 00 000 000000 000 000 00000000. 0000 000 0000 00 DumpTop AZ-500-KR 000 000000. <https://www.dumptop.com/Microsoft/AZ-500-KR-dump.html> (517 Q&As Dumps, 30%OFF Special Discount: KrDump)

NEW QUESTION: 212

00 00 000 0000 000 Microsoft Entra 0000 0000.

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

00 000 000 Microsoft Entra Identity Protection 000 00 000 000 000000.

* 00: 001 00, 002 00

* 00 : 000 00 00 : 00 00

* 00: 00 00, 00 00 00

0000 Microsoft Entra ID 00000 0 00 00 000000 00000 000.

0 0000 00 000 00000 000? 00 0000 000 000 00000 000000.

00: 00 100 100000.

Answer Area

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

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

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

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

Answer:

Answer Area

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

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

Explanation:

Answer Area

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

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

NEW QUESTION: 213

□□□ □□
 □□□ □□ □□ □□□ □□ □□□ □□□□□.
 □□□ □□□ □□□□□ □□□ □□□ □□□ □□ □□□ □□□ □□□□□.
 □□□□□ □□□□□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□ □□□□□.
 Azure □□□ □□: User1 -28681041@ExamUsers.com
 Azure □□□□: GpOAe4@IDg
 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.

AZ-500-KR ☐☐ ☐☐☐ ☐☐☐☐☐☐ ☐☐ DumpTop ☐☐ ☐☐☐☐ ☐☐☐ AZ-500-KR ☐☐! DumpTop ☐ ☐☐ **AZ-500-KR** ☐☐ ☐☐☐ ☐☐☐☐☐☐, DumpTop AZ-500-KR ☐☐ ☐☐☐ ☐☐☐☐☐☐☐☐☐☐☐☐. ☐☐☐☐☐ ☐☐☐☐☐☐☐☐☐☐☐☐ DumpTop AZ-500-KR ☐☐☐ ☐☐☐☐☐☐. <https://www.dumptop.com/Microsoft/AZ-500-KR-dump.html> (517 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)