Microsoft.AZ-500-KR.v2026-08-28.q246

□□□□:	AZ-500-KR
□□□□:	Microsoft Azure Security Technologies (AZ-500 Korean Version)
□□□:	Microsoft
□□ □□ □□□:	246
□□:	v2026-08-28
# □□ □:	107
# □□ □□□:	2460
https://www.krdump.com/Microsoft.AZ-500-KR.v2026-08-28.q246.html	

NEW QUESTION: 1

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

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

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

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

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

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

□□: □□ 1□□ 1□□□□.

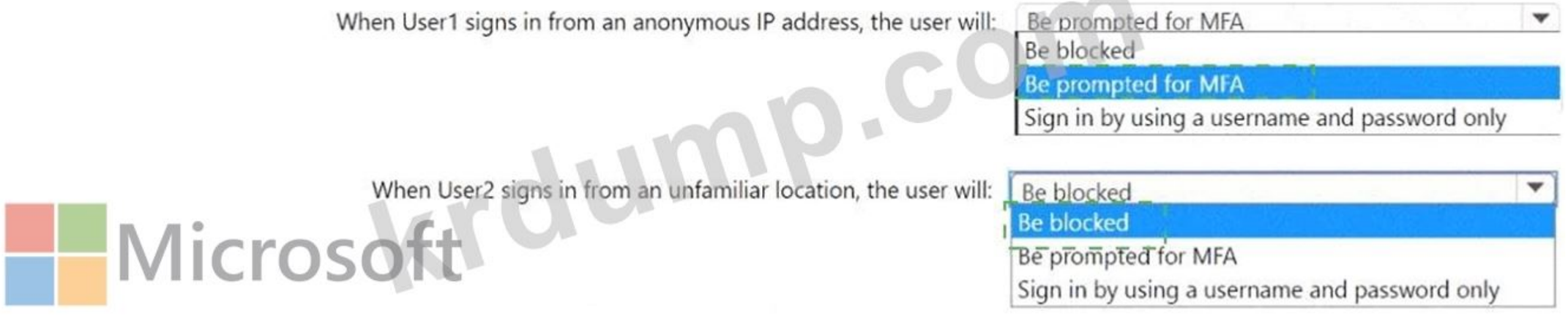
Answer Area

When User1 signs in from an anonymous IP address, the user will: Be prompted for MFA
- 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



Explanation:

NEW QUESTION: 2

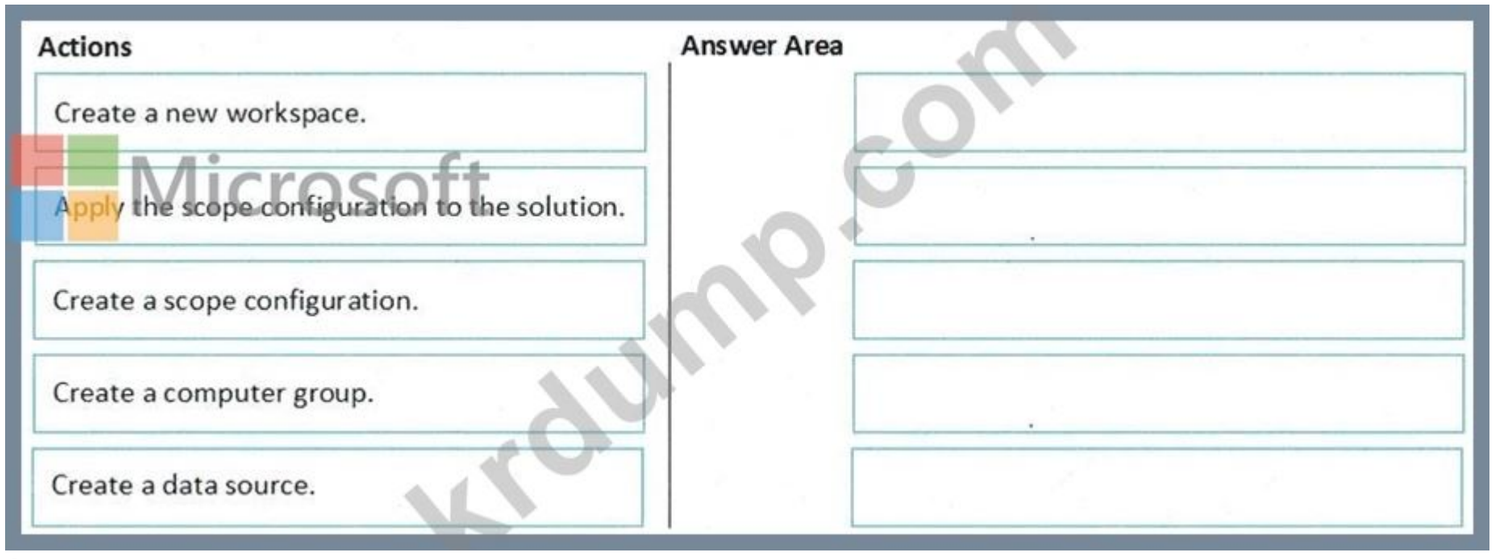
LAW1□□□ Azure Log Analytics □□ □□□ □□□□ Sub1□□□ Azure □□□ □□□□.

Windows Server 2016□ □□□□ LAW1□ □□□ Azure □□ □□□ 500□ □□□□.

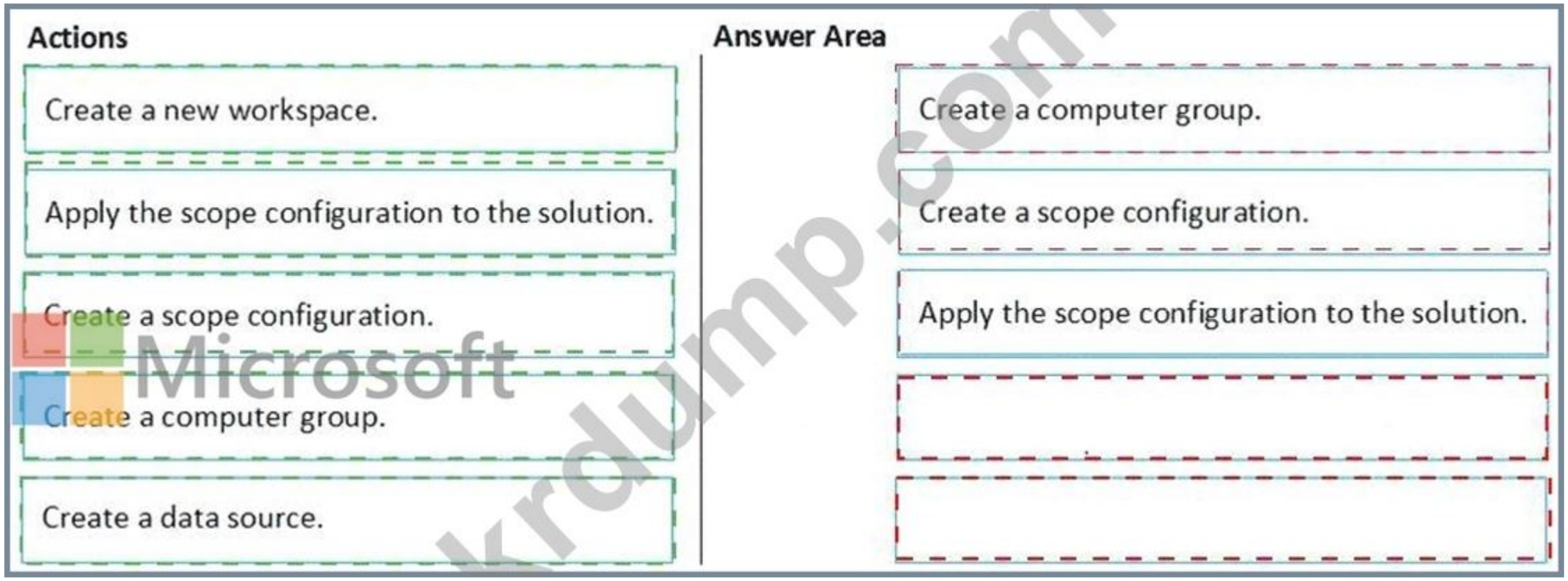
LAW1□ □□□ □□□□ □□ □□□□ □□□ □□□□□.

□□□ □□□□ □□ □□ □□□ 100□□ □□ □□□□□ LAW1□ □□□□□□ □□ □□□.

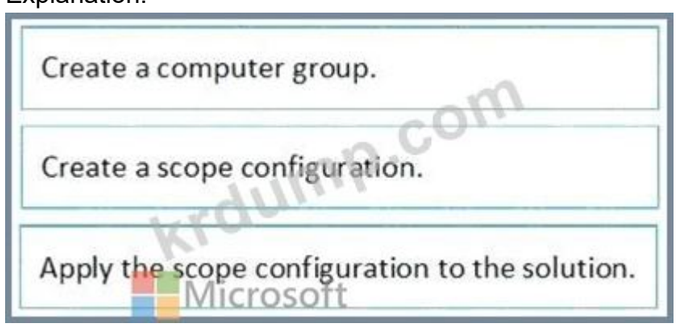
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□□ □□ □□□□ □□ □□□ □□ □□□□ □□ □□□ □□□□ □□□□□.



Answer:



Explanation:

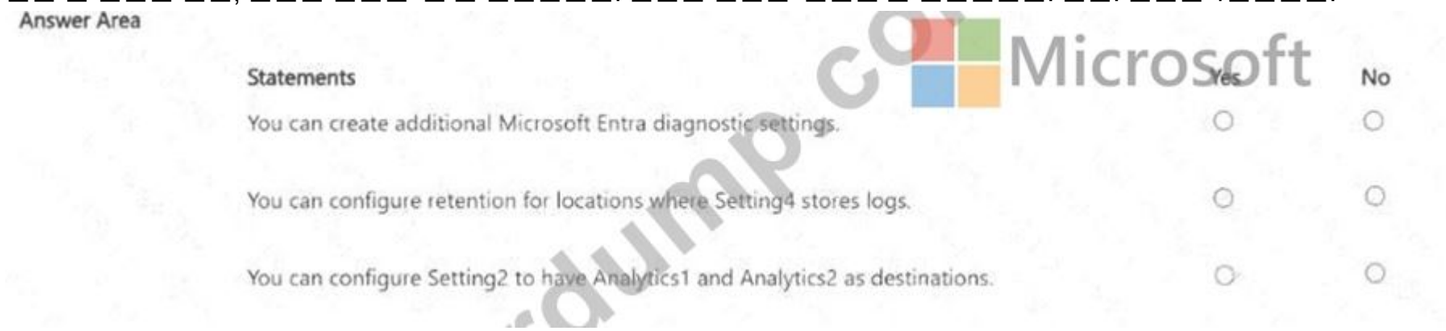


References:
https://docs.microsoft.com/en-us/azure/azure-monitor/insights/solution-targeting

NEW QUESTION: 3
storage1, storage2, storage3□□□ □ □□ □□□ □□, Analytics1, Analytics2, Analytics3□□□ □ □□ Log Analytics □□ □□, EventHub1, EventHub2, EventHub3□□□ □ □□ Azure □□□ □□□ □□□ Azure □□□ □□□□.
Microsoft Entra ID□ □□ □□ □□ □□□ □□ □□□ □□□□.

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

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



Answer:

Explanation:

NEW QUESTION: 4

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

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

NSG1□ NSG2□ □ □ □□ □□□ □□□ □□□□.

□□□□ □□ □□ □□□ □□ □□□ □□□□ □□□□.

Name	Connected to
VM1	Subnet1
VM2	Subnet2

□□□□ □□ □□ □□□ □ □□ □□□□ □□□□.

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

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

Answer Area

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

Answer:

Answer Area

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

Explanation:

NEW QUESTION: 5
□□ □□ □□□ □□ □□□□□ □□□ □□□ □□□□.
Azure □□□ □□□□.
□□□□□ □□□□ □-□□□□ □□□ Microsoft Defender for Cloud□ □□□□ □□□□□.
Microsoft Entra □□ □□□ □□ □□ □□□□□ □□□□□ ID□ □□□□ □□□.
□□ □□□ □□□□□□ □□□□ □□□?
A. □□□□□ □□□ □□ ID
B. □□□ □□
C. □□ □□
D. □□□□ □□□ □□ ID
E. □□□ □□
Answer: E (LEAVE A REPLY)

NEW QUESTION: 6
□□□ Subscription1□□□ Azure □□□ □□□□. Subscription1□ □□ □□ □□ □□ □□□□ □□□□ Azure Active Directory □□□□ □□□□ □□□□.

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

□□□ □□□ □□□□□ □□□□□□□.
□□□ Subscription1□ □□□□ □□□□ □□□.
□□ □□□□ □□□□ □□□ □ □□□, □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.

Answer:

Explanation:

Table Description automatically generated

Reference:

https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/billing-subscription-transfer

NEW QUESTION: 7

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

AUI□ AU2□ □□ □□□□ □□□ □ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

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

AU1□ AU2□ □□ □□□ □□□ □ □□□? □□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □□ 1□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 8

□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

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

SQL1□□□ □□ □□□ □□□(TDE)□ □□□□□□□□□.

□□ □□ □□□ □□ □□□ □□□ □□□ □□□□□.

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

Azure Resource Manager(ARM) □□□□ □□□□ Azure SQL □□□□□□□ □□□ □□□□□. □□□□□□□ □□ □□ □□ □□□□□.

Name	Resource group	TDE
SQL2	RG2	Disabled
SQL3	RG1	Disabled

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

Statements	Yes	No
SQL1 will have TDE enabled automatically.	○	○
The deployment of SQL2 will fail.	○	○
SQL3 will be deployed and marked as noncompliant.	○	○

Answer:

Statements	Yes	No
SQL1 will have TDE enabled automatically.	○	◌
The deployment of SQL2 will fail.	◌	○
SQL3 will be deployed and marked as noncompliant.	◌	○

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

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

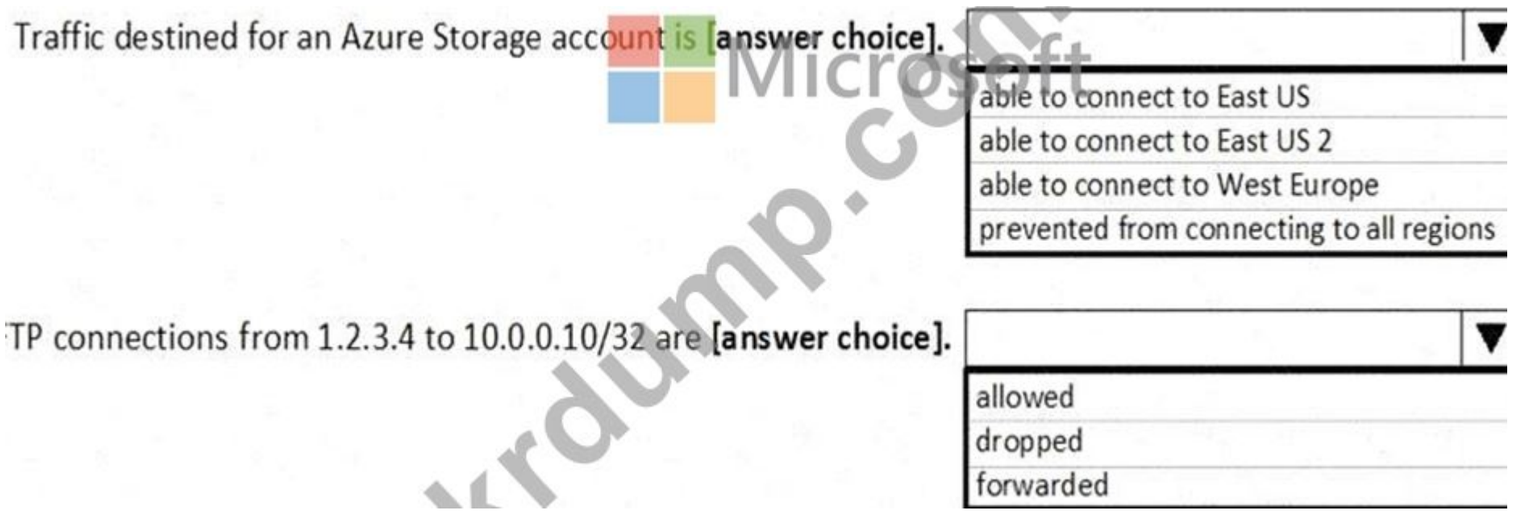
NEW QUESTION: 9
Azure Active Directory(Azure AD)□ □□□□□ □□□ □□□□. Azure AD □□□ □□□□□ □□□ Azure SQL Database □□□□□ □□□□.
□□□□□□ □□□□ □ Active Directory □□□ □□□□ □□□□□□ □□□□□ □□□□ □□□□ □□□.
□□□□ Microsoft SQL Server Management Studio□ □□□□ □□□□□ □□□ □ □□□ □□ □□□. □□□□ □□ □□□□ □□□□□ □□□.
□□ □□ □□□ □□□□ □□□?
A. Active Directory - □□□□
B. Active Directory - MFA □□□ □□ Universal
C. SQL Server □□
D. Active Directory - □□
Answer: (SHOW ANSWER)
References:
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure

NEW QUESTION: 10
□□□ □□□ App1□□□ Azure □□□ □□□ Azure □□□ □□□□.
App1□ Endpoint1□□□ □□□□ □□□□□□ □□□□ Cosmos1□□□ Azure Cosmos DB □□□□□□□ □□□□□. Endpoint1□ □□ □□□ □□□□□.
Cosmos1□ □□ □□ □□□ □□□□ □□□.
□□ DNS □□□ □□□□ □□□?
A. Endpoint1. Privatelink,blob,core,windows,net
B. Endpoint1. Privatelink,documents,azure,com
C. Endpoint1.Privatelink,azurewebsites,net
D. Endpoint1. Privatelink, database, azure, com
Answer: B (LEAVE A REPLY)

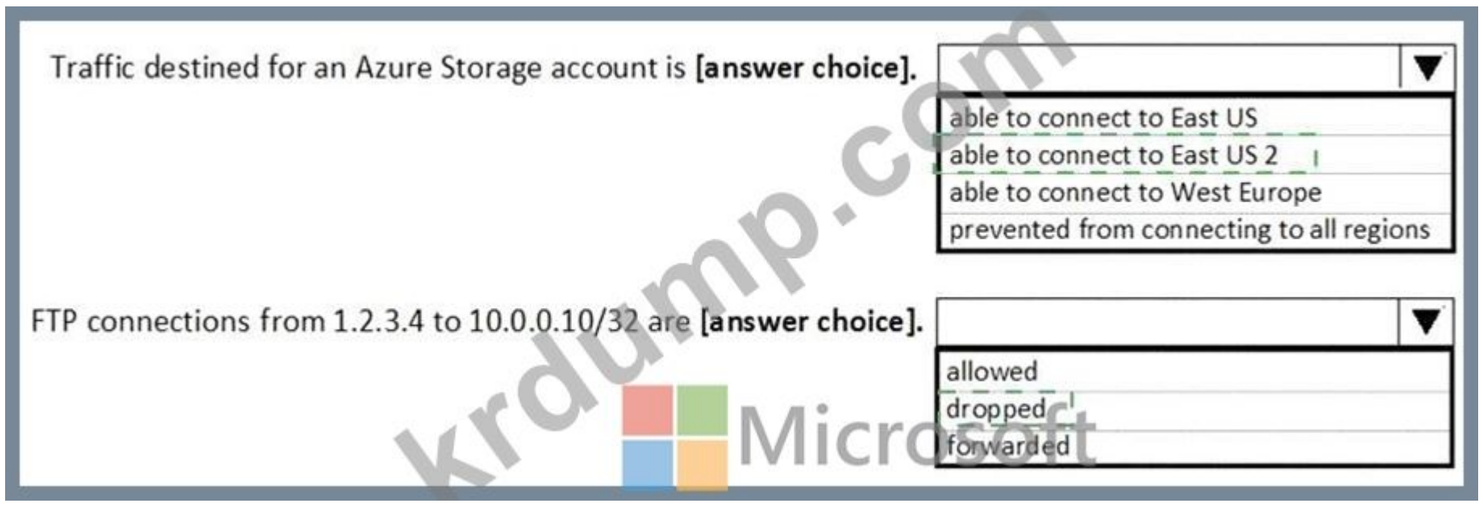
NEW QUESTION: 11
Azure □□□□ □□□□ □□□□ □□ □□(NSG)□ □□□□.
Get-AzureRmNetworkSecurityRuleConfig□ □□□□ □□ □□□ □□□ □□□ □□ □□□.

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

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

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



Answer:



Explanation:

Box 1: able to connect to East US 2

The StorageEA2Allow has DestinationAddressPrefix {Storage/EastUS2}

Box 2: dropped

Reference:

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

NEW QUESTION: 12

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

□ □□□ App1□□□ □□□ □□□□□□□ □□□□□. App1□ OAuth 2 □□□ □□ □□□ □□□□ Azure AD □□□ □□□ □□□□□.

Azure AD□ App1□ □□□□ □□□.

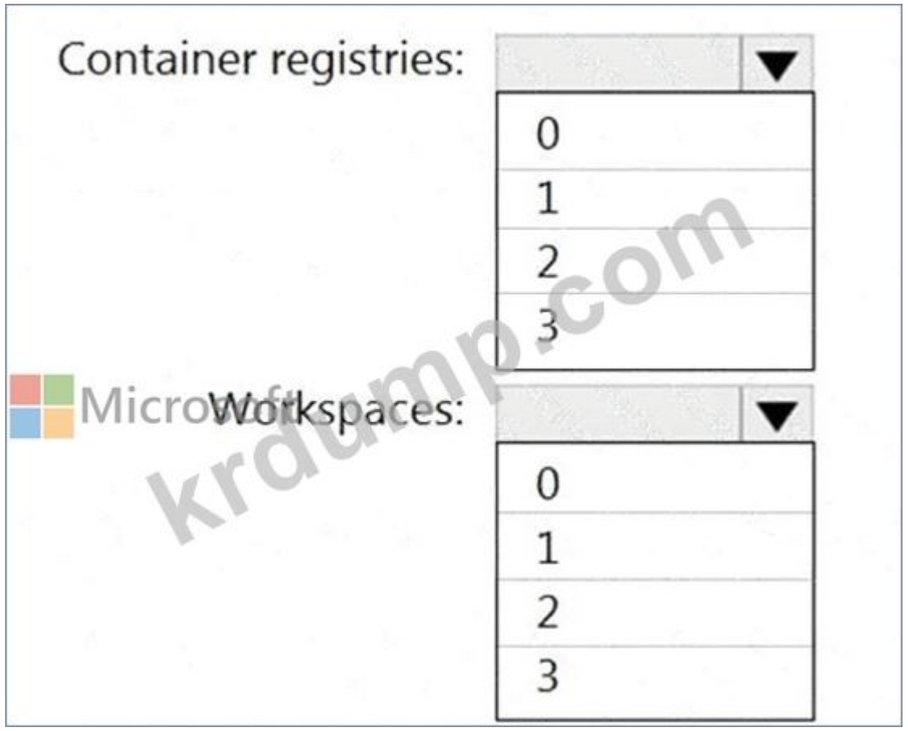
□□□□□□□ □□□□□ □□□□□□ □□ □□□ □□□ □□□?

A. □□□□ URI

B. □□ URL

C. □
D. □□□□□□ ID
Answer: A (LEAVE A REPLY)
For Native Applications you need to provide a Redirect URI, which Azure AD will use to return token responses.
References:
https://docs.microsoft.com/en-us/azure/active-directory/develop/v1-protocols-oauth-code

NEW QUESTION: 13
□□ □□ □□□ □□□□□ Azure Sentinel □□□□ □□ □□□ □□□□ □□□.
Azure □□□□ □□□□□□ Azure Machine Learning □□ □□□ □□ □□□ □□□□□?



Answer:

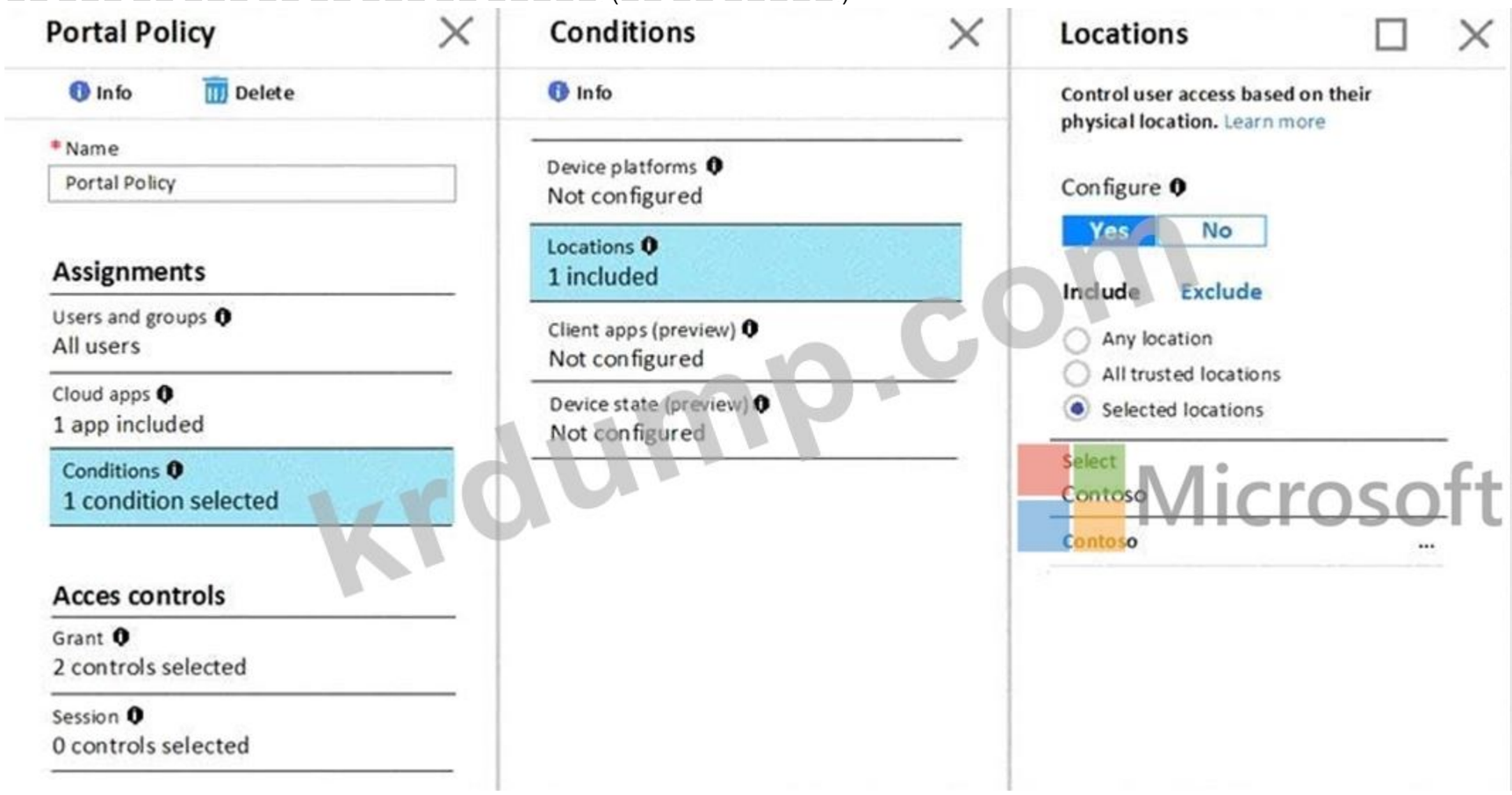
Explanation:

Table Description automatically generated with medium confidence

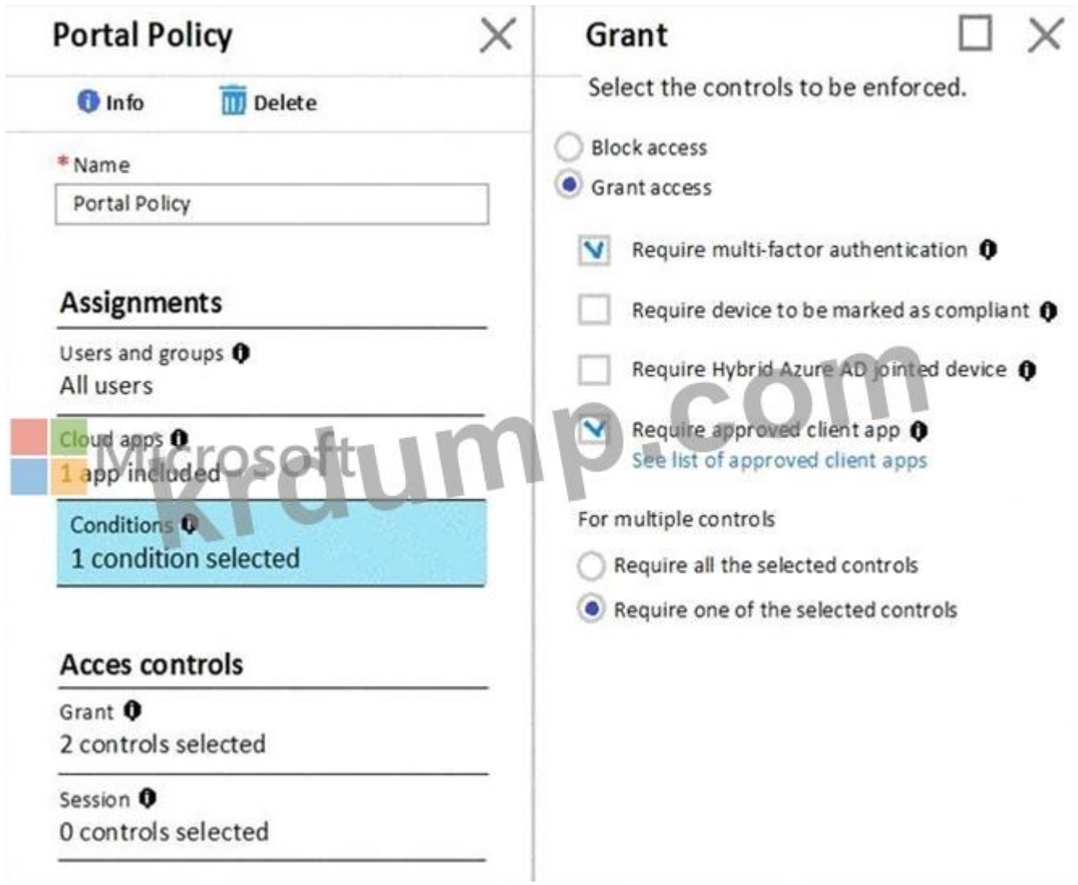
Reference:

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

NEW QUESTION: 14
□ Azure Active Directory(Azure AD) □□□□ □□□ □ Azure □□□ □□□□.
□□ □□□□□ □□ □□□ □□□ □□□ □□ □□□□. □□ □□□ Microsoft Azure Management □□□□ □□ □□ □□□□ □□□□ □ □□□□□.
□□ □□□ □□ □□□ □□ □□ □□□ □□ □□□□□. (□□ □□ □□□□□.)



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



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

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

Answer:

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

Explanation:

Box 1: No

The Contoso location is excluded

Box 2: NO

Box 3: NO

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

NEW QUESTION: 15

□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

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

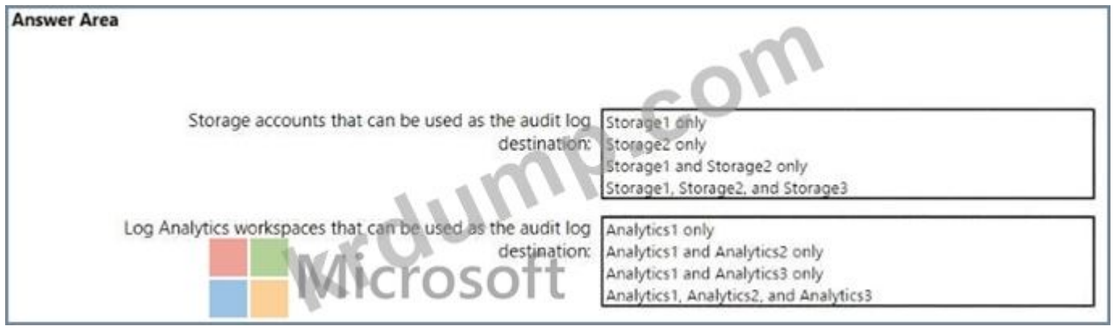
□□ □□ □□□ Azure Storage □□□ □□□□.

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

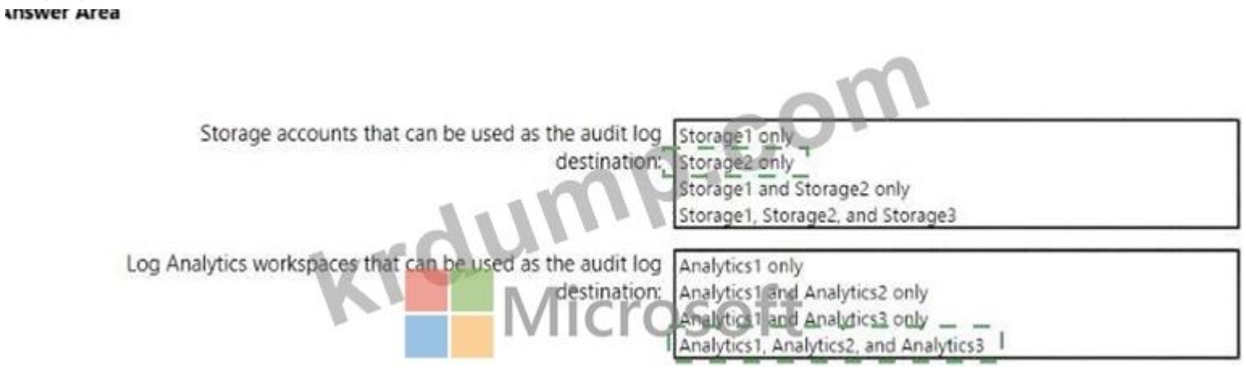
SQL1□ □□ □□□ □□□□ □□□.

□□ □□ □□□□ □□□ □ □□ □□□□ □□□ Log Analytics □□ □□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

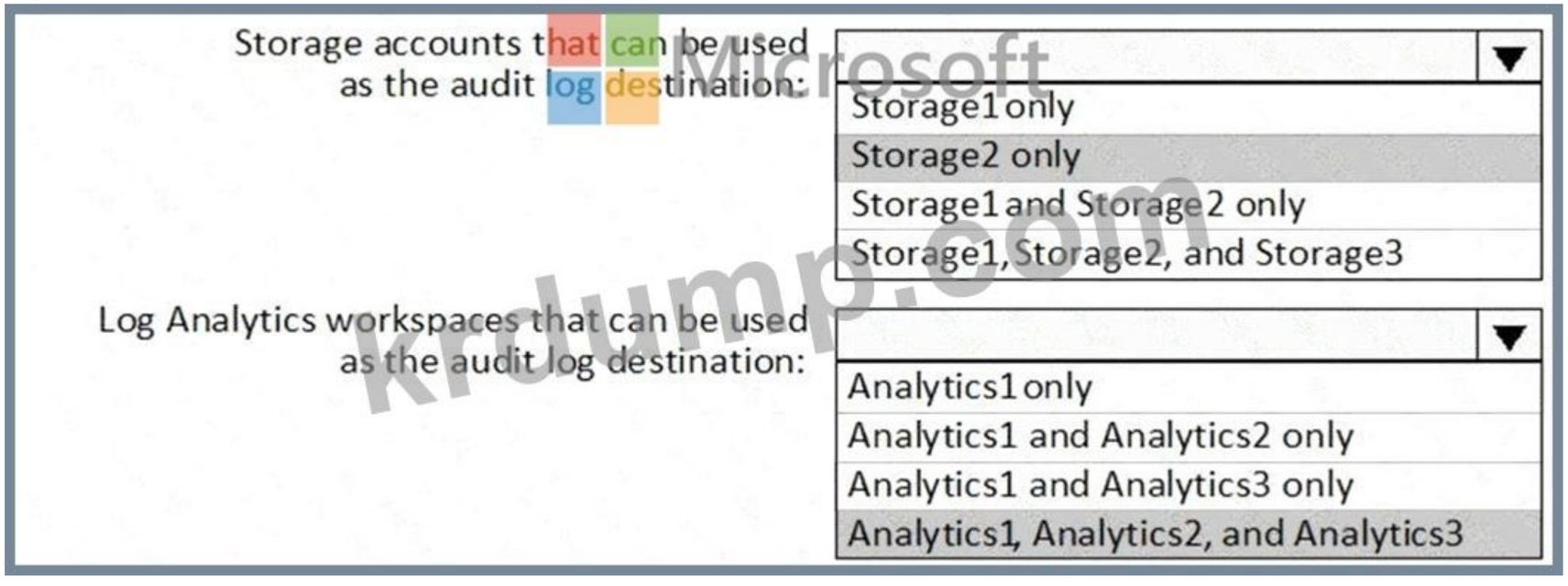
□□: □□ 1□□ 1□□□□.



Answer:



Explanation:



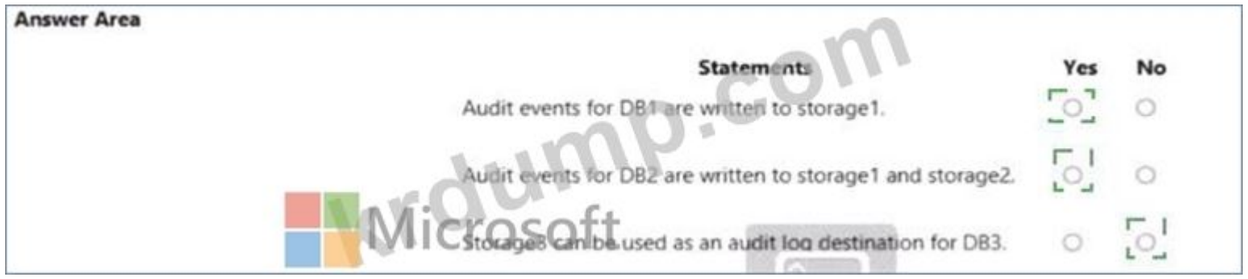
NEW QUESTION: 16

□ □□ □□□ □□, SQL□□□ □□□ Azure SQL □□□ □□□□, □□□ □ □□ Azure SQL □□□□□□□ □□□ Azure □□□ □□□□. □□□ □□□ □□ □□ □□ □□□□ □□□□. SQ11□ □□□ □□□ □□□□.

* □□: □□

* □□ □□: storage1
Azure SQL □□□□□□□ □□ □□ □□ □□□□□.

Answer:



Explanation:

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

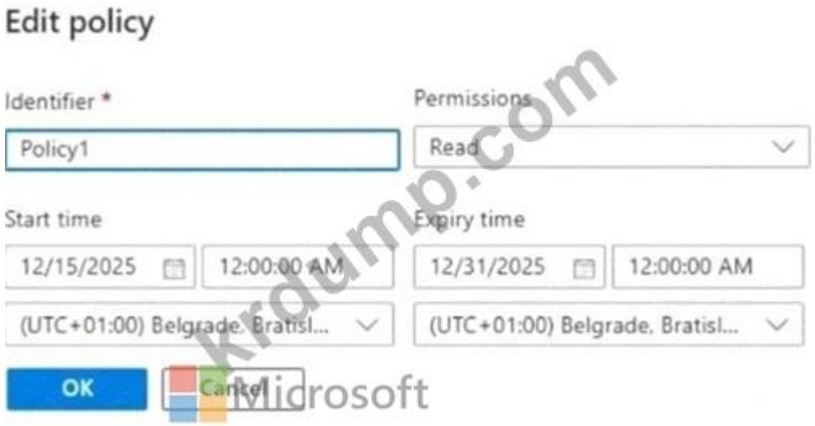
NEW QUESTION: 17
User2□ PIM□ □□□ □ □□□ □□□□ □□□.
□□ □□ □□□ □□ □□□?
A. User2□□ □□□ □□□ □□□ □□□□□.
B. contoso.com□ □□ □□ □□□ □□□□□.
C. contoso.com□ □□ ID □□ □□□ □□□□□.
D. User2□ □□ □□ □□ □□(MFA)□ □□□□□□.
Answer: D (LEAVE A REPLY)

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

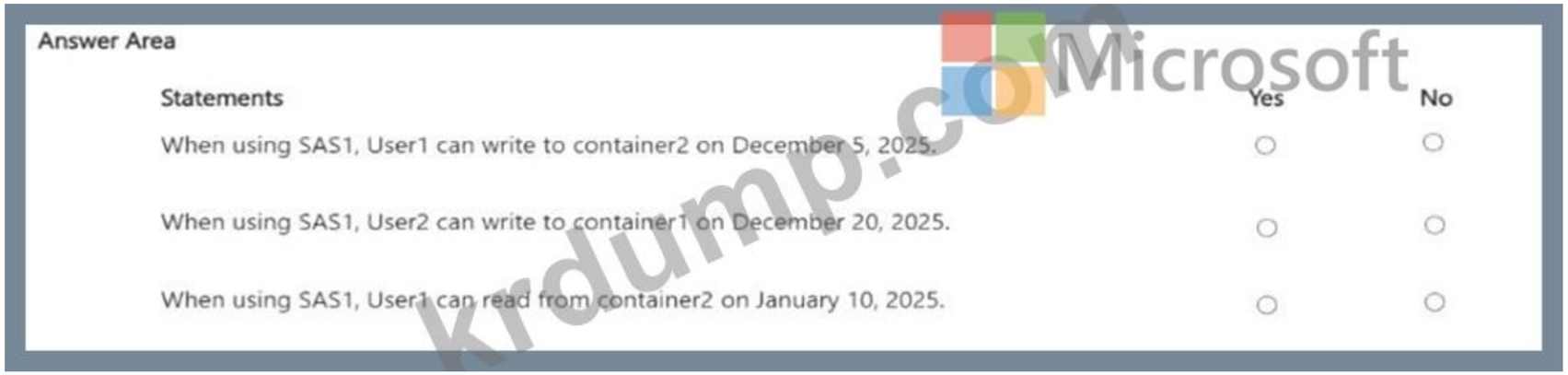
NEW QUESTION: 18
□□□1□ □□□2□□ □ □□ □□□□ □□ □□ □□□ Blob □□□□□ □□□ Azure □□□ □□□□.

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

Policy1□ □□ □□□ □□ □□□□□.



storage1 □□□□ SAS1□□□ □□□ □□ □□□ □□(SAS)□ □□□□.
* □□□ □□□: Blob
* □□□□ □□□ □□: □□□□
* □□□ □□: □□, □□, □□ □□, □□, □□
* Blob □□ □□ □□: □□ □□□ □□□□□.
* □□□ □□ □□□ □□: □□/□□
* □□□ □ □□□/□□:
□□□: 2025□ 12□ 1□
□□□: 2025□ 12□ 31□
□□□ MM/DD/YYYY □□□□□.
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.



Answer:

Answer Area

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

Explanation:

NEW QUESTION: 19

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

Name	Member of
Group1	*None*
Group2	Group1

□□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	Member of
User1	Group1
User2	Group2

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

Name	Assigned server admin	Database
sqlsvr1	User1	DB1
sqlsvr2	Group1	DB2

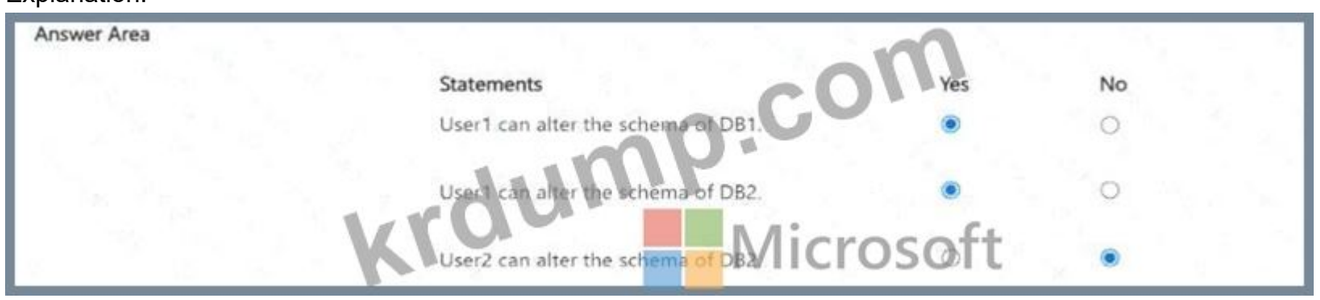
□□□ Microsoft Entra □□ □□□□ □□□□ □□□□.
□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.
□□: □□ 1□□ 1□□□□.

Answer Area

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

Answer:

Explanation:



NEW QUESTION: 20
AKS1□□□ □□□ Azure Kubernetes Service(AKS) □□□□□ □□□ Azure □□□ □□□□.
Azure DevOps Microsoft □□□ □□□□□ □□□□ □□□ □□□□ □□□□ □□□□ Azure □□□□ □□□□□□ □□□□.
□□□□ □□ □□□□□□□ AKS1□ □□□□ □ □□□ □□□□ □□□. □□□□ □□ □□□ □□□□□ □□□.
AKS1□ □□ □□□ □□□□ □□□?
A. □□□ IP □□ □□
B. □□□□□□ □□□□□ □□□□ □□□□(AGIC)
C. □□ □□□□□

D. □□ □□□□

Answer: (SHOW ANSWER)

NEW QUESTION: 21

Azure □□□ □□□□ □□□□.

user1□□ blob1□ □□ □□□ □□□ □□□□ □□□. □□□□ □□□ □□□ 6□ □□ □□□□□ □□ □□□.

□□□ □□□□ □□□?

A. □□ □□□ □□

B. □□ □□□ □□(SAS)

C. □□ □□ □□□ □□(RBAC)

D. □□□□ ID

Answer: B (LEAVE A REPLY)

Depending on how you want to authorize access to blob data in the Azure portal, you ' ll need specific permissions. In most cases, these permissions are provided via Azure role-based access control (Azure RBAC). For more information about Azure RBAC, see What is Azure role-based access control (Azure RBAC)?.

https://learn.microsoft.com/en-us/azure/storage/blobs/authorize-data-operations-portal

NEW QUESTION: 22

SQL1□□□ Azure SQL □□□□□□□ □□□ Azure □□□ □□□□.

App1□□□ □□□ □ □□ □□□ □□□□□.

App1□ SQL1□ □□ □□ □ □□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.

* □□□□□ □□□□ □□□ App1□ SQL1□ □□ □□□ □□□ □□□□□.

* □□ □□□ □□□ □□□□□.

* □□□ □□□ □□□□□□.

App1□ SQL1□ □□□□□ □ □□ □□□ □□□ □□□□ □□, App1□ □□ □□□□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □□ 1□□ 1□□□□.

Answer:

Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

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

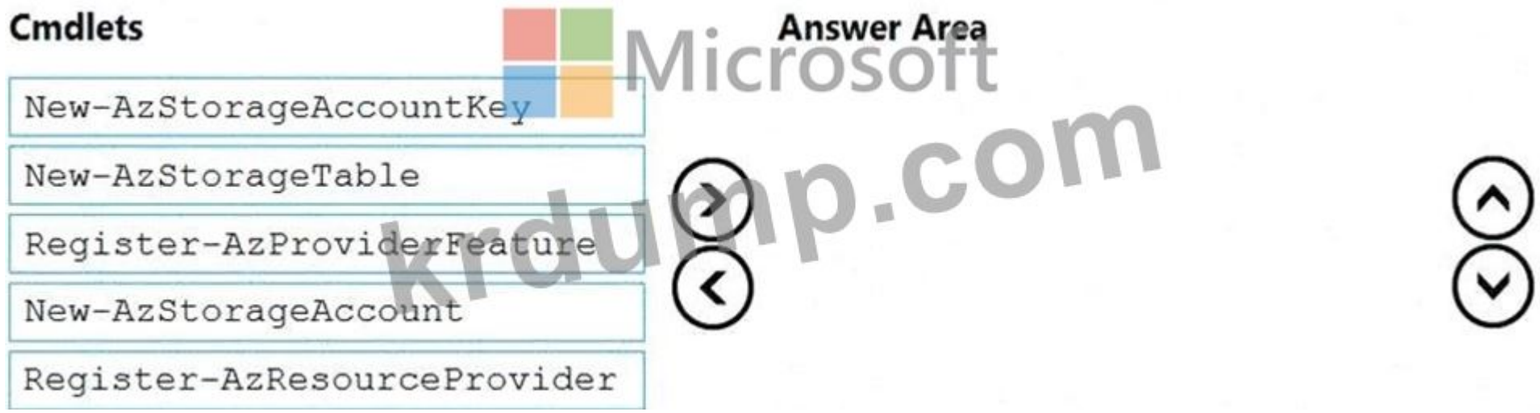
NEW QUESTION: 23

Azure □□□ □□□□.

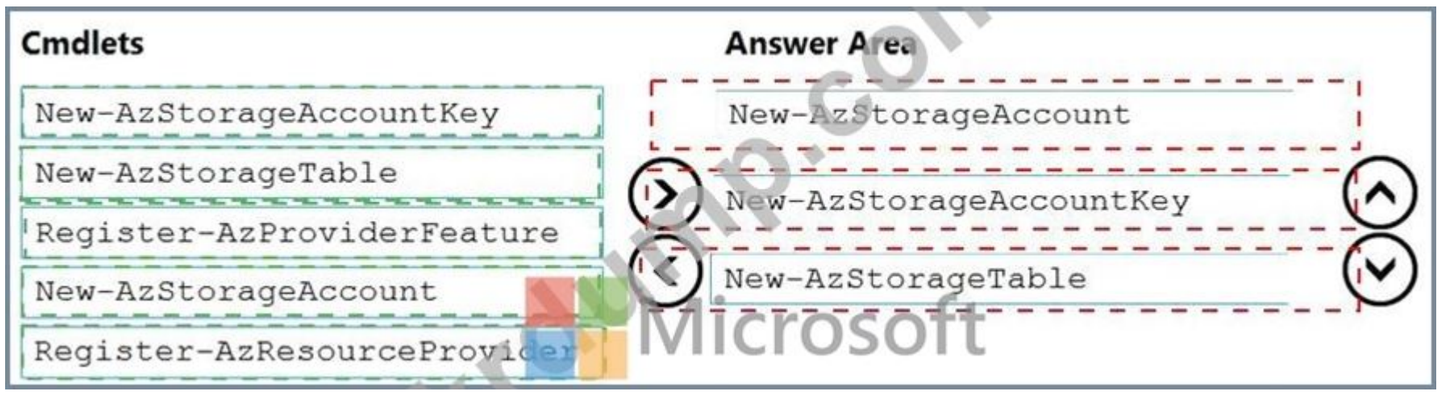
□□□ □□□ □□ □□□□□.

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

Azure Cloud Shell□□ □□ □ □□ cmdlet□ □□□□ □□□□ □□□? □□□□ cmdlet □□□□ □□ cmdlet□ □□ □□□□ □□ □□□ □□□□ □□□□□.



Answer:



Explanation:

Text, table Description automatically generated with medium confidence

Reference:

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

NEW QUESTION: 24

Azure □□□□ Vault1□□□ Azure Key Vault□ □□□□ □□□□. Vault1□ key1□□□ 2048□□ RSA □□ □□□□□□.

key1□ 90□□□ □□□□□ □□ □□□.

□□ □□ □□□ □□ □□□?

A. key1□ EC □□ □□ □□□□□.

B. □ □□ □□□ □□□□□.

C. Vault1□ Key Vault Premium□□ □□□□□□□□.

D. Vault1□ □□□ □□ □□□ □□□□□.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 25

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

□□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

RG1□□□ □□□ □□□ □□□□.

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

□□: □□ 1□□ 1□□□□.

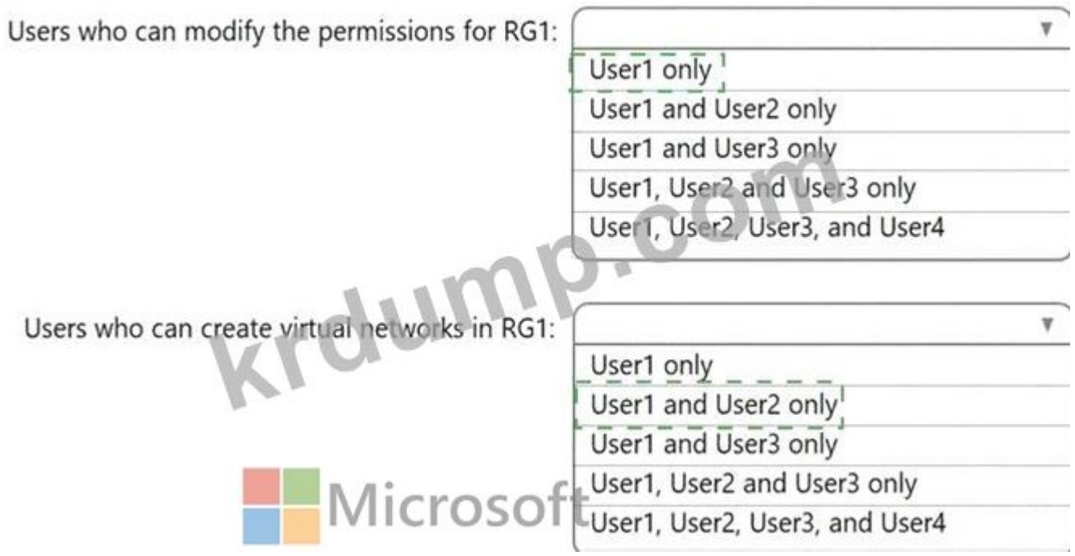
Users who can modify the permissions for RG1:

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

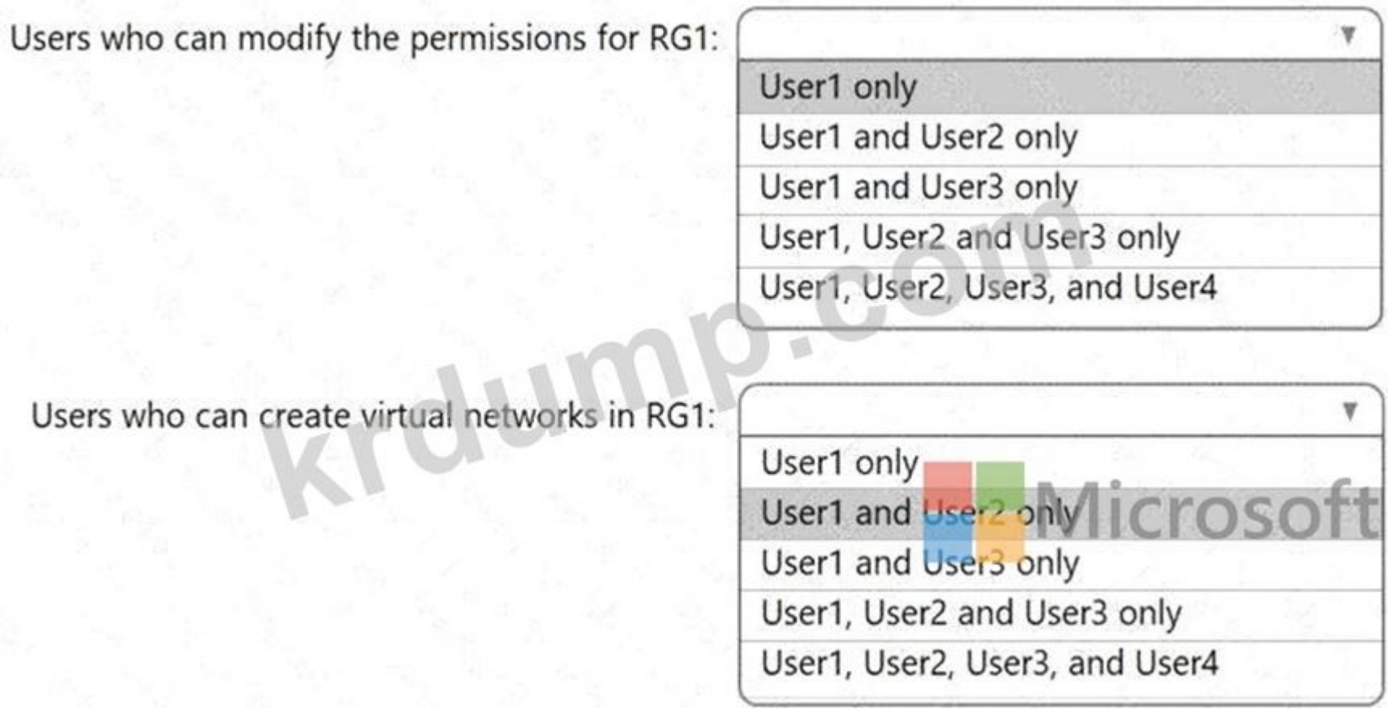
Users who can create virtual networks in RG1:

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

Answer:



Explanation:



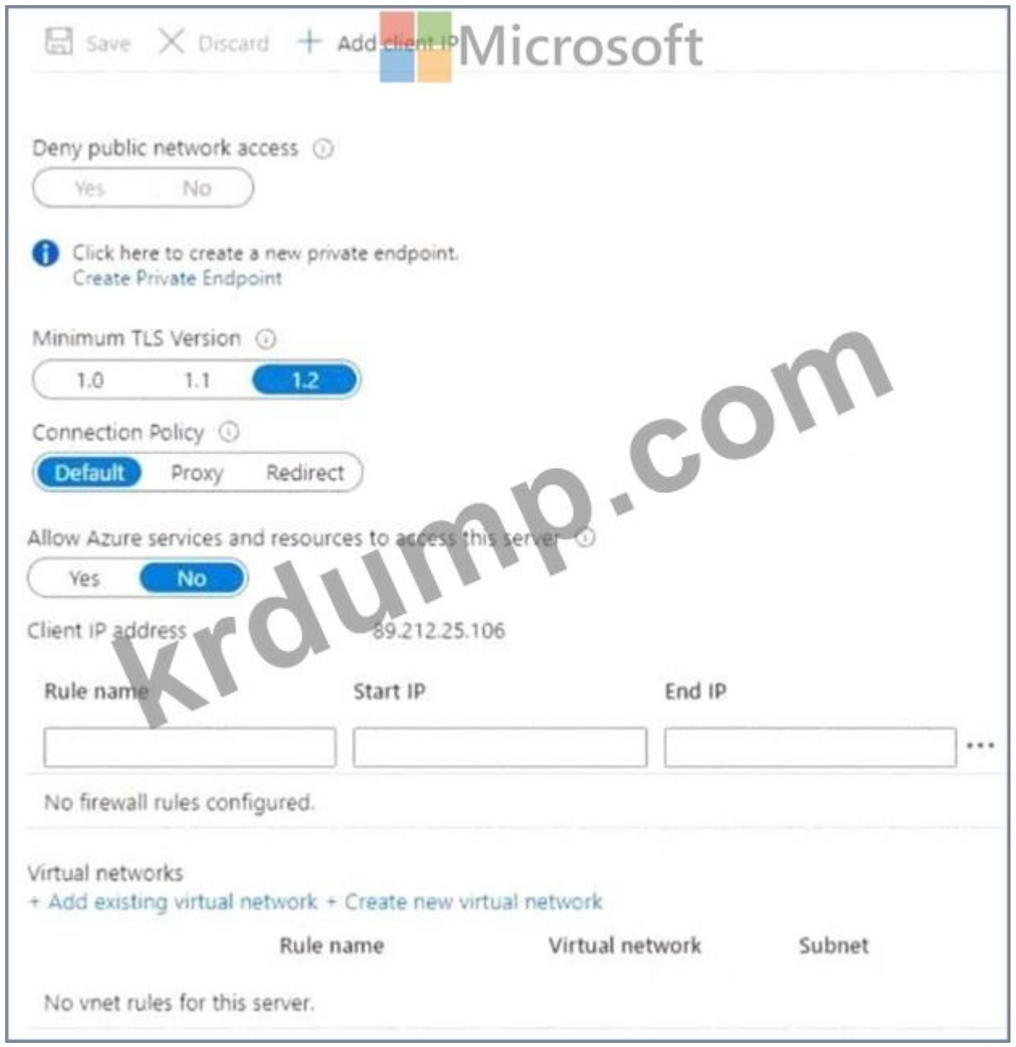
Box 1: Only an owner can change permissions on resources.

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

NEW QUESTION: 26

SQL!□□□ Azure SQL Database □□ □□□ VM1□□□ Azure □□ □□□ □□□ Azure □□□ □□□□. VM1□ □□ IP □□□ □□□□□.

SQL1□ □□□ □ □□ □□□□ □□□ □□ □□□ □□□□.



VM1□ SQL1□ □□□ □ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.

□□□ □□ □□□?

A. □□□ □□□ □□□ □□□□.

B. □□ □□ □□□□□ □□□□□.

C. □□ □□□ □□□□ □□□□□.

D. Azure □□□ □ □□□□ □ □□□ □□□□□□ □□□ □□ □□□□□.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 27

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

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

□□□□ □□ □□ □□□ □□□ □□□□□.

Name	Members
Group1	User1, User2, User3
Group2	User2

□□ □□□ □□□□ □□ □□ □□(MFA) □□ □□□ □□□□□.

* □□:
* □□: □□1
* □□2 □□

□□□: Azure MFA □□ □□

□□ □□: □□

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

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

Answer:

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

Explanation:

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

NEW QUESTION: 28

□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

Name	Type
RG1	Resource group
VM1	Virtual machine

□□ □□□ □□□□□.

Managed1□□□ □□□ □□□ ID□ □□□□.

Group1□□□ □□□ Microsoft 365 □□□ □□□□.

RG1□ □□ □□ □□□ □□□ □□□□□ □□ ID□ □□ □□□ □□□ □ □□□ □□□□ □□□. □□□ □□□□ □□□? □□ □□□□ □□□ □□□ □□□□ □□□□□. □□:
□□□ □□ □□□ □□□ 1□□ □□□□□.

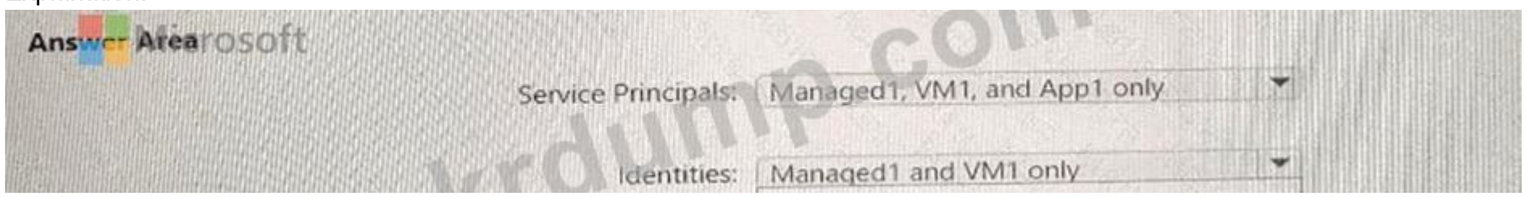
Answer Area

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: 29

□□ □□ □□□ □□□ Azure □□□ □□□□.

Amazon Web Services(AWS) □□□□□ □□□□. AWS □□□ Microsoft Defender for Cloud□ □□□□ □□□□.

□□ □□□□ □□ Azure □ AWS □□□□ □□ □□ □□□ □□ □□□□□ □□□ □ □□□ □□ □□□□ □□□□ □□□. □□ □□□□ □□ □□ □□□ □□□□ □□□.

* □□□ □□□ □□□□□ □□□□□□.

□□□ □□□□□□□.

□□□ □□□□□□□□?

A. Microsoft Sentinel□ AWS CloudTrail □□□□ □□ □□□□□.

B. AWS □□□□ □□ Azure Monitor □□□□□ □□□□ AWS □□ □□□ Microsoft Sentinel□ □□□□□.

C. Microsoft Defender for Endpoint□ Microsoft Sentinel□ □□□□□.

D. Microsoft Sentinel□ Microsoft Defender for Cloud □□□ □□□□ □□□□□.

Answer: (SHOW ANSWER)

NEW QUESTION: 30

Windows Server1□ Server2□ □□□□ □□ □□□□□ □□□ Server1, Server2, Server3□□□ □□□ □ㅓ□□□□ □□ 3□□ □□□□. Server3□ □ㅓ□□□□ □□□□□ □□□, □□ □□□ Azure□ □□□□ □ □□□□.

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

Azure Sentinel□ □□□□ Microsoft Defender □□□ □□□□ □□□□ □□□.

□□□ □□ □□□?

A. Server1, Server2 □ Server3□□ □□□ □□□ □□□□.

B. □ □□□ □□□□□ □□□ □□□□□□ □□□□□.

C. □ □□□ Microsoft Agent□ □□□□□.

D. Server1□ Microsoft Agent□ □□□□ Server2□ Server3□ □ㅓ□□□ □□□ □□□□□□ □□□□□.

Answer: C (LEAVE A REPLY)

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/connect-windows-firewall

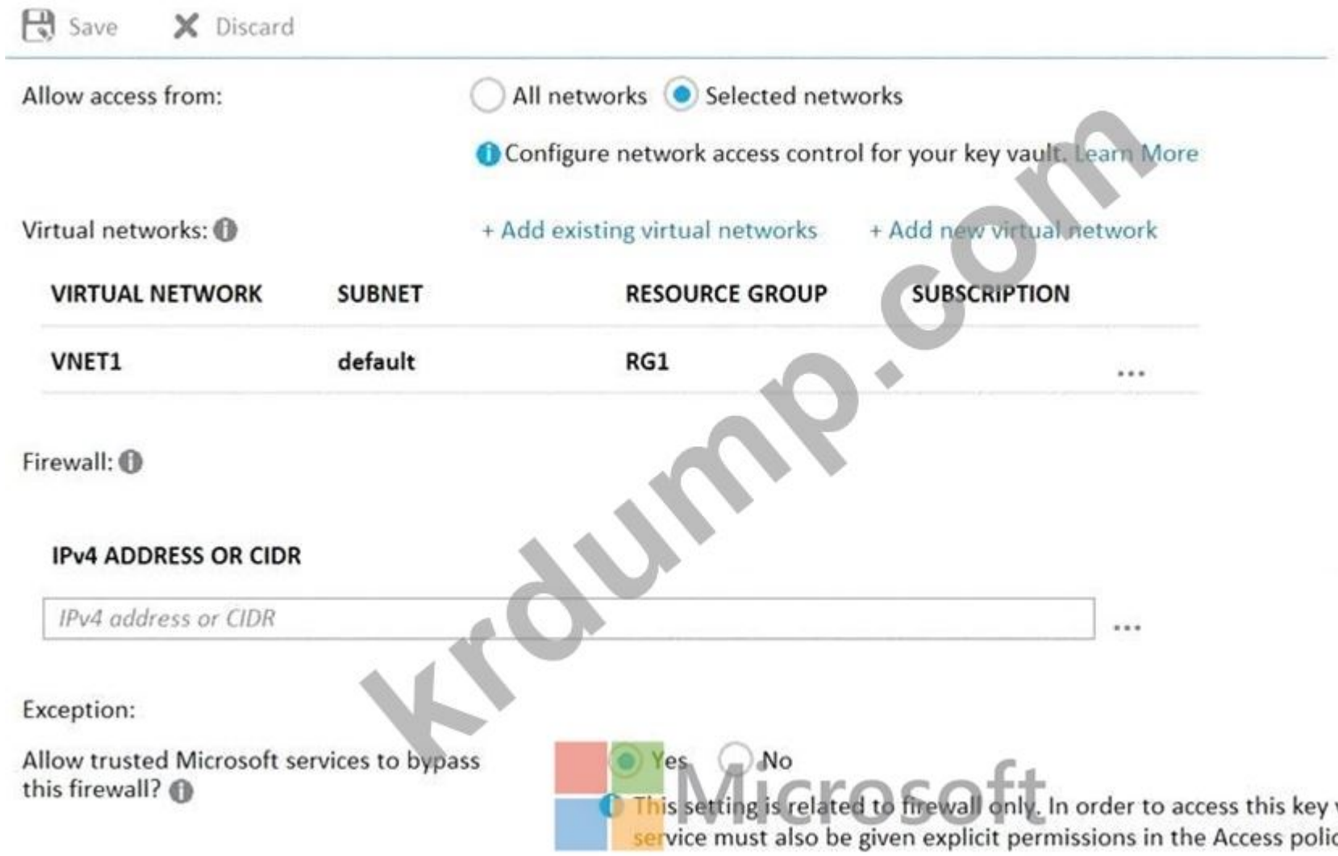
NEW QUESTION: 31

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

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

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

KeyVault1□ □□ □□□ □□ □□□□□.

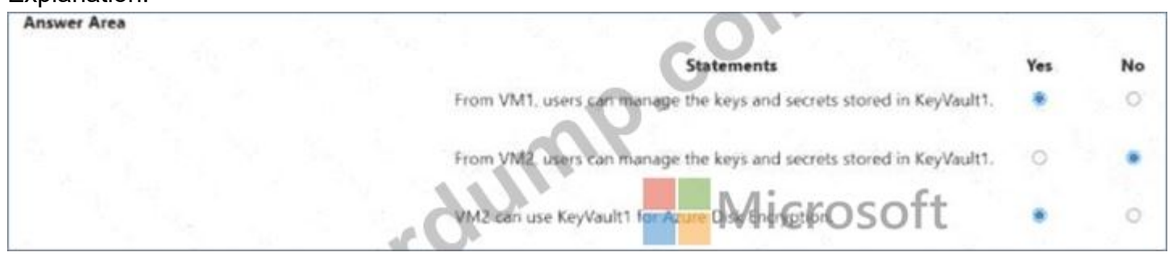


□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.

□□: □□ 1□□ 1□□□□.

Answer:

Explanation:



NEW QUESTION: 32

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

□+□□□□ ID□ □□ Azure AD□ □□□□ □, LAB□ □□□□ givenName □□□ □□ □□□□ Azure AD□ □□□□ □ □□□ □□□ □□ □□□.
□□ □ □□ □□□ □□□ □□□?

A. □□□ □□ □□□□ □□□□ □□ □□ □□□ □□□ □□□□ □□□.

B. □□□□□ DNAT □□□ □□□□ □□□.

C. □□□□□ □□□□ □□□ □□□ □□□ □□□□ □□□.

D. Active Directory □□□ □ □□□□ □□□□ □□ □□ □□□ □□□ □□□□ □□□.

Answer: A (LEAVE A REPLY)

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

Reference:

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

NEW QUESTION: 33

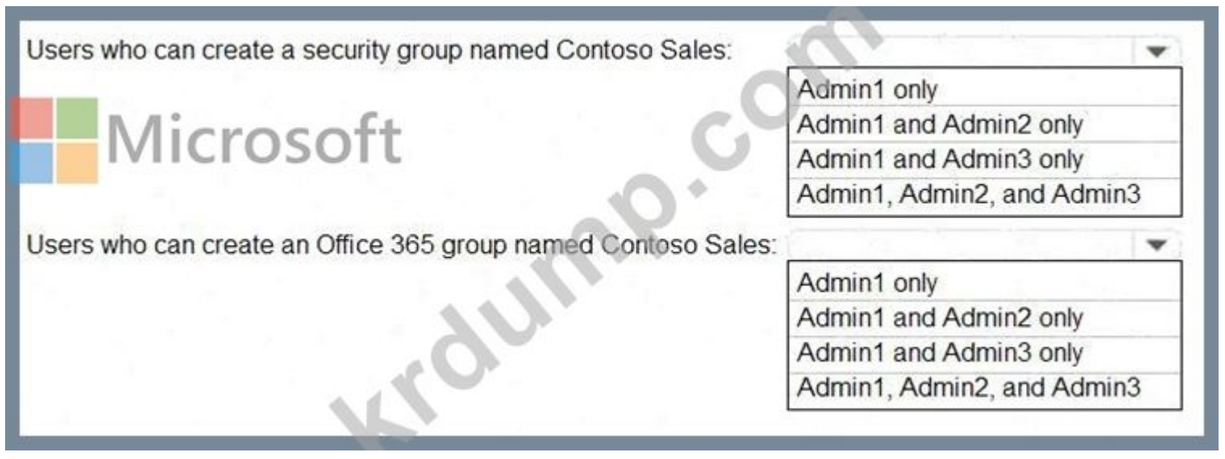
□□ □□ □□□ □□□□ □□□ contoso.com□□□ Azure Active Directory(Azure AD) □□□□ □□□□.

Name	Role
Admin1	Global administrator
Admin2	Group administrator
Admin3	User administrator

Contoso.com□□ □□ □□ □□□ □□□□ □□□□. □ □□□□ 'Contoso'□□ □□□ □□□□ □□□ □□ □□ □□ □□ □□□ □□□□.

contoso.com□□ Contoso Sales□□ □□□ □□ □ □□ □□□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □□ 1□□ 1□□□□.



Answer:

Users who can create a security group named Contoso Sales:

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

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

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

Explanation:

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

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

NEW QUESTION: 34
contoso.com□□□ Microsoft Enterprise □□□□ □□□ Azure □□□ □□□□. contoso.com□ App1□□□ □□□□□□□ □□□□□□. App1 □□□ Android □□□□□□□ □□□ □□□ □□□□ □□□. Azure □□□□ □□□ □□□□ □□□?
A. □□
B. □□□□□
C. □□ □□
D. □□□ □ □□
Answer: A (LEAVE A REPLY)

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

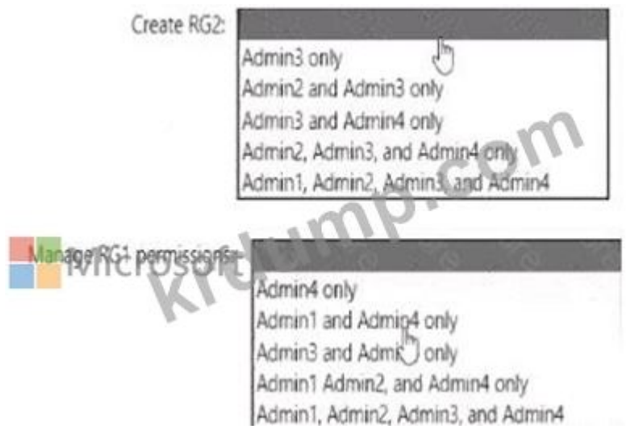
Name	Tier
GW1	Basic
GW2	Standard V2
GW3	WAF V2

URL □□□□ □□□□ SQL □□ □□□ □□□□□ □□□ □□□□ □□□.
□ □□ □□□ □□□□ □□□□□□ □□□□□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□. □□: □□□ 1□□□□.

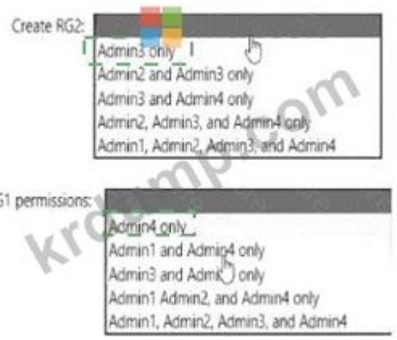
Answer:

Explanation:

NEW QUESTION: 36
RG2 □□ □ RG1 □□ □□□ □□□□ □□□. □ □□□ □□□ □ □□ □□□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□. □□: □□□ 1□□□□.

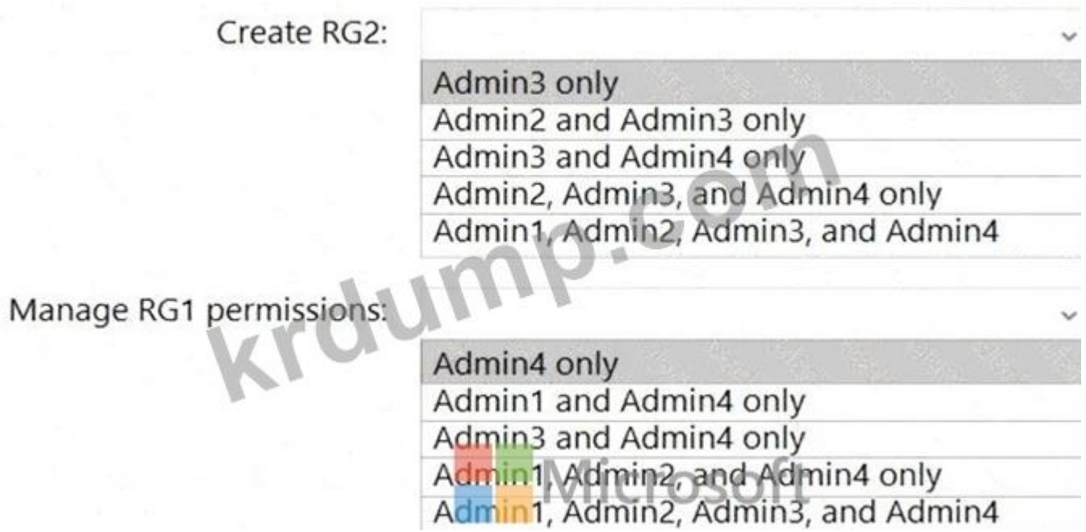


Answer:



Explanation:

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



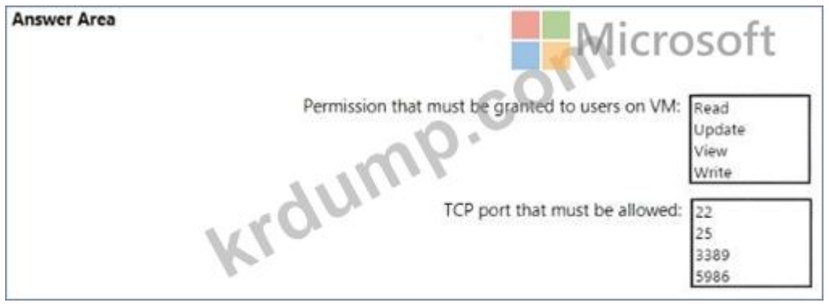
Box 1: Admin3 only

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

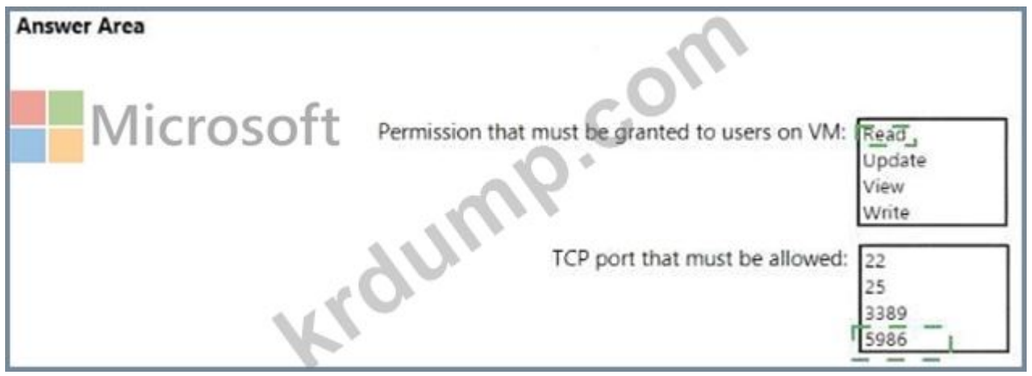
Box 2: Admin4 only

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

NEW QUESTION: 37
Azure □□ □□ □□□ □□ JIT(Just-in-Time) VM □□□□ □□□□ □□□□.
JIT VM □□□□ □□□□ □□□□□ □□ □□□ □□ PowerShell □□□ □□□ □□□□ □□□.
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.



Answer:



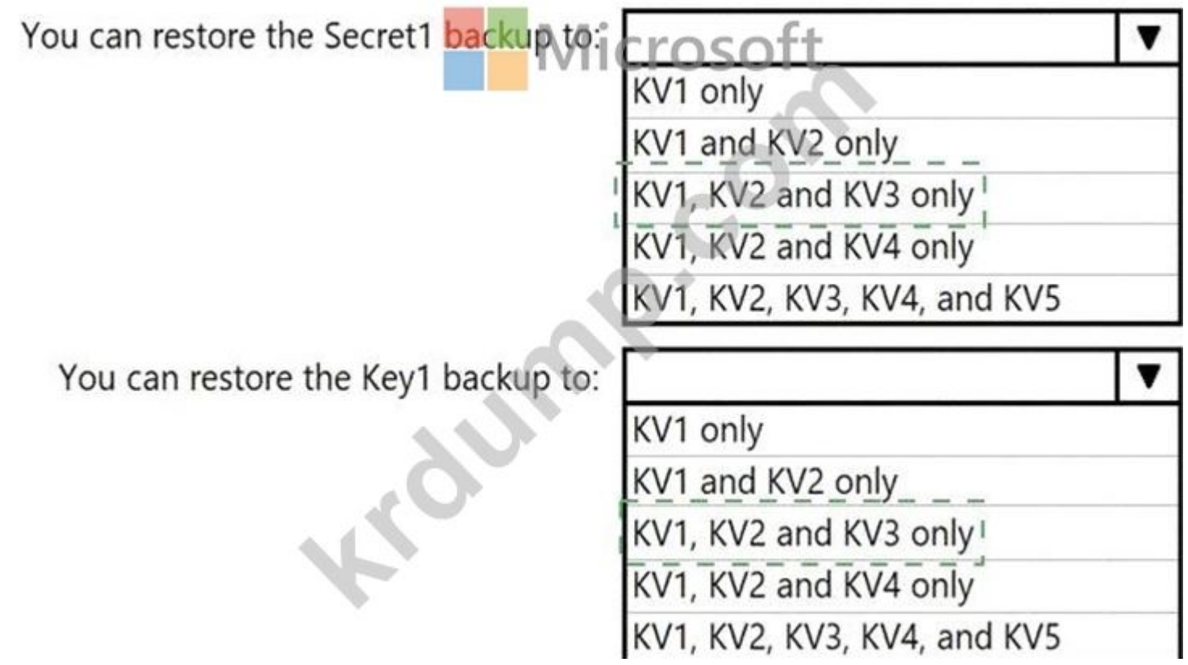
Explanation:
1. Read permission
2. 5986
https://docs.microsoft.com/en-us/azure/security-center/just-in-time-explained#what-permissions-are-needed-to-configure-and-use-jit

NEW QUESTION: 38
□□ □□□ Azure □ □□ □□ □□□ □□ □□□□.

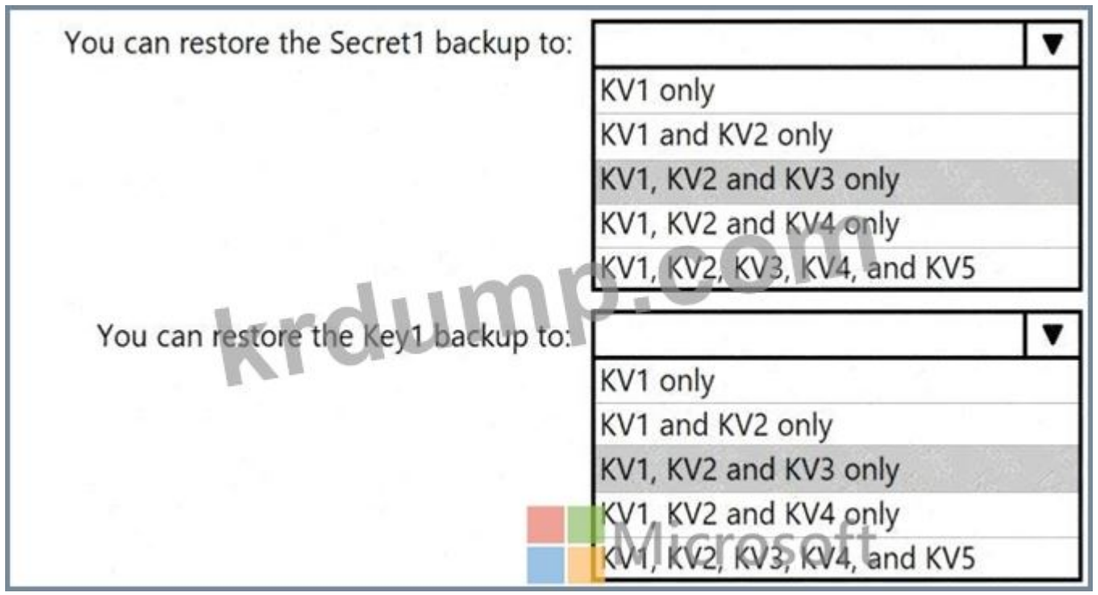
Name	Location	Azure subscription name
KV1	West US	Subscription1
KV2	West US	Subscription1
KV3	East US	Subscription1
KV4	West US	Subscription2
KV5	East US	Subscription2

KV1□ Secret1□□□ □□□ □□□ Key1□□□ □□□ □□□ □□□□ □□□ □□ □□ □□□□□.
Secret1□ Key1□ □□□□□.
□ □□□ □□ □ □□□□ □□□ □ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.

Answer:



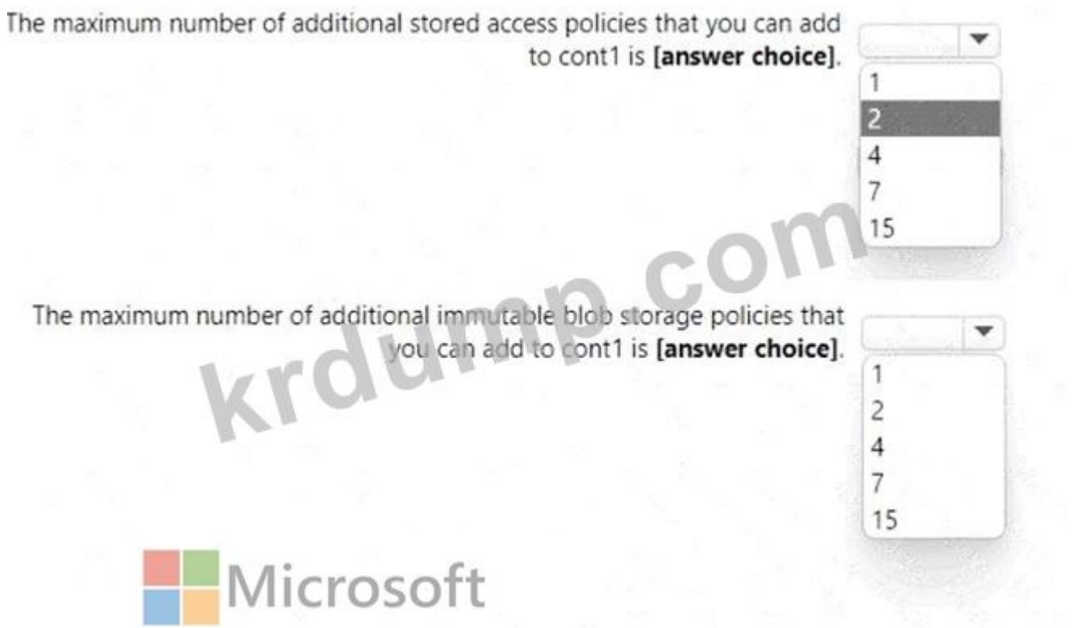
Explanation:



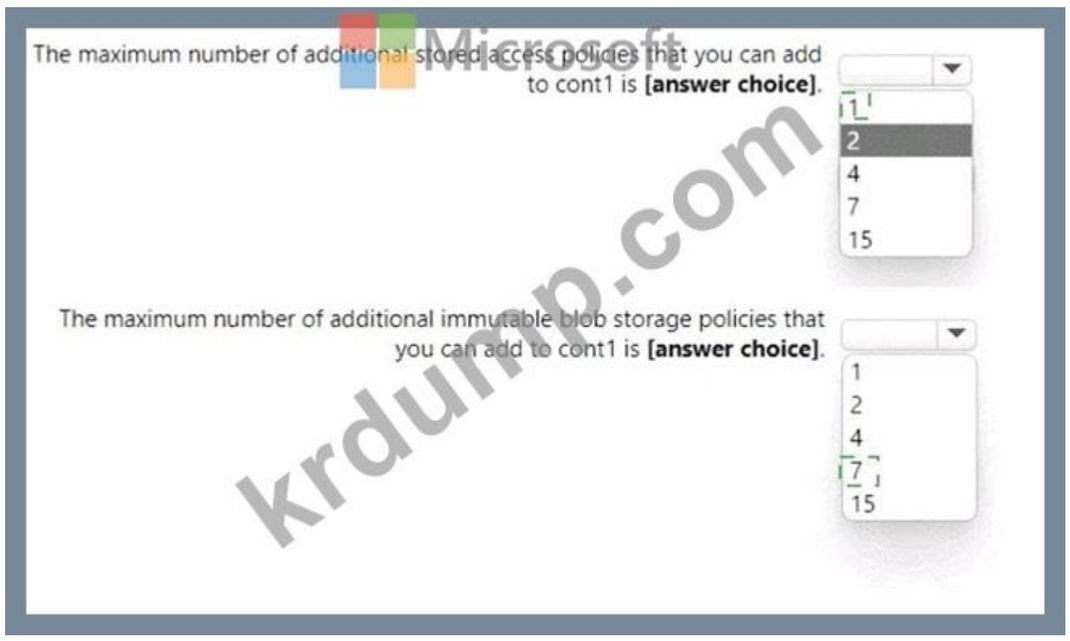
The backups can only be restored to key vaults in the same subscription and same geography. You can restore to a different region in the same geography.
https://docs.microsoft.com/en-us/azure/key-vault/general/backup?tabs=azure-cli

NEW QUESTION: 39
cont1□□□ Blob □□□□□ □□□ Azure □□□ □□□□. Cont1□□ □□ □□□ □□ □□□ □□□ □□□□.

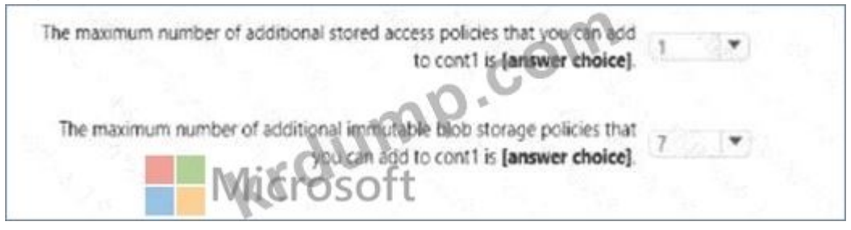
□□□□ □□□ □□□ □□□□ □ □□□ □□□□ □□ □□□ □□□□□ □□□□ □□□ □□□□□.



Answer:



Explanation:



NEW QUESTION: 40
100□□ □□ □□□ □□□ Azure □□□ □□ Azure Security Center Standard □□□ □□□□□ □□□□.
□ □□ □□□ □□□ □□□ □□□ □□□□□.
Azure Resource Manager □□□□ □□□□ □□□ □□□ □□□ □□ □□□ □□□□ □□□.
□□ □□□ □□ □□□□□ □□□□ □□□□□ □□□ □□ □ □□ □□□□ □□□? □ □□□ □□□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.
A. □□□□ □□□ □□ ID
B. □□□□□ □□□ □□ ID
C. □□ □□ ID
D. Azure Active Directory(Azure AD) ID
E. Key Vault □□□ □□□□ □□ □
F. □□ □□ □
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 41
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □ □ □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□□ □□□□.
Azure Active Directory(Azure AD)□ □□□□□ □□□ □□□□.
□□ □□□□□ Azure HDInsight □□□□□ □□□□.
□□□□ □-□□□□ Active Directory □□ □□□ □□□□ □□□□□ □□□□□ □□□ □□□□□.
□□□ □□□ □□□□□ □□□ □□□□ □□□.
□□ □□: Azure AD □□□□□□ □□□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)
Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.
Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:
* Create Azure Virtual Network.
* Create a custom DNS server in the Azure Virtual Network.
* Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.
* Configure forwarding between the custom DNS server and your on-premises DNS server.
Reference:
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

NEW QUESTION: 42
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □ □ □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□□ □□□□.
Azure Active Directory(AzureAD)□ □□□□□ □□□ □□□□.

□□ □□□□□ Azure HDInsight □□□□□ □□□□.
□□□□ □-□□□□ Active Directory □□ □□□ □□□□ □□□□□ □□□□□ □□□ □□□□□.
□□□ □□□ □□□□□ □□□ □□□□ □□□.
□□□: □□□□□ □□□ □□□□□□ □□□□□ □□□□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)
Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.
Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:
Create Azure Virtual Network.
Create a custom DNS server in the Azure Virtual Network.
Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.
Configure forwarding between the custom DNS server and your on-premises DNS server.
References:
https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

NEW QUESTION: 43
□□ □□□□ □□□□□ Sub1□□□ Azure □□□ □□□□. □ □□□□ □□ □□□□ □□□□ □□□□.
* Sub1□ □□ □□□ □□□ □□ 5□□ □□□.
* Azure □□□□ □□ □□□ □□□ □□ 10□□ □□□.
□□□ □ □□□ □□ □□ □□(MFA)□ □□□□□ □□□□□.
Sub1□ □□ □□ □□ □□□ □□ □□ □□□ □□□□□. (□□ □□ □□ □□□□□.) □□ □□□□ □□ MFA□ □□□□ □□□□□.
* Sub1□ □□ □□□ □□□ □□ 5□□ □□□.
* Azure □□□□ □□ □□□ □□□ □□ 5□□ □□□.
□□□ □□□ □□□ □ □□ □□□ □ □□□ □□□□□?
A. 14
B. 10
C. 5
D. 0
E. 7.5
Answer: E (LEAVE A REPLY)

NEW QUESTION: 44
Appl□□□ Azure □□□ □□□ Azure □□□ □□□□.
Appl□ □□ □□□ □□□ □□□ □□□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
* Windows □□□□□ App1□ □□ □□□□ □□□□□.
* □□□ □□□□ □□□ □□□ □□□ Appl□ □□□□□□ □□□□□.
□□ □□□ □□□ □□ □□□ □□□□ □□□? □□ □□□□ □□□ □□□ □□□ □□ □□□ □□ □□□□□□. □ □□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□. □□□□ □□□ □ □□□ □□ □□□ □□□□□□ □□□□□ □ □□ □□□□.
□□: □□ 1□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 45

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

□□□□ □□ □□□ □□□ □□□ □□□.

□□ □□□□ □□□□ □□□?

A. □□□2

B. □□□4

C. □□□1

D. □□□3

Answer: A (LEAVE A REPLY)

NEW QUESTION: 46

EASM1□□□ Microsoft Defender □□ □□ □□ □□(Defender EASM) □□□□ □□□ Azure □□□ □□□□. □□ □□ □□ □□□□□ □□□□□. □□□ □□ □□□□□ □□□□ □□□.

* □ □□ □□□□ □□ □□□□ □□ □□

* □ □□□ □□□
□□□□□ □□ □□□ □□□□ □□□?
A. □□□□ □□
B. □□ □□ □□
C. □□□ □□□
D. □□ □□ □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 47
Microsoft Entra □□ □□□ □□□□ □□ □□ □□□ □□□ □□□□ Microsoft Entra □□□□ □□□□.

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

Entra □□ □□ □□□ Azure AD □□□□ □□□ □□ □□□ □□ □□□ □□□ □□□ □□□□ □□□ □□□□□?
A. Admin2 □ Admin3□ □□
B. Admin1. Admin2, Admin3. □ Admin4
C. Admin2 □ Admin4□ □□
D. Admin2, Admin3, Admin4□ □□
E. Admin1□
F. Admin1, Admin2, Admin3□
Answer: F (LEAVE A REPLY)

NEW QUESTION: 48
storage 1□□□ □□□ Azure Storage □□□ □□ □□□□□.
storage1□ □□ □□□□ □□ □□□ □□ □□□□ □□□□ □□□□□ □□□. □□, □□ □□□ □□□□□ □□□□□□ □□□.
storage1□ □□□ □ □□□ □□□□ □□□?
A. □□□ □□ □□
B. □□□ □□□ □□
C. □□ TLS □□
D. □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 49

Microsoft Defender□ □□□□ Azure □□□ □□□□.
□□□ □□□□ □□□□ CIS Microsoft Azure Foundations Benchmark v2.0.0□ □□□□□□.
□□□□ □□□ □□ □□ □□ □□□ □□(RBAC) □□□ □□□□□ □ □ □□ □□□□ □□□ □□□ □□□ □□ □□ □□□□ □□□□□ □□ □□□. □□□□ □□ □□□ □□□ □□□ □□□ □□ □□□.
□□□ □□□□ □□□?
A. □□□ □□ □□
B. □□□ □□
C. □□□ □□□ □□□
D. □□□ □□ □□□ □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 50
□□ □□ □□□ □□ □□□ □□□ Azure □□□ □□□□.

Name	Azure region	Connected to	Associated network security group (NSG)
VM1	West US	VNET1/Subnet1	None
VM2	West US	VNET1/Subnet2	NSG2
VM3	Central US	VNET2/Subnet1	NSG3
VM4	West US	VNET3/Subnet1	NSG4

VNET1, VNET2, VNET3□ □□ □□□□□ □□□□. □□ □□□ □□□□□.
* □□ □□ □□□ ASG1□ ASG2□□ □ □□ □□□□□□ □□ □□□ □□□□.
* VM1□ □□□□ □□□□□□ ASG1□ □□□□□.

Answer Area

ASG1:

ASG2:

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

NEW QUESTION: 51
□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

Name	Type
VM1	Virtual machine
VNet1	Virtual network
AFW1	Azure firewall

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

A. SNAT □□ IP □□ □□

B. □□□□ □□

C. DNAT □□

D. □□ □□□□ □□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 52

Admin1□□□ □□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□. Admin1□□□ □□□□□□ □□□ □□□ □□□□□□□.
App1□□□ □□□□ □□ □□□□ Azure AD□ App1□ □□□□□.
Admin1□ App1□ □□ □□ □□□□ □□□□□ □□□ □□□ □ □□□ □□□□□.
Azure Portal□□ Admin1□ App1□ □□ □□ □□□□ □□□□ □ □□□ □□□□ □□□.
□□□ □□ □□□?

A. App1□ □□ □□□□ □□□□□□.

B. App1□ API □□□ □□□□□.

C. App1□ □□□□□□ □□□□□□□□ □□□□□.

D. Admin1□□ □□□□ □□□□□□ □□□ □□□ □□□□□.

Answer: A (LEAVE A REPLY)

This is a tricky one because uploading a certificate is also required. However, the question states that the Token Encryption option is unavailable. This is because the app is not added as an enterprise application.

When the app is added as an enterprise application, the Token Encryption option will be available. Then you can upload the certificate.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/howto-saml-token-encryption

NEW QUESTION: 53

□□ □□ □□□ □□ □□□□□ □□□ Azure □□□ □□□□.
□□□□ □□ □□ □□□ □□ □□□ □□□□ □□□□.
□□ □□□□ □□□ contoso2024□□ □□□□ □□□ □□□□.

* File1□□□ □□□ □□□ □□□□ Contained□□ □□□ □□□□
* File2□□ □□□ □□□ □□□□ Share1□□□ □□□ □□ □□

□□ □□□ □□ contoso2024□ □□ □□ □□□□□□ □□□□□.

Create a private endpoint

Validation passed

✓ Basics ✓ Resource ✓ Virtual Network ✓ DNS ✓ Tags 6 Review + create

Basics

Subscription	Azure Pass - Sponsorship
Resource group	RG1
Region	East US
Name	PE1
Network Interface Name	PE1-nic

Resource

Subscription ID	a45b7def-a1cc-4700-afeb-80f3df1585fd (Azure Pass - Sponsorship)
Link type	Microsoft.Storage/storageAccounts
Resource group	RG1
Resource	contoso2024
Target sub-resource	blob

Virtual Network

Virtual network resource group	RG1
Virtual network	VNet2
Subnet	Subnet21
Network Policies	Disabled
Application security groups	None

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

Answer Area

Statements	Yes	No
From VM1, you can access File1 by using a private IP address.	○	○
From VM2, you can access File1 by using a private IP address.	○	○
From VM2, you can access File2 by using a private IP address.	○	○

Answer:

Answer Area

Statements	Yes	No
From VM1, you can access File1 by using a private IP address.	○	○
From VM2, you can access File1 by using a private IP address.	○	○
From VM2, you can access File2 by using a private IP address.	○	○

Explanation:

Answer Area

Statements	Yes	No
From VM1, you can access File1 by using a private IP address.	○	●
From VM2, you can access File1 by using a private IP address.	○	●
From VM2, you can access File2 by using a private IP address.	○	●

NEW QUESTION: 54

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

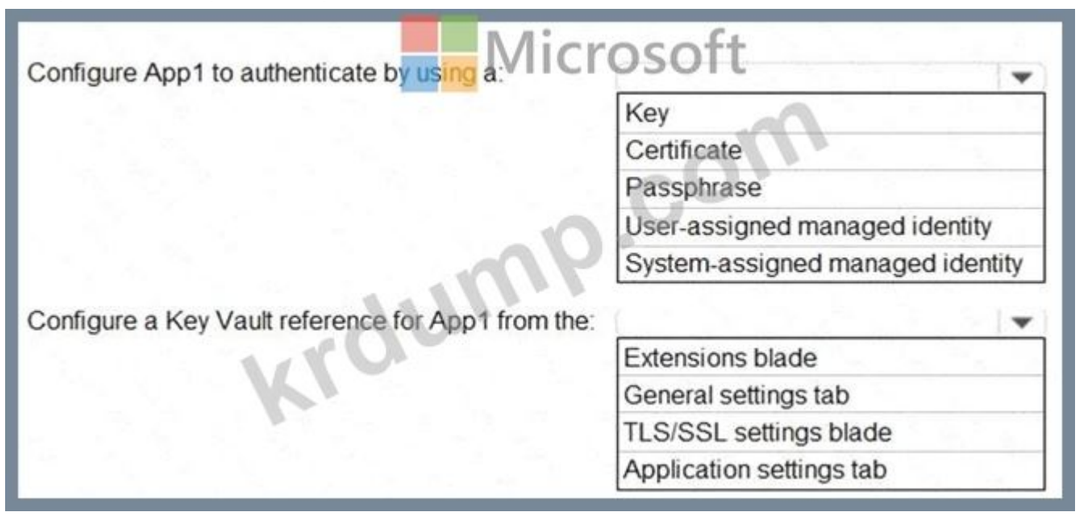
Name	Type	Category
Initiative1	Initiative definition	Security Center
Initiative2	Initiative definition	My Custom Category
Policy1	Policy definition	Security Center
Policy2	Policy definition	My Custom Category

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

□□□ □□□□ □□□?
A. Policy1 □ Policy2□
B. □□□□□1□
C. Initiative1 □ Initiative2□
D. □□□□□1, □□□□□2, □□1, □□2
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/security-center/custom-security-policies

NEW QUESTION: 55
webapp1□□□ Azure □□□ □□□□.
Azure Repo□ □□□□ webapp1□ □□ □□□□ □□□ □□□□ □□□.
□□ □□ □□□ □□□□ □□□?
A. Azure DevOps □□
B. Azure Storage □□
C. Azure Application Insights □□□
D. Azure DevTest Labs □
Answer: A (LEAVE A REPLY)

NEW QUESTION: 56
App1□□□ □□□ Vault1□□□ Azure Key Vault□ □□□ Azure □□□ □□□□.
Vault1□ □□□ □□□□ □□□□□□ App1□ □□□□ □□□.
App1□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.

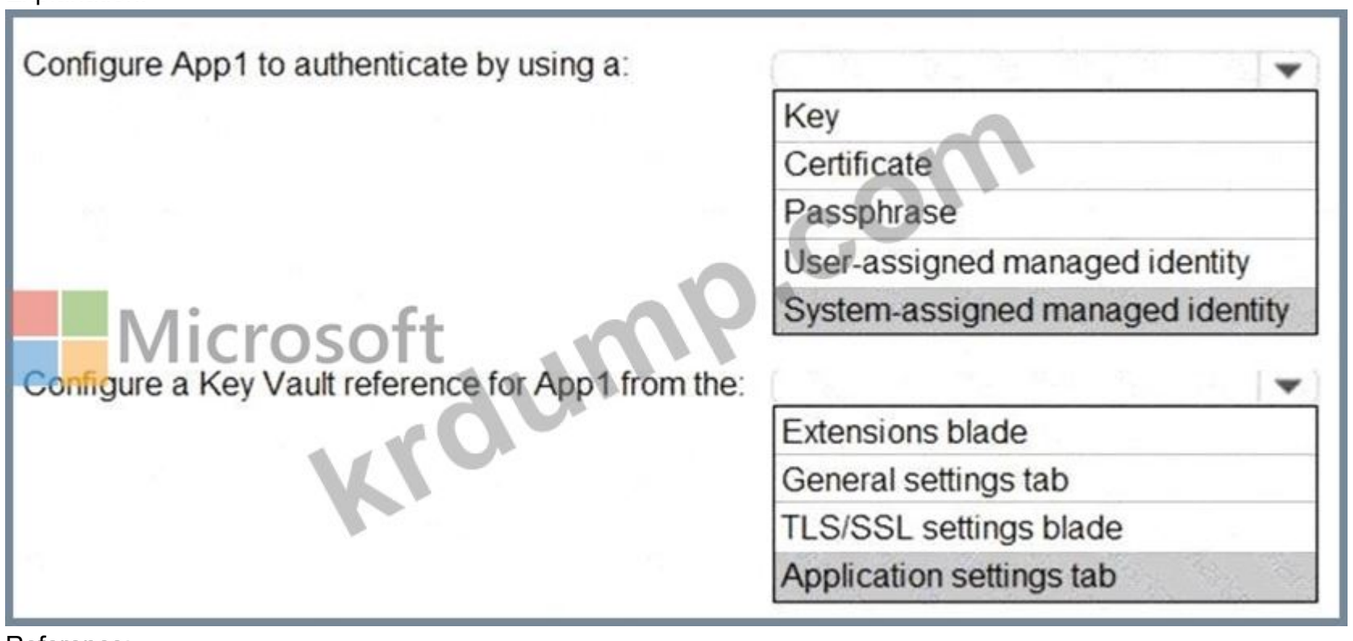


Answer:

Configure App1 to authenticate by using a: [Key / Certificate / Passphrase / User-assigned managed identity / System-assigned managed identity]

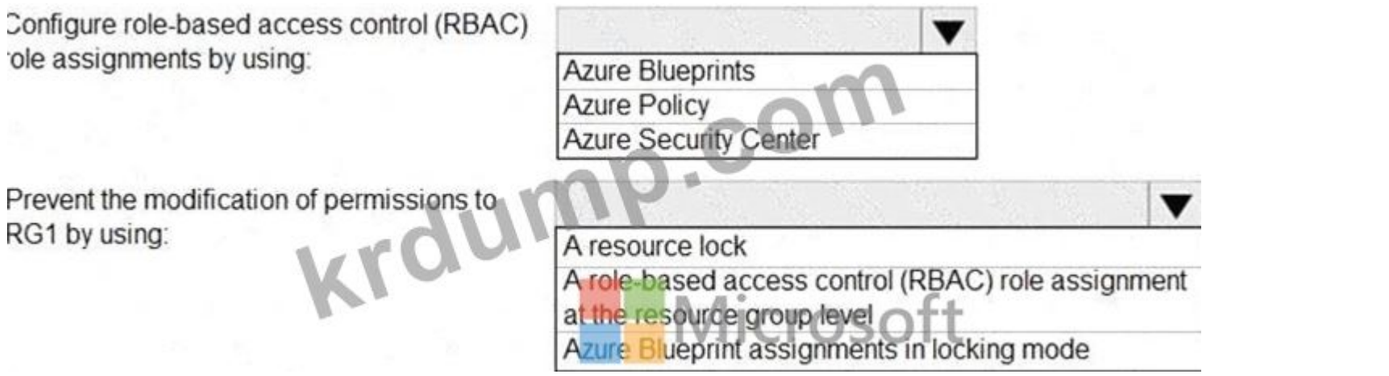
Configure a Key Vault reference for App1 from the: [Extensions blade / General settings tab / TLS/SSL settings blade / Application settings tab]

Explanation:

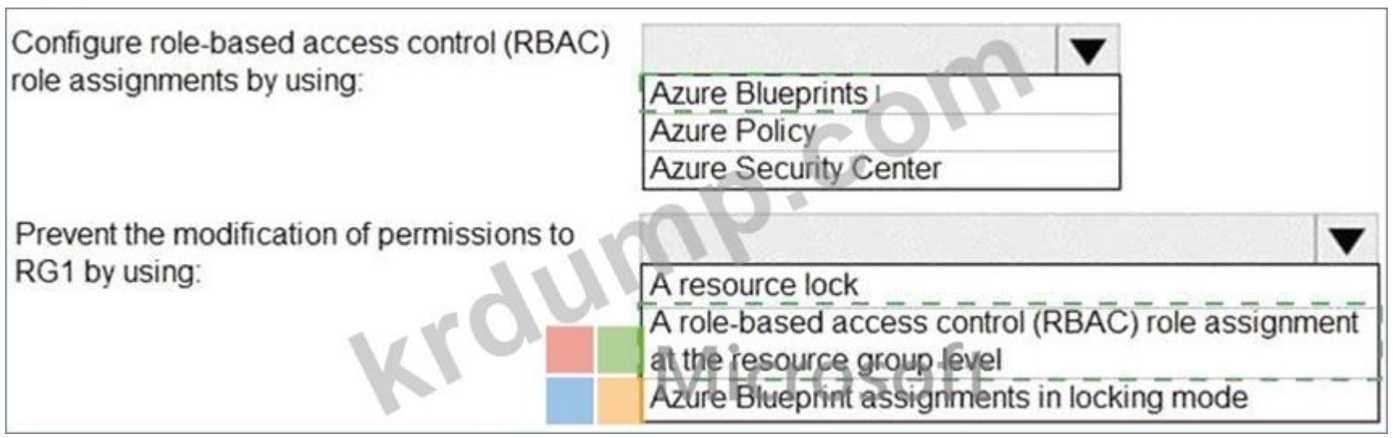


Reference:
https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity?tabs=dotnet

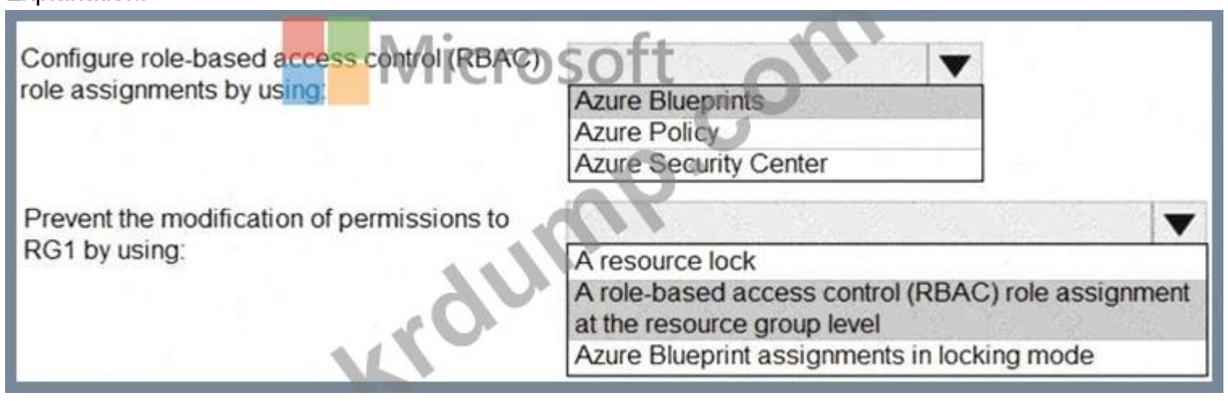
NEW QUESTION: 57
Azure □□ 20□□ Group1□□□ □□ □□□ □□□□. □ □□□ □□ □□ □□□ □□□□□.
□ □□□□ RG1□□□ □□□ □□□ □□□□ □□□□.
□ □□□ □□ RG1□ □□ □□ □□□ □□□□□ □□□□ □□□.
* □□1□ □□□□□ □□□ □□□ □□□□□.
* RG1□ □□ □□ □□□ □□□□□.
□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□□ □□□□□.
□□: □□ 1□□ 1□□□□.



Answer:



Explanation:



NEW QUESTION: 58

Azure Key Vault□ □□□ Azure □□□ □□□□.

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

□□□ □□□□ □□□?

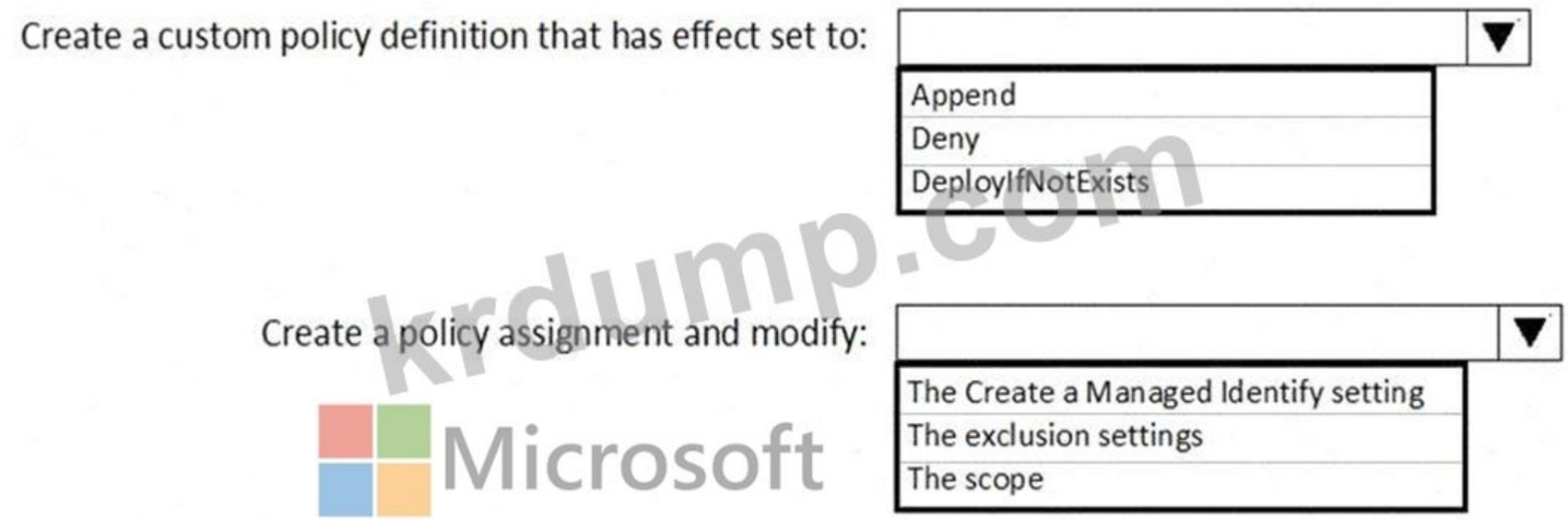
A. Key Vault □□

B. Azure □□

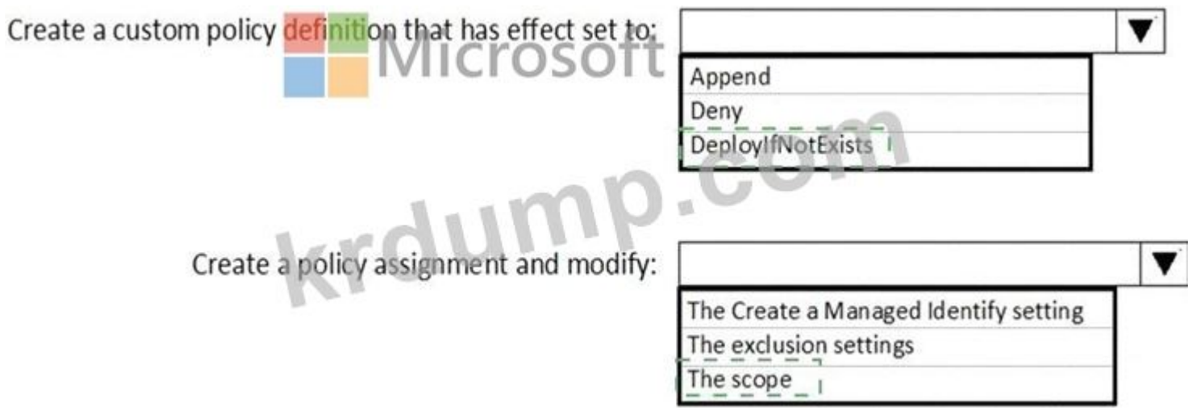
C. Azure Purview

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

NEW QUESTION: 59
□□□ □□ □□ □□□ □□□□□ Microsoft Antimalware□ □□□□ □□□.
□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□□ □□□□□.
□□: □□ 1□□ 1□□□□.



Answer:



Explanation:
1. DeployifNotExists
2. Scope
Topic 2, Contoso
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

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

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

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

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

Sub1
Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.
User2 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

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

Sub1 contains the Azure policies shown in the following table.

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

Sub2

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

Sub2 contains the virtual machines shown in the following table.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Contoso identifies the following technical requirements:

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

NEW QUESTION: 60

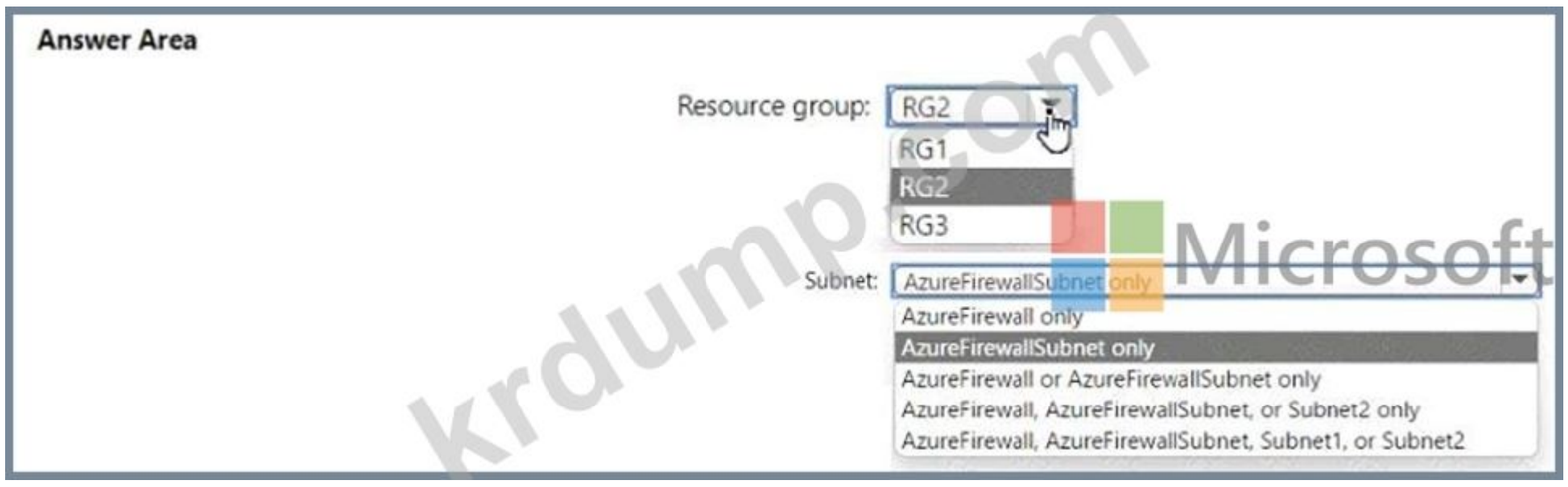
□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

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

VNet1□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

Azure Portal□ □□□□ AzFW1□□□ Azure □□□□ VNet1□ □□□ □□□□□.
AzFW1□ □□□□ □ □□□ □ □□ □□□ □□□ □□□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.



Answer:

Explanation:

NEW QUESTION: 61
□□□ □□
□□ 2
VNETOI-Subnet0-NSG □□□□ □□ □□(NSG)□ NetworkSecurityGroupRuleCounter □□□ □□ □□□□ logs31330471 Azure Storage □□□ 30□ □□ □□□□□ □□ □□□.
Answer:

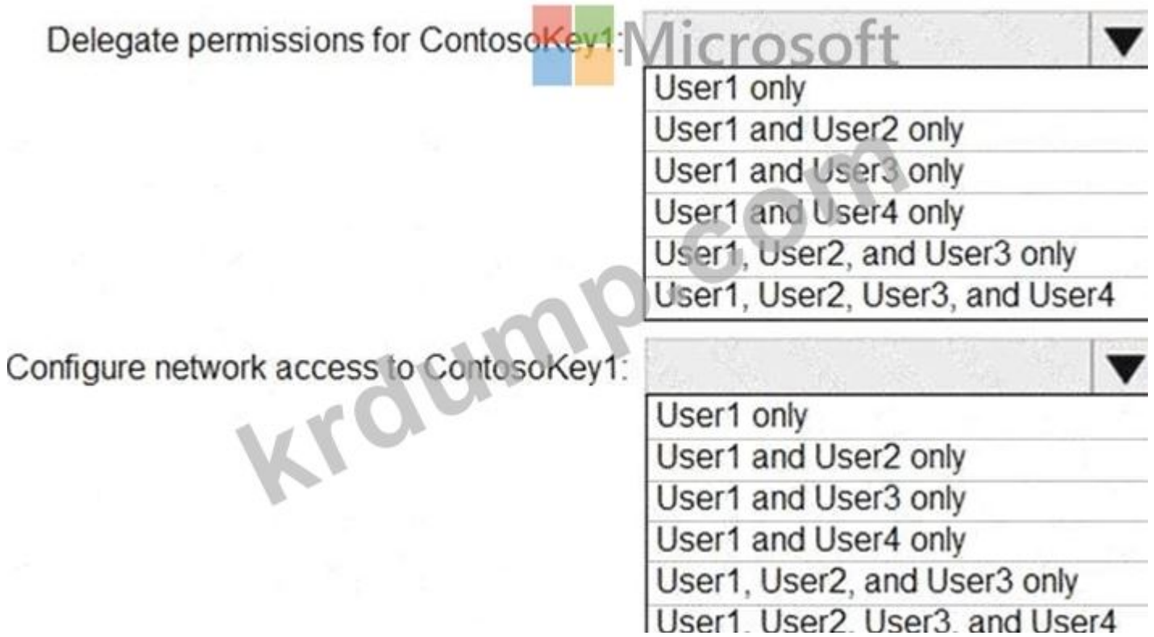
see the task answer with step by step below:
* Enable diagnostic resource logging for the NSG. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to select the Rule counter category under Logs and choose the logs31330471 storage account as the destination.
* Configure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

NEW QUESTION: 62
User1□□□ □□□□ □□□ Microsoft Entra □□□□ □□□□.
□□□□ □□ □□ □□ □□□ □□□□ □□□□□.
User1□ □□ □□ □□□ □□□□ □ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
User1□□ □□ □□□ □□□□ □□□?
A. □□ □□□
B. □□ □□□
C. □□□ □□ □□ □□□
D. □□□ □□□
Answer: A (LEAVE A REPLY)

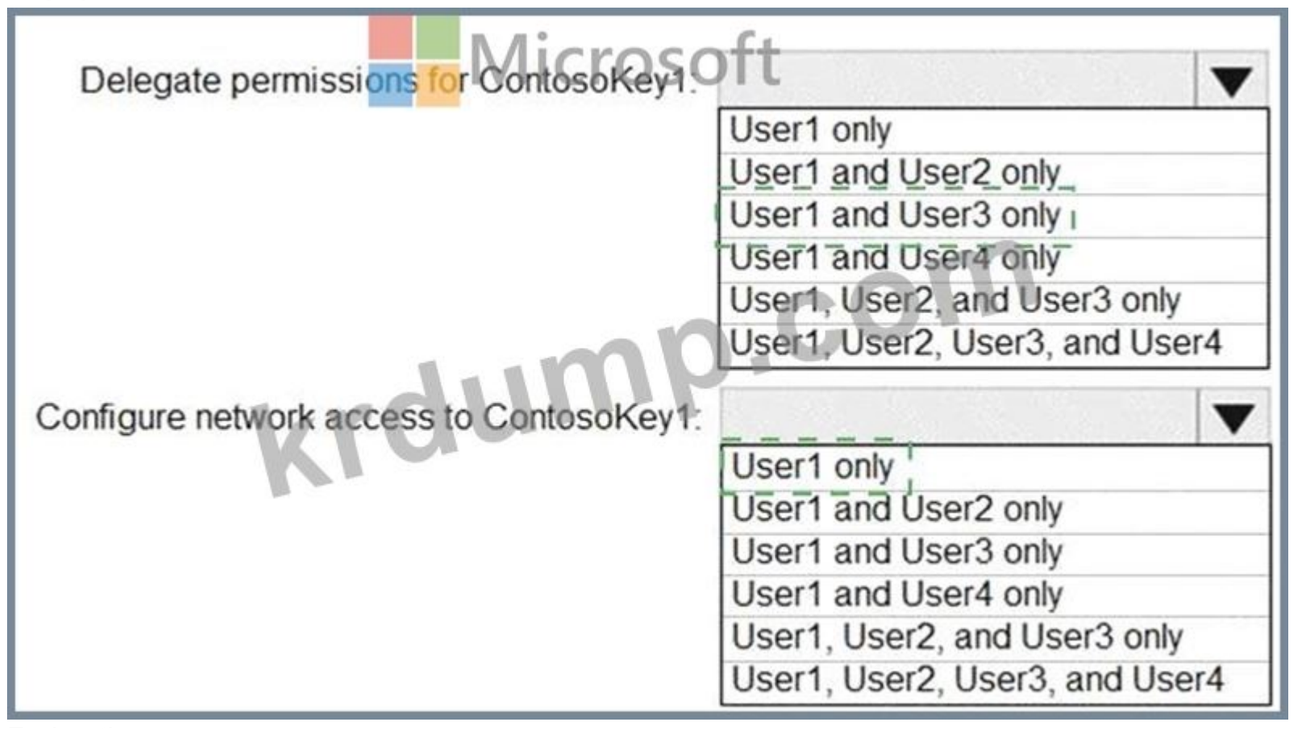
NEW QUESTION: 63
ContosoKey1□□□ Azure Key Vault□ □□□ Azure □□□ □□□□.
□□ □□ □□□ □□ □□□□ □□□ □□□ □□□□□.

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

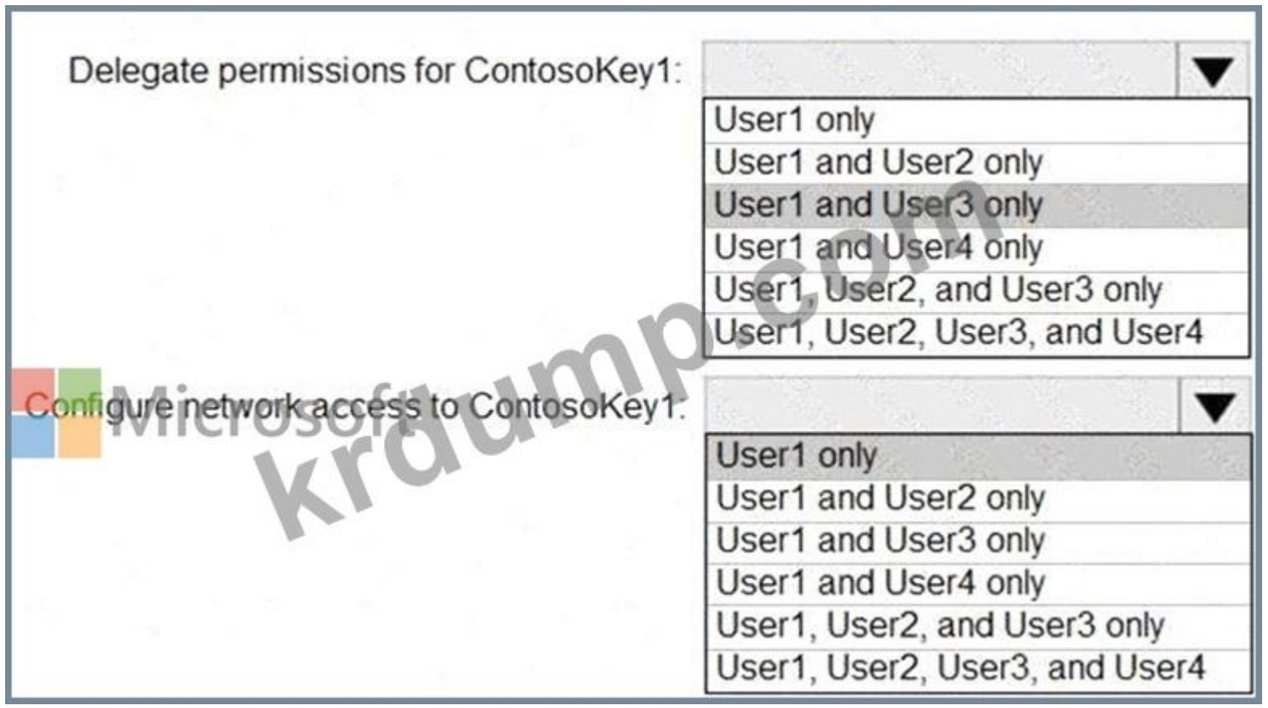
□□ □□□ □□□ □ □□ □□□□ □□□□ □□□.
* ContsosKey1□ □□ □□□ □□□□□.
* ContosoKey1□ □□ □□□□ □□□□ □□□□□.
□□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.



Answer:



Explanation:



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

NEW QUESTION: 64
App1□□□ Azure App Service □, AC1□□□ Azure □□□□ □□□□, storage1□□□ □□□ □□□ □□□ Azure □□□ □□□□. AC1□ App2□□ □□ □□□□□□.
□□□□ https:/app1.contoso.com/echo/resource-cache? param1 URL□ □□□□ App1□ □□□ □□□□.
=□□. App1□ App2□ □□□□, App2□ storage1□□ □□□□ □□□□□.
□□□□□ IP □□□□ □□□ □□□□ □□ □□□ □□□□□ □□□□ □□□. □□ Microsoft Defender for Cloud □□□□ □□□□ □□□?
A. API□ Microsoft Defender
B. □ □□□□ Microsoft Defender
C. □□□□□ Microsoft Defender
D. □□□□ Microsoft Defender
Answer: (SHOW ANSWER)

NEW QUESTION: 65
500□□ □□□□ AU1□□□ □□ □□□ □□□ Azure AD □□□□ □□□□.
Azure Active Directory □□ □□□□ □□ □□□ □□□ □□□□ AU1□ □□□□ □□□ □□□□□.
□□ □□□ □□□□ □□□ □□□ □□□□□ □□□.
□□□ □□□ □□□□ □□□?
A. □ □□□□ UPN(□□□ □□ □□) □ □□ □□□
B. □ □□□□ □□ □□□□
C. □ □□□□ □□□ □□ □□(UPN)□
D. □ □□□□ □□□ □□ □□(UPN) □ □□ □□□□

E. □ □□□□ □□ □□□

Answer: (SHOW ANSWER)

NEW QUESTION: 66

□□ □□□ □□□□ File1.yaml□□□ □□□ □□□□.

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

File1.yaml□ □□□□ container1□□□ Azure □□□□ □□□□□ □□□□.

Variable1□ Variable2□ □□ □□□ □ □□ □□□ □□□□ □□□.

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

□□: □□ 1□□ 1□□□□.

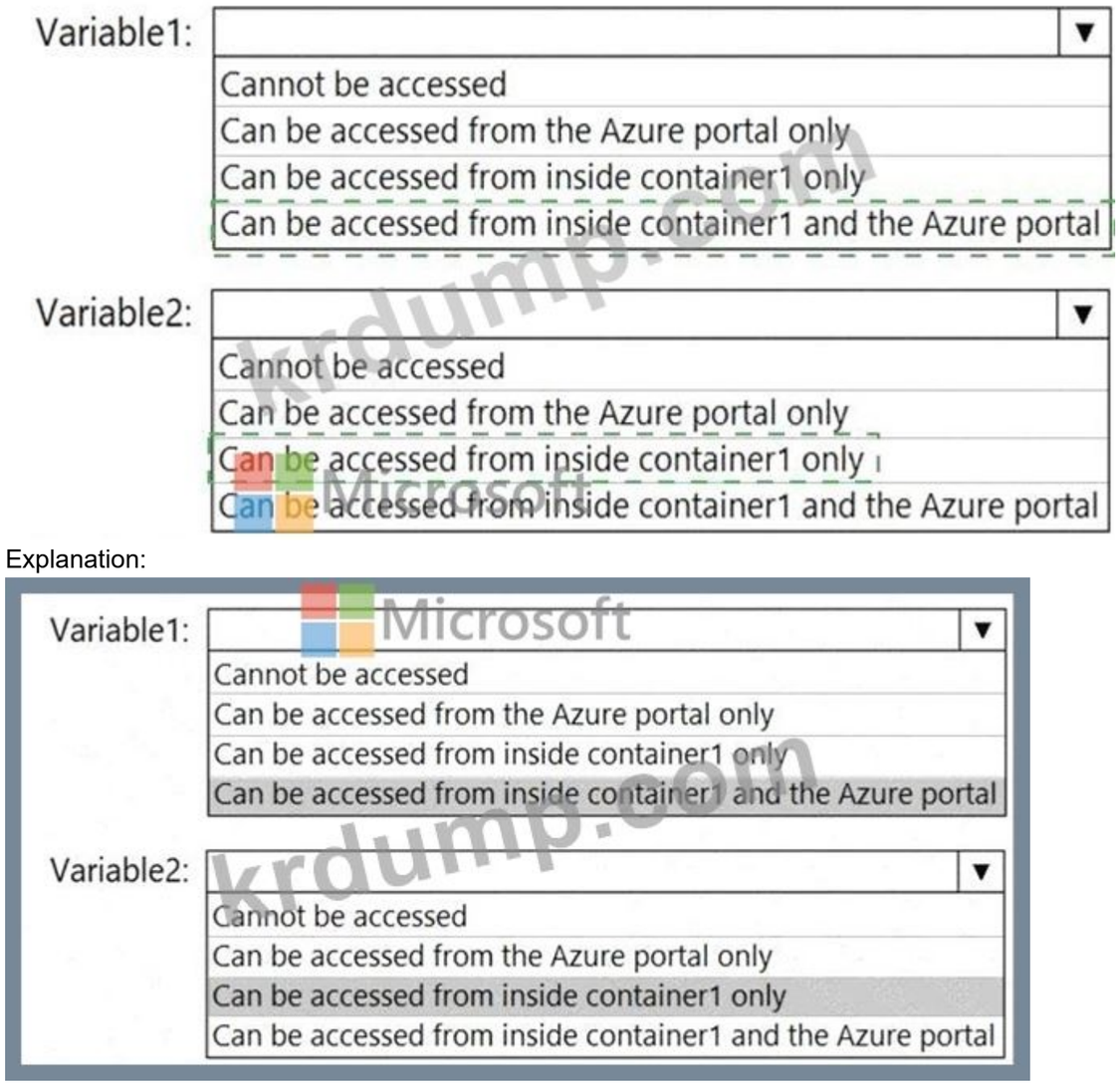
Variable1:

- Cannot be accessed
- Can be accessed from the Azure portal only
- Can be accessed from inside container1 only
- Can be accessed from inside container1 and the Azure portal

Variable2:

- Cannot be accessed
- Can be accessed from the Azure portal only
- Can be accessed from inside container1 only
- Can be accessed from inside container1 and the Azure portal

Answer:



Explanation:

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

NEW QUESTION: 67
Azure □□□ □□□□ MG1□□□ □□ □□□ RG1□□□ □□□ □□□ □□□□. RG1□□ VM1□□□ □□ □□□ □□□□. □□ □□ □□ □□ □□□ □□ Azure □□□ □□□□.

Name	Scoped to
Role1	MG1
Role2	RG1

Role1□ □□ □□□ □□ □□ □□ □□□ □□□□□.

□□ □□ □□□ □□□□□ □□□ □□□□□.

Name	Role
User1	Role1
User2	Role1, Role2
User3	Role2

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

Answer:

Explanation:

NEW QUESTION: 68

App1□□□ □□ □□□ Azure □□□ □□□□. App1□□ □□ □□ □□ □□ □ □□□ □□□□.

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

App1□ □□ □□□ □□□□ □□ □□□ □□□ □ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.

□□□ □□ □□□?

A. Microsoft.Graph Calendars.ReadWrite□ □□ □□□ □□ API □□□ □□□□□.

B. Microsoft.Graph Calendars.ReadWrite□ □□ □□□ □□□□□□ API □□□ □□□□□.

C. □□□ □□ □□□ □□□□□.

D. Microsoft.Graph Calendars.ReadWrite.Shared□ □□ □□□ □□ API □□□ □□□□□.

Answer: A (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 69

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

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

□□ □□□□ □□□□ □□□□ □□□□□.

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

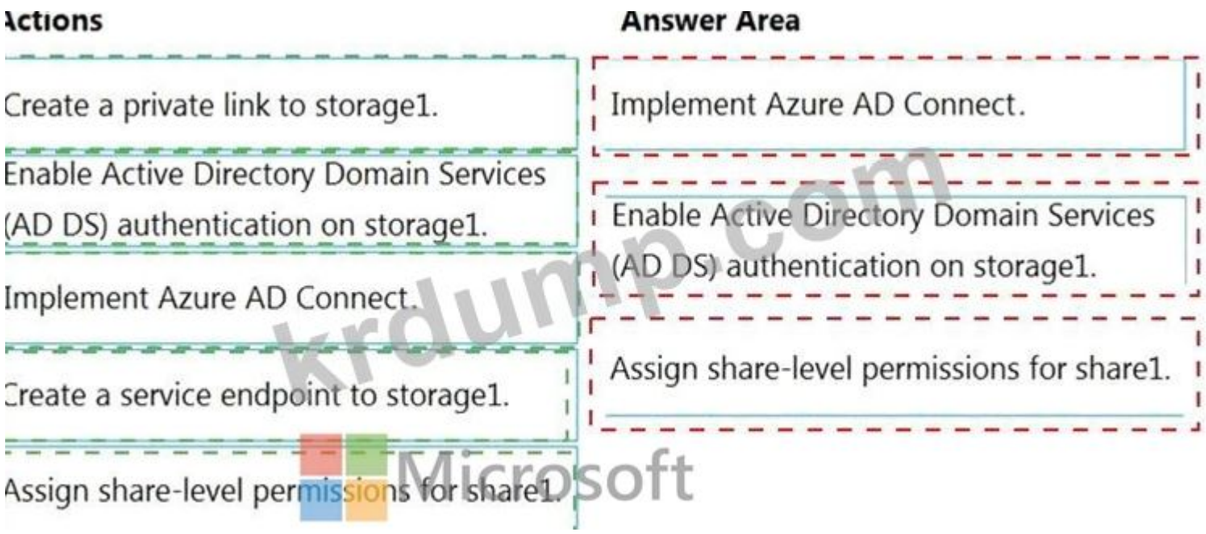
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□□ □□ □□□□ □□ □□□ □□ □□□□ □□ □□□ □□□□ □□□□□.

Actions

- 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 Area

Answer:



Explanation:

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

NEW QUESTION: 70
□□ □□ □□□ □□ □□□□□ □□□□ Sub1□ Sub2□□ □ □□ Azure □□□ □□□□.

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

□□ □□□ □□□ Azure Virtual Network Manager □□□□□ □□□□.
* □□: NetMgr1
* □□: □□ □□
* □□: □□□
* □□□□ : Sub1
NetMgr1□ □□ □□ □□ □□□ □□ □□□□ □□□ □□□□.

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

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

Answer Area

Answer:

Explanation:

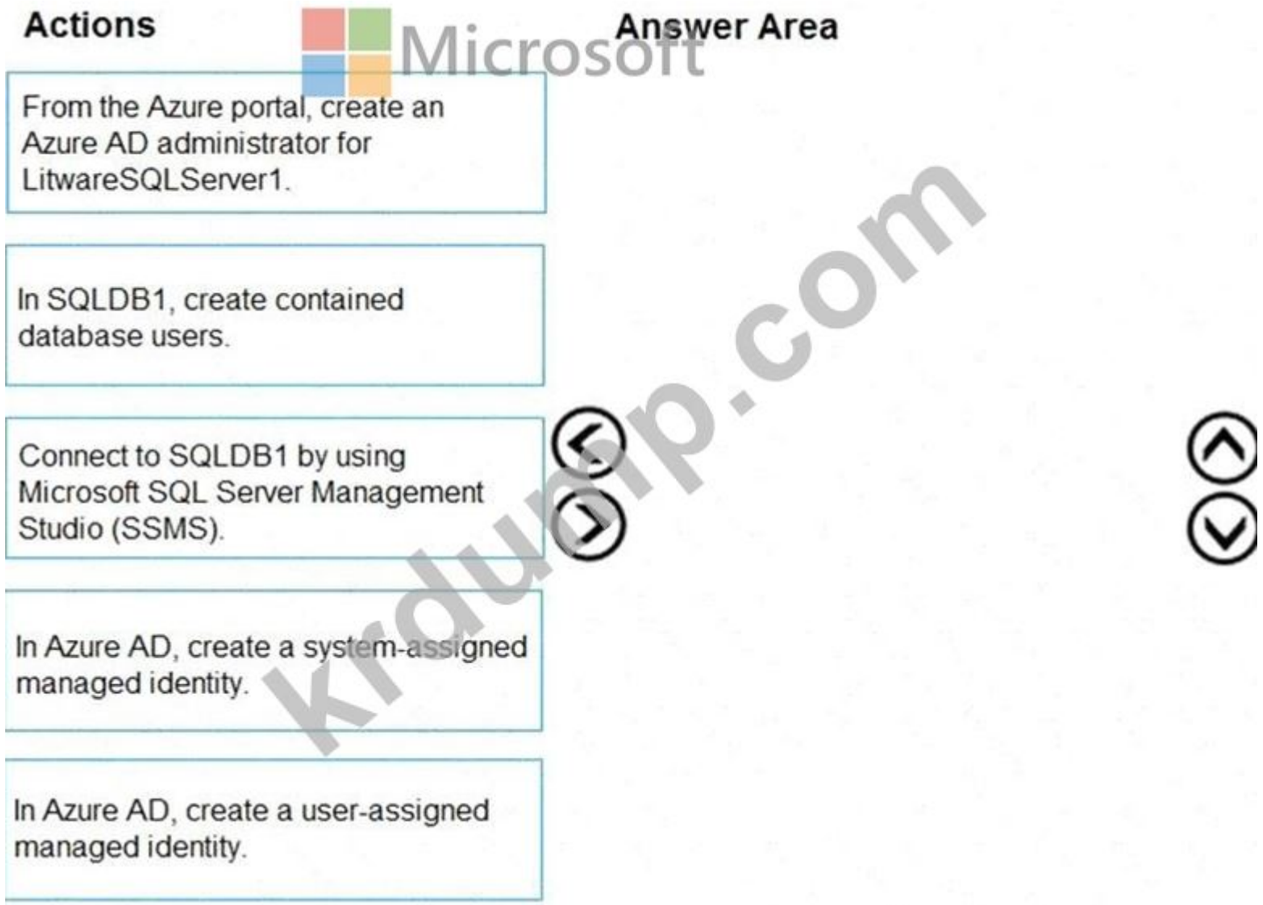
Answer Area

NEW QUESTION: 71
□□ □□ □□□ □□□□□ □□□□ □□□□□ □□□. □□ □ □□□ □□□ □ □□□?
A. KeyVault1□
B. KeyVault2 □ KeyVault3□ □□
C. KeyVault1 □ KeyVault3□ □□
D. KeyVault1 KeyVault2 □ KeyVault3
Answer: B (LEAVE A REPLY)
The storage account and the key vault must be in the same region and in the same Azure Active Directory (Azure AD) tenant, but they can be in different subscriptions.

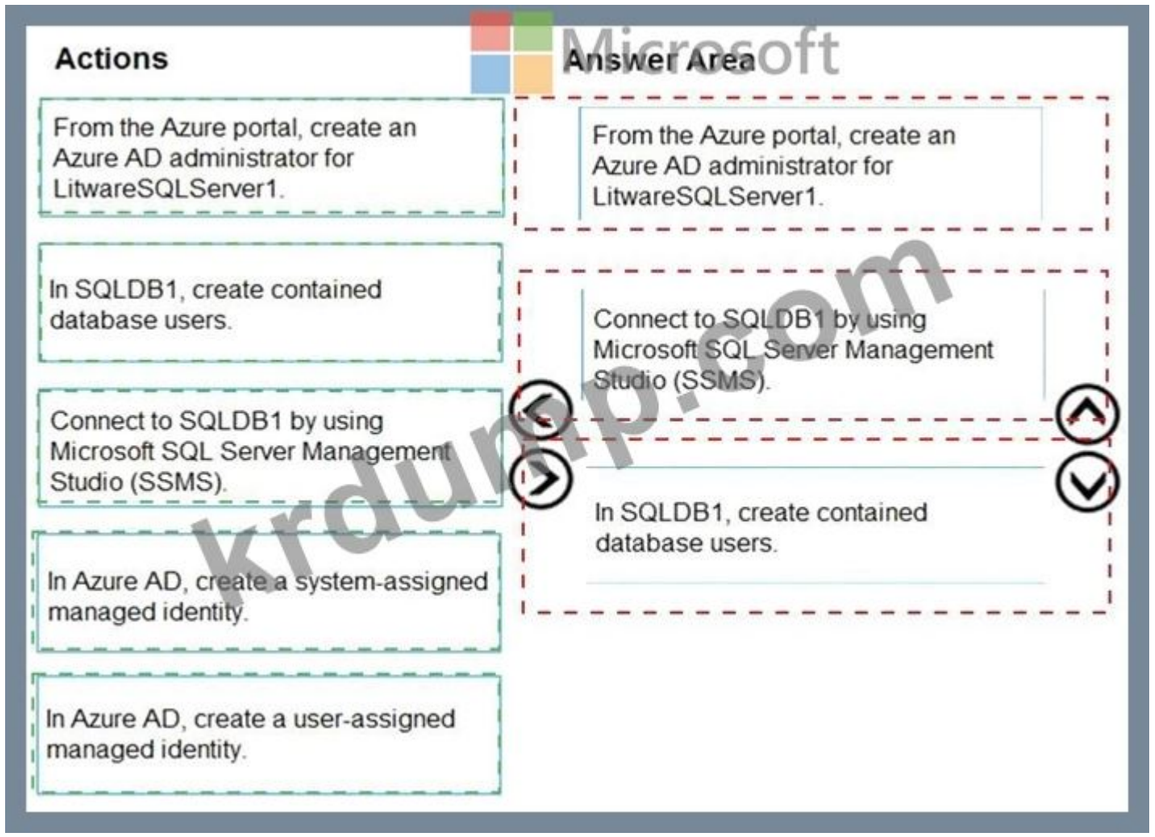
Storage1 is in the West US region. KeyVault1 is the only key vault in the same region.
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-overview

NEW QUESTION: 72
4□□ Azure SQL □□ □□□□□ □□□ Azure □□□ □□□□.
□□□□ □□□□□ SQL □□ □□□ □□ □□□□ □□□□ □□□.
□□ □□ □□□ □□ □□□?
A. Azure Advanced Threat Protection(ATP) □□□□□ □□□□.
B. □□ □□□ □□□ □□□□□□.
C. Azure Monitor□ SQL Health Check □□□□ □□□□□.
D. Azure Sentinel □□ □□□ □□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 73
□□□ □ □□□□□□ □□ □□□ □□□□□ SQLDB1□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□□ □□ □□□□? □□□□ □□ □□□□ □□ □□□ □□ □□□□ □□ □□□ □□□□ □□□□□.



Answer:



Explanation:

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

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

NEW QUESTION: 74

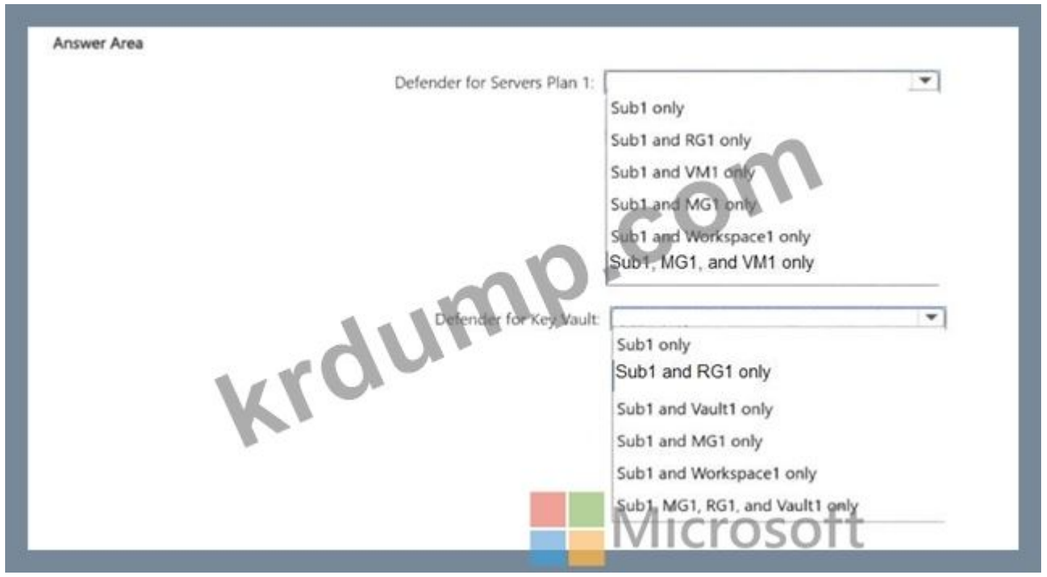
MG1□□□ □□ □□□ □□, □ □□□□ Sub1□□□ Azure □□□ □□□□. Sub1□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

Sub1□ □□□□ □□□□ □□□? Microsoft Defender for Servers Plan1 □ Microsoft Defender for Key Vault□ □□□□ □□□□□□.

Azure □□□□ Defender for Servers Plan 1□ □□□□ □ □□ □□□□ Defender for Key Vault□ □□□□ □ □□ □□□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □□ □□□ 1□□□□.



Answer:

Explanation:

Answer Area

NEW QUESTION: 75

WebApp1□□□ Azure App Services □□□ Vault1□□□ Azure Key Vault□ □□□ Azure □□□ □□□□. Vault1□□ □□ □□ □□ □□ □□□□ □□□□.

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

WebApp1□ TLS□ □□□ □□□□□.

WebApp1□ □□□□ □□□□ □□□.

Vault1□ □□ □□□□ WebApp1□ □□□ □ □□□?

A. Cert1, Cert2, Cert3 □ Cert4

B. Cert1 □ Cert2□

C. Cert1 □ Cert3□

D. Cert3 □ Cert4□ □□

Answer: B (LEAVE A REPLY)

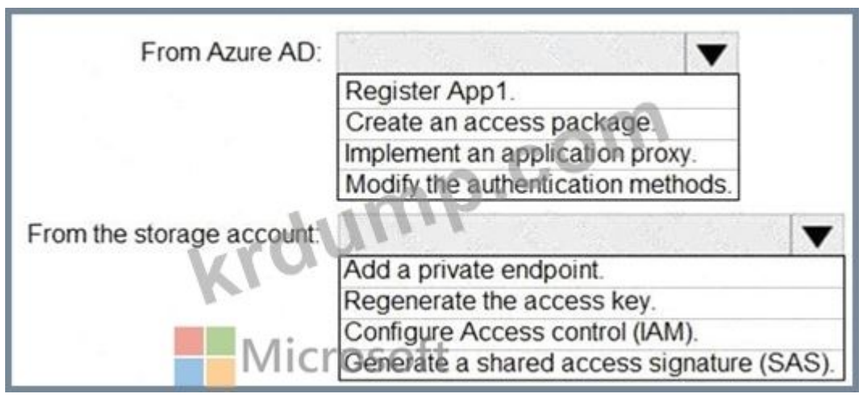
NEW QUESTION: 76

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

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

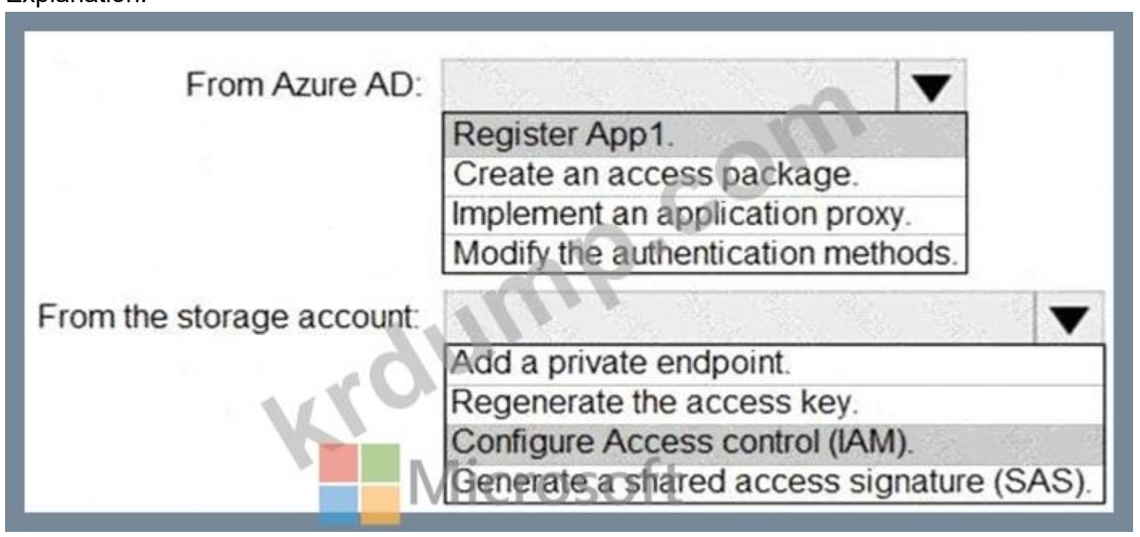
□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□□ □□□□□.

□□: □□ 1□□ 1□□□□.



Answer:

Explanation:

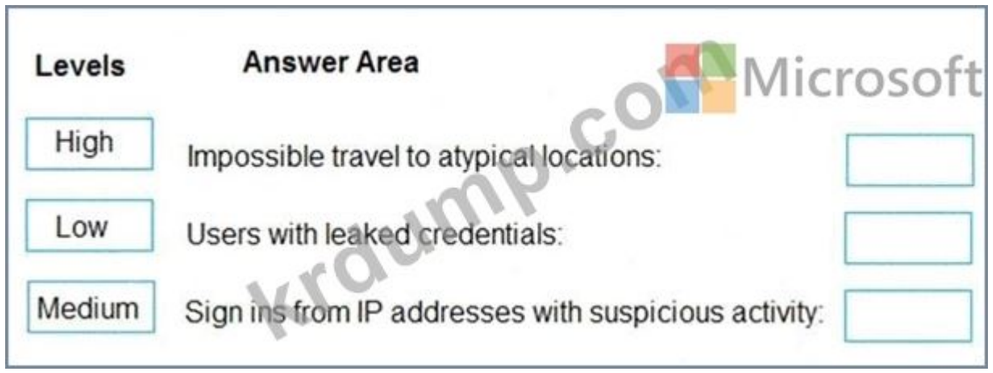


Reference:
https://azure.microsoft.com/en-in/blog/announcing-the-preview-of-aad-authentication-for-storage/
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/storage/common/storage-auth-aad-rbac-portal.md

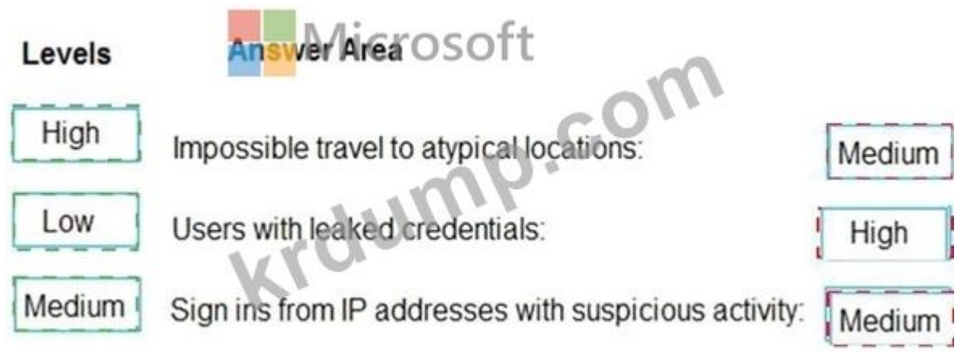
NEW QUESTION: 77
□□□ □□□ □□□ □□□□ □□□□.
□□□ □□□□ □□□□□ □□ Azure Active Directory(Azure AD) □□ □□□□ □□ □□□ □□□□ □□□.
□□ □□ □□□ □□ □□□ □□□□ □□□.
* □□ □□□ □□□ □□□
* □□□□□ □□□□ □□□ □□□□□□.
* □□□□□ □□□ □□ IP □□□□ □□□

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

□□: □□ 1□□ 1□□□□.



Answer:



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

NEW QUESTION: 78

□□ □□ □□□ □□ □□□ □□□ Azure □□□ □□□□.

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

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

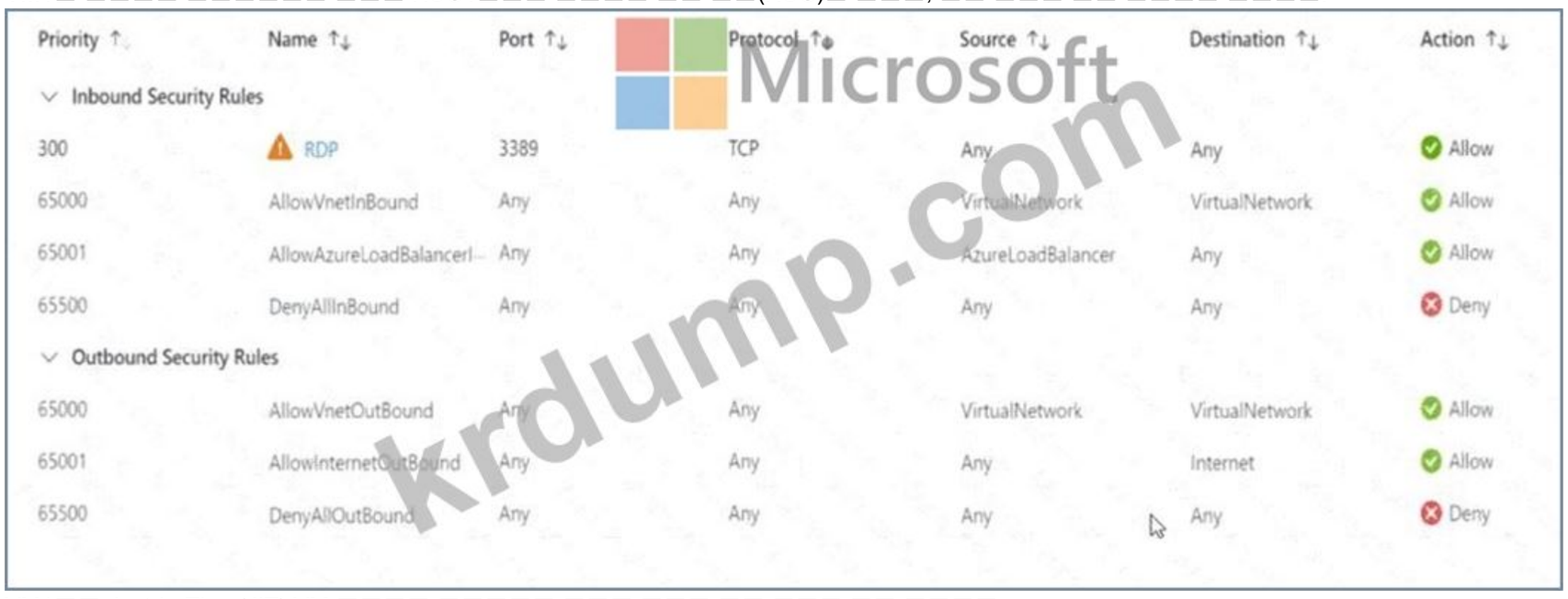
□□ □□ □□□ □□ □□□ □□□□□.

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

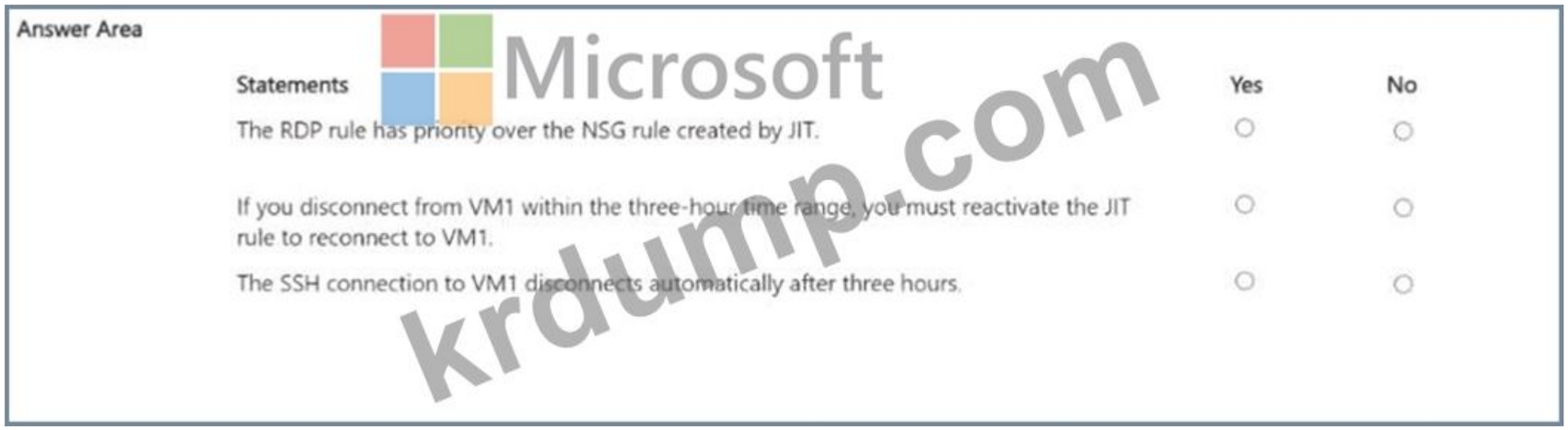
Log Analytics □□□□□ □□ □□ □□□ □□□□ □□□?

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

NEW QUESTION: 79
VM1□□□ □□□ □□ □□□ □□□ Azure □□□ □□□□.
VM1□ □□□□ □□□□□□ □□□ NSG1□□□ □□□□ □□ □□(NSG)□ □□□, □□ □□□ □□ □□□□ □□□□.

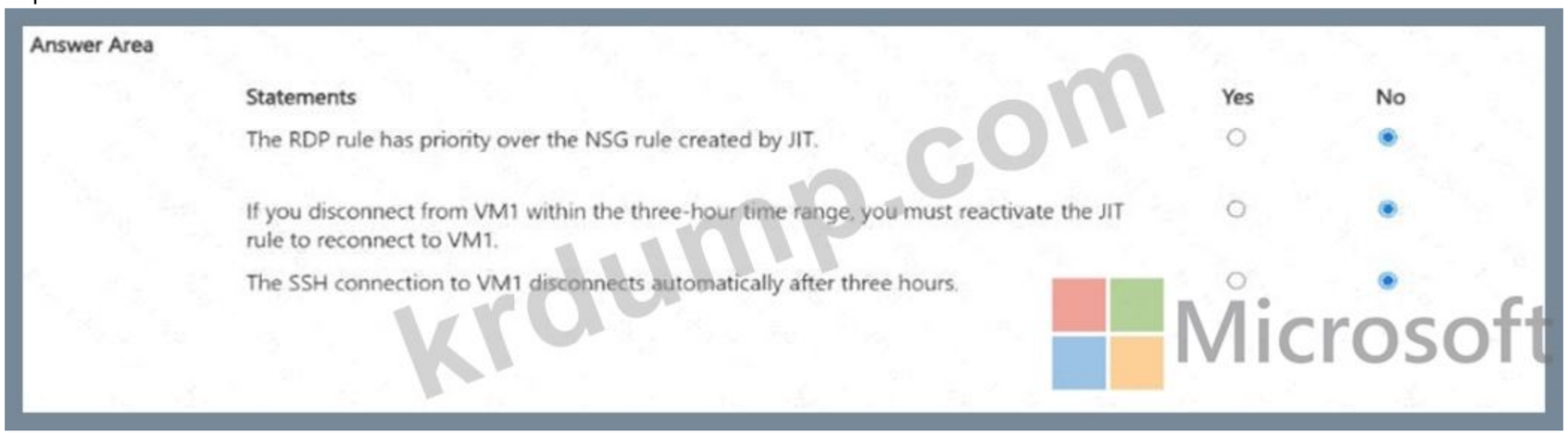


VM1□□ Just-in-Time(JIT) VM □□□□ □□□□□ □□□ □□□ □□ □□□ □□ □□□□.
* □□ □□: 3389, 22
* □□ □□ □□: 3□□
* □□□□ □□ IP □□: □□
JIT □□□ □□□□□ SSH□ □□□□ VM1□ □□□□□.
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.



Answer:

Explanation:



NEW QUESTION: 80

□□□□□□ Azure Active Directory(Azure AD)□ □□□□□ adatum.com□□□ □+□□□□ Active Directory □□□□ □□□□. Azure AD Connect□ Server1□□□ □□□ □□□ □□□ □□□□ □□ □□.

adatum.com □□□□ □□□ □□□□ □□□ □□□ □□□ □ □□□ □□ □□□. □□□□□ □□ □□ □□□ □□□□ □□□.
□□□ □□□□□ □□ Azure AD □□□ □□□□ □□□?
A. □□ □□□
B. □□□ □□□
C. □□□ □□□
Answer: B (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions

NEW QUESTION: 81
contoso.com□□□ Azure Active Directory(Azure AD) □□□□ □□□ Sub1□□□ Azure □□□ □□□□.
Admin1□□□ □□□□ □□ ID□ □□□□ □ □□□□.
* OpenID □□ □□□ □□
* Hotmail □□
* contoso.com□ □□
* fabrikam.com□□□ Azure AD □□□□ □□
Azure Account Center□ □□□□ Sub1□ □□□□ Admin1□ □□□ □□□□□.
Sub1□ □□□□ □□ □□□□ □□□ □ □□□?
A. contoso.com□
B. contoso.com, fabrikam.com □ Hotmail□ □□
C. contoso.com □ fabrikam.com□ □□
D. contoso.com, fabrikam.com, Hotmail □ OpenID □□ □□□ □□
Answer: C (LEAVE A REPLY)
When you transfer billing ownership of your subscription to an account in another Azure AD tenant, you can move the subscription to the new account ' s tenant. If you do so, all users, groups, or service principals who had role based access (RBAC) to manage subscriptions and its resources lose their access. Only the user in the new account who accepts your transfer request will have access to manage the resources.
Reference:
https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer
https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transferring-subscription-to- anaccount-in-another-azure-ad-tenant

NEW QUESTION: 82
□□□ □□□□ □□□ □□ □□□ □□□□ □□□.
□□ CAPolicy1 □□□ □□□□ □□□?
A. □□□□ □ □□ □□
B. □□
C. □□□
D. □□
Answer: D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session- lifetime

NEW QUESTION: 83

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

Name	Type
container1	Container
folder1	File share
table1	Table

User1□□ storage1□ □□ □□ □□□ □□□□□.

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

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

Answer:

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

Explanation:

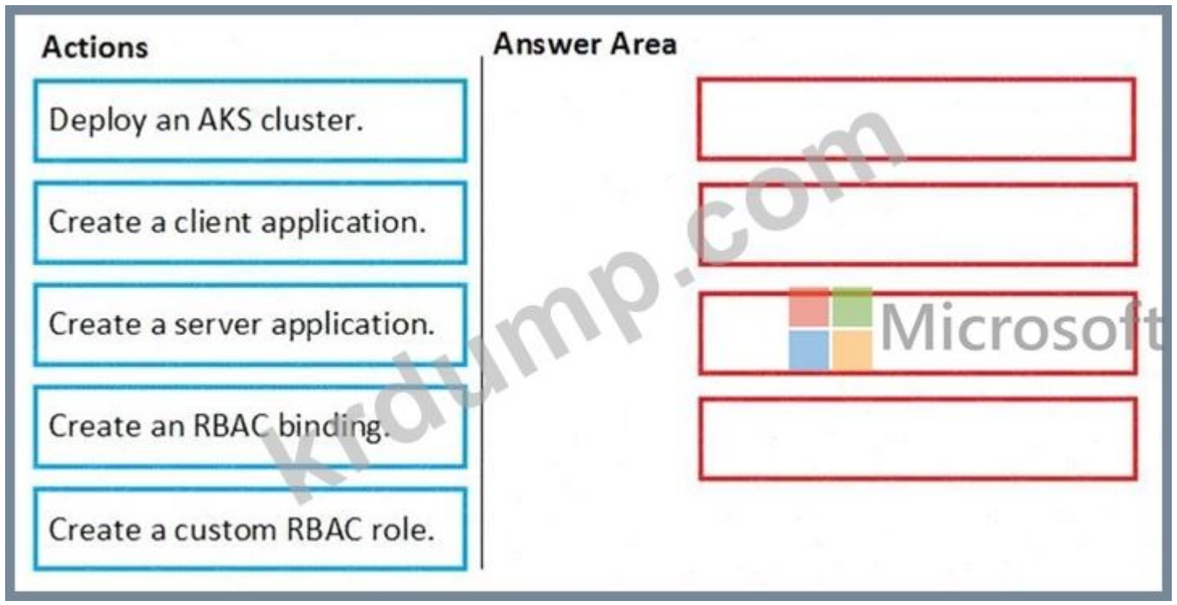
No, Yes, No

NEW QUESTION: 84

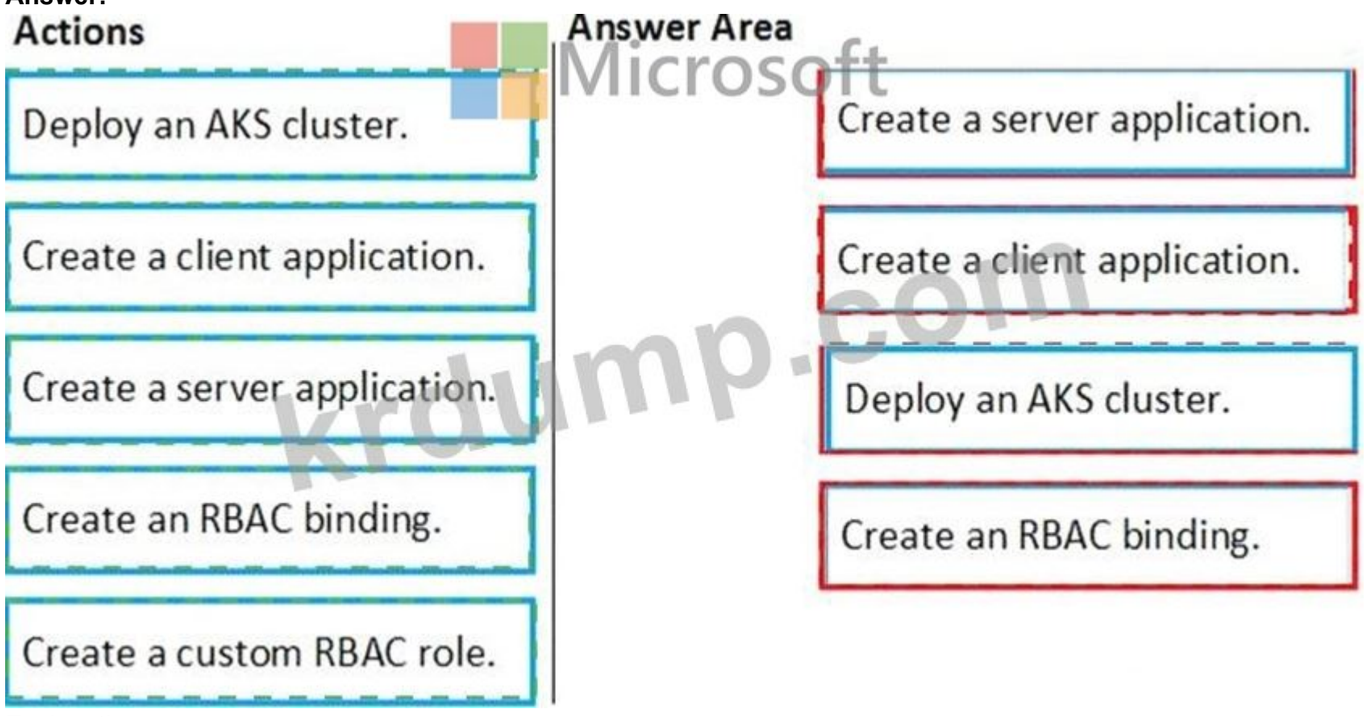
□□□ □□ □□ □□□ □□□□□ AKS1□ □□□□ □□□.

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

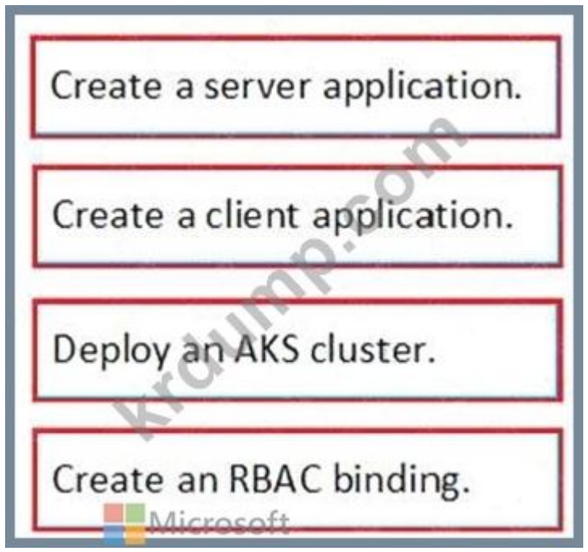
□□: □□ □□□ □ □ □□□ □ □□□□. □□ □□□ □□□□ □□ □□ □□□□ □□□□□.



Answer:



Explanation:



Scenario: Azure AD users must be to authenticate to AKS1 by using their Azure AD credentials.
Litewire plans to deploy AKS1, which is a managed AKS (Azure Kubernetes Services) cluster.
Step 1: Create a server application
To provide Azure AD authentication for an AKS cluster, two Azure AD applications are created. The first application is a server component that provides user authentication.
Step 2: Create a client application
The second application is a client component that ' s used when you ' re prompted by the CLI for authentication. This client application uses the server application for the actual authentication of the credentials provided by the client.
Step 3: Deploy an AKS cluster.
Use the az group create command to create a resource group for the AKS cluster.
Use the az aks create command to deploy the AKS cluster.
Step 4: Create an RBAC binding.
Before you use an Azure Active Directory account with an AKS cluster, you must create role-binding or cluster role-binding. Roles define the permissions to grant, and bindings apply them to desired users. These assignments can be applied to a given namespace, or across the entire cluster.
Reference:
https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration
Topic 1, Litware, inc
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question on this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next sections of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question on this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
Overview

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

Existing Environment

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

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

The tenant contains the groups shown in the following table.

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

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

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

Azure Security Center is set to the Free tier.

Planned changes

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

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

Litware identifies the following identity and access requirements:

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

Platform Protection Requirements

Litware identifies the following platform protection requirements:

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

Security Operations Requirements

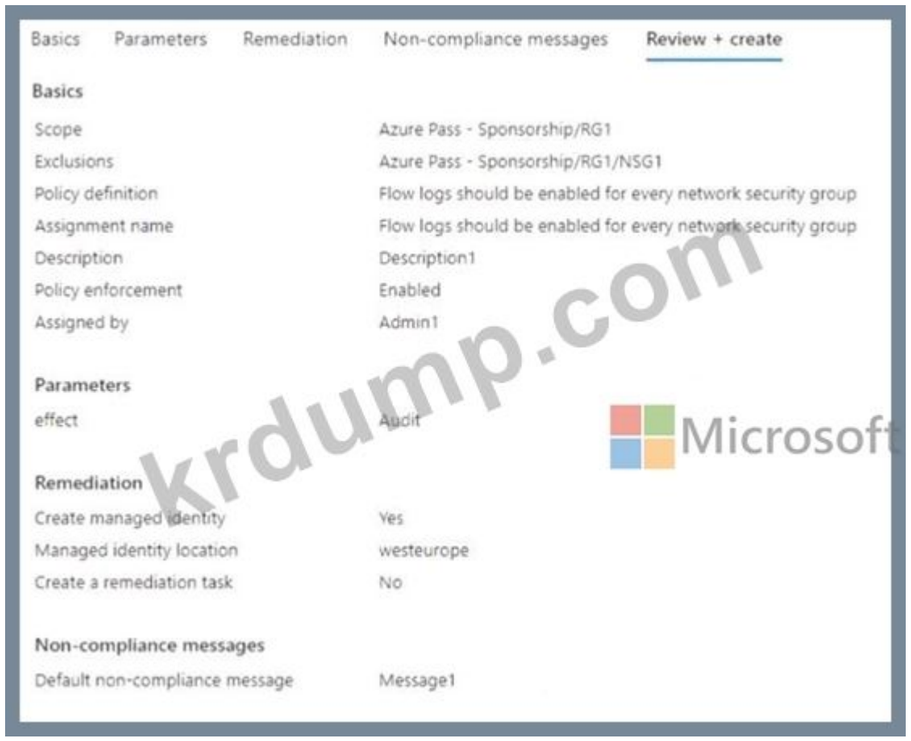
Litware must be able to customize the operating system security configurations in Azure Security Center.

NEW QUESTION: 85

□□ □□ □□ □□ RG1□□□ □□□ □□□ NSG(□□□□ □□ □□)□ □□□ Azure □□□ □□□□.

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

□□ □□□ □□□ Azure □□□ □□□□.



RG1□ □□□ □□□□□.

NSG1□ NSG2□ □□□ □□□□ □□□ □□□?

A. NSG1 □ NSG2□ □□ □□ □□□ □□□□□□.

B. NSG1□ □□□□ □□ □□□ □□□□□□.

C. NSG1 □ NSG2□ □□ □□ □□□ □□□□□□□.

D. NSG2□ □□□□ □□ □□□ □□□□□□.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 86

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

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

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

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

□□ □□: Active Directory Federation Services(AD FS)□ □□□ □□□□□□ □□□□ □□ □□□□.

□□□□ □□□ □□□□□?

A. □

B. □□□

Answer: B (LEAVE A REPLY)

A federated authentication system relies on an external trusted system to authenticate users. Some companies want to reuse their existing federated system investment with their Azure AD hybrid identity solution. The maintenance and management of the federated system falls outside the control of Azure AD. It ' s up to the organization by using the federated system to make sure it ' s deployed securely and can handle the authentication load.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

NEW QUESTION: 87
□□: □ □□□ □□□ □□□ □□ □□ □□ □ □□□ □□□□ □□□□. □□□ □ □□□□ □□□ □□□ □□□□. □□ □□ □□□ □□□□□ □□□□□.
□□□ weylandindustries.com□□□ □□ □□□□ □□□□ Active Directory □□□□□ □□□□ □□□□. □□ □□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□ □□□□.
Active Directory□ Azure AD □□□□ □□□□ □□□ □□□□□. Azure AD Connect□ □□□□□ □□□.
□□□ □□ □□□□□ □□ □□□ □□□ □□□ □□□ Azure AD □□□□ □□□□ □□□ □□□ □□□ □□□ □□□ □□ □□ □□□□□ □□ □□□.
□□ □□: □□□□ □□□ □□□□ □□ □□□□ □□ □□□ SSO□ □□□□ □□ □□□□.
□□□□ □□□ □□□□□?
A. □
B. □□□
Answer: A (LEAVE A REPLY)
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

NEW QUESTION: 88
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: (SHOW ANSWER)
Deleted users and deleted Office 365 groups are available for restore for 30 days.
You cannot restore a deleted security group.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-restore-deleted

NEW QUESTION: 89
Subscription1□□□ Azure □□□ □□□□.
□□□□□ Subscription1□ □□□ □□ □□□ □□□□ □□□.
□□ Azure □□ □□ □□□□□ □□□ □□□□ □□□?
A. □□ □□ □□ □□ □□
B. Azure Security Center□□ □□□□ □□□ □□□□□ □□

C. VM□ Azure Monitor □□□ □□□□□ □□
D. Azure Monitor □□□ '□□ □ □□'□ □□ □□□ □□□□ □□□.
Answer: B (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/security-center/tutorial-security-policy
https://docs.microsoft.com/en-us/azure/security-center/policy-reference

NEW QUESTION: 90
Azure □□□ □□□□.
Role1□ Role2□□ □ □□ □□□ □□ □□□ □□ □□□□□.
□□□ □□ □□□ □□ □□□ □□□□ □ □□□□□.
* Role1□ □□□ □□□□□□ □□ □□□ □□□□□.
* Role2□ □□□ Azure Bastion□ □□□□□.
□□□ □□ □□□ □□□ □□□□ □□□.
□ □□□ □□ □□□ □□□□ □□□□ □□□? □□□□ □□ □□□ □□□□ □□□ □□□ □□□□□□. □ □□□ □□□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□. □□□□ □□□ □ □□□ □□ □□□ □□□□□□ □□□□□ □ □□ □□□□.

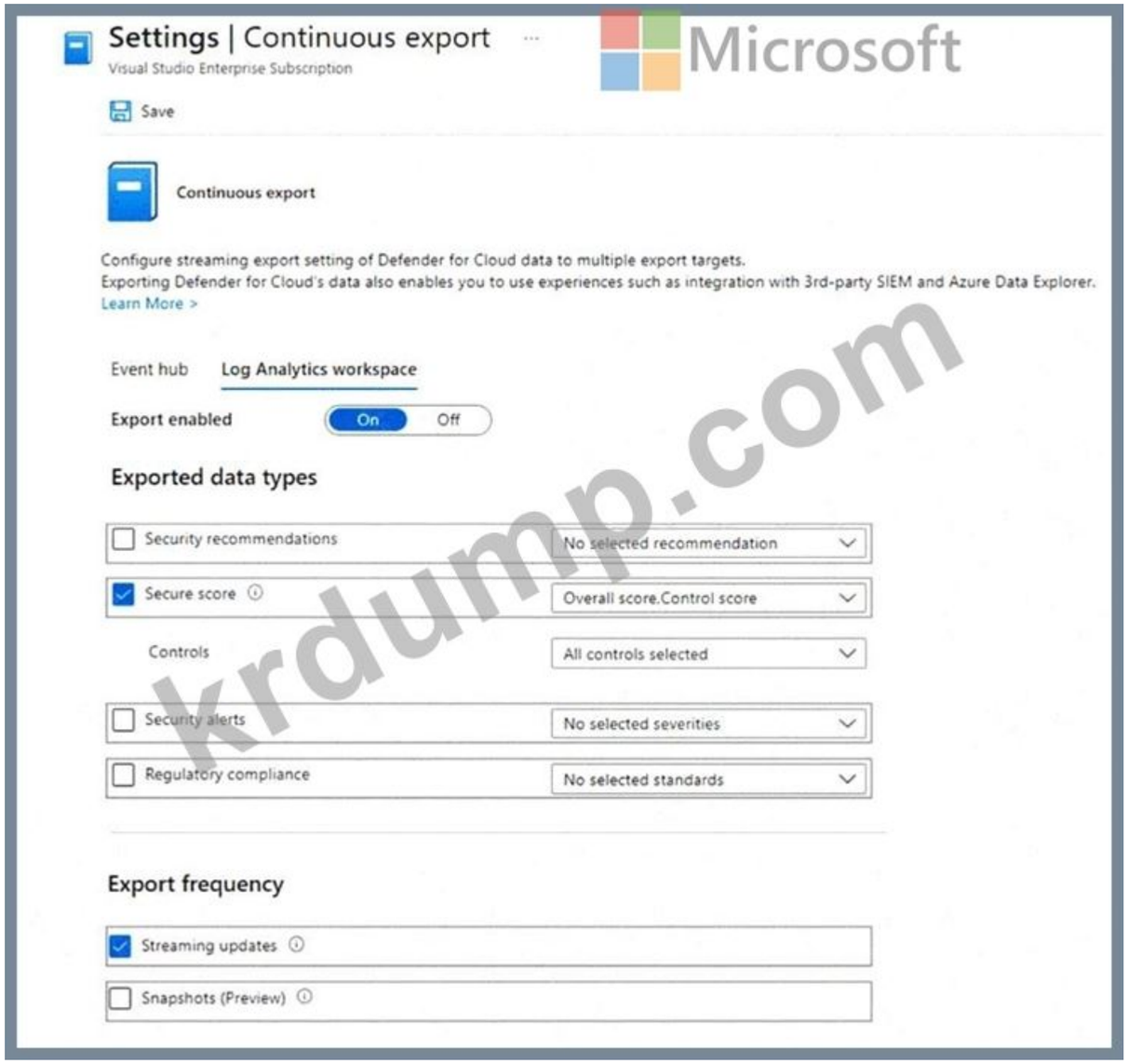
Answer:

Explanation:

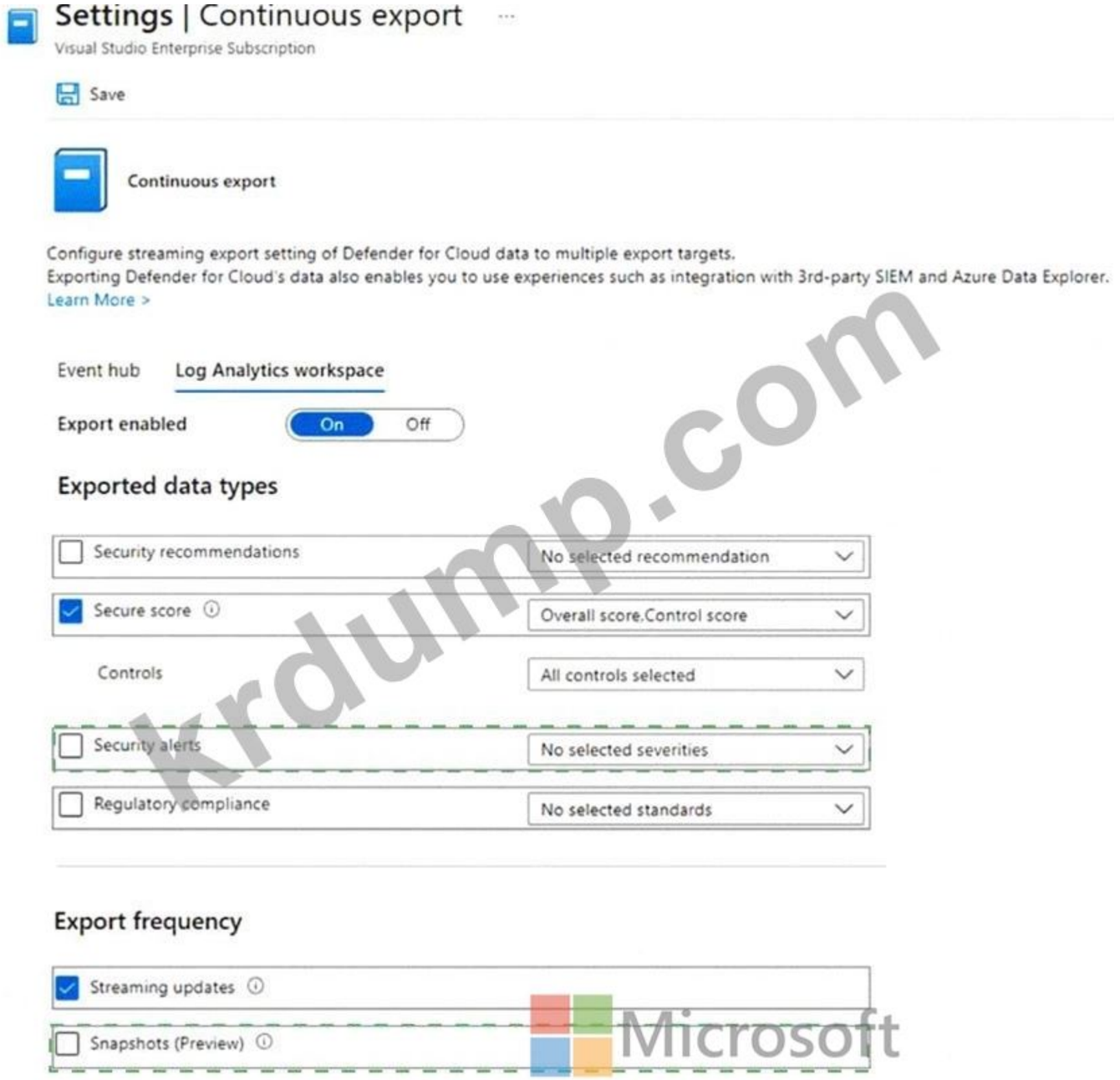
NEW QUESTION: 91
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □ □ □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□□ □□□□.
Azure Active Directory(Azure AD)□ □□□□□ □□□ □□□□.
□□ □□□□□ Azure HDInsight □□□□□ □□□□.
□□□□ □□□□ Active Directory □□ □□□ □□□□ □□□□□ □□□□□ □□□ □□□□□.
□□□ □□□ □□□□□ □□□ □□□□ □□□.
□□ □□: Azure □□□ Azure Active Directory Domain Services(Azure AD DS)□ □□□□□.
□□□ □□□ □□□□□?

A. □
B. □□□
Answer: A (LEAVE A REPLY)
References:
https://docs.microsoft.com/en-us/azure/hdinsight/domain-joined/apache-domain-joined-configure-using-azure- adds

NEW QUESTION: 92
Microsoft Defender for Cloud□ □□□□ Azure □□□ □□□□.
□□ □□□ □□ □□ □□ □□□□ □□□ □□□□□.
Defender for Cloud □□□□ □□ □□□□ □□□□ □□□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.

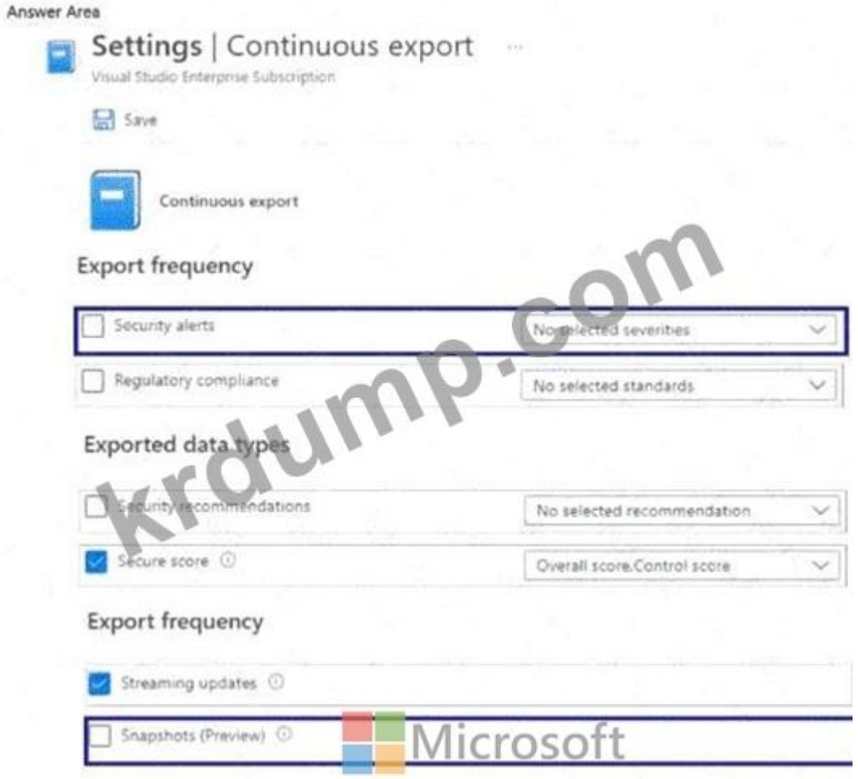


Answer:



Explanation:

Answer Area



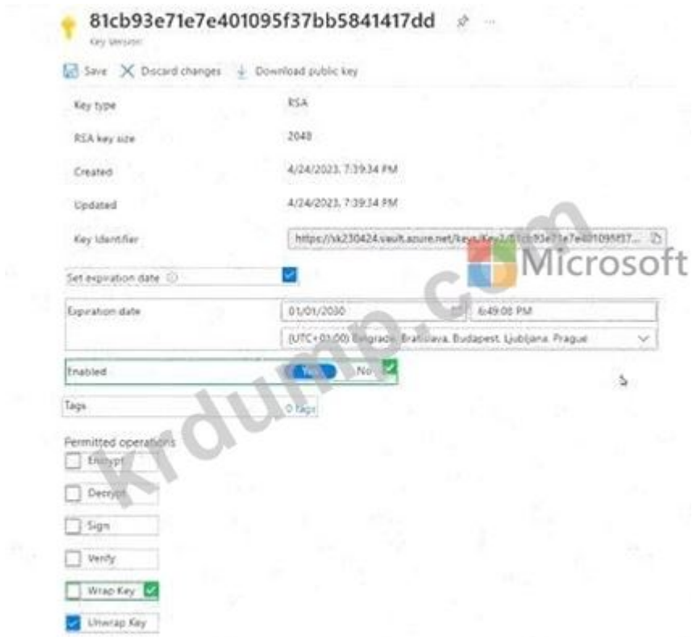
NEW QUESTION: 93
Microsoft Enterprise PIM(Privileged Identity Management)□ □□□□ Azure □□□ □□□□. User1□□□ □□□□ □□ □□□ □□□ □□□ □□□ □□□□. □ □□□ □□ 2□□ □□□ □□ □□□ □□ □□□□ □□□. □□□ □□ □□□?
A. □□ □□□ □□□ □□□□□.
B. □ □□□ □□□ □□□□□.
C. □□ □□ □□□ □□□□□.
D. □□□ □□ □□□□ □□□□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 94
WebApp1□□□ □ □□ □□□□.
WAF1□□□ □□□ □ □□□□□□ □□□(WAF) □□□ □□□□□.
WAF1□ □□□□ WebApp1□ □□□□ □□□.
□□ □□ □□□ □□ □□□?
A. Azure Front Door□ □□□□□.
B. WebApp1□ □□ □□□ □□□□□.
C. Azure Firewall□ □□□□□.
Answer: A (LEAVE A REPLY)
References:

https://docs.microsoft.com/en-us/azure/frontdoor/quickstart-create-front-door

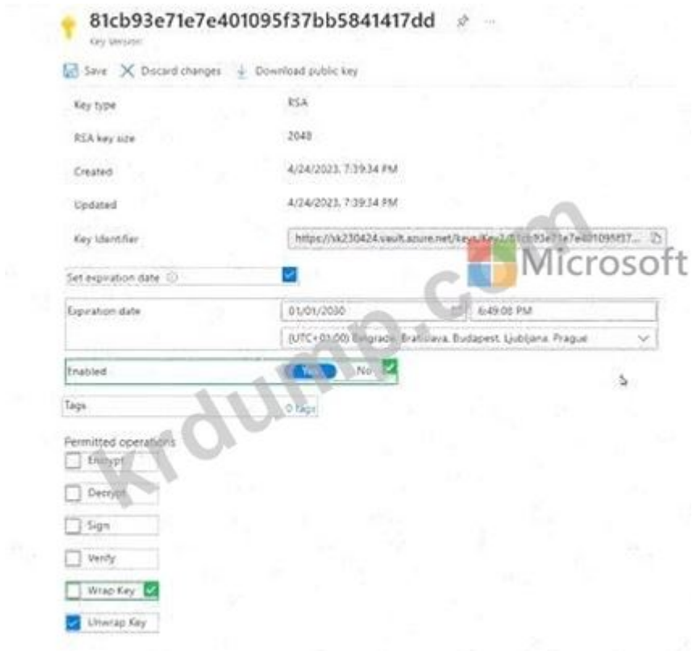
NEW QUESTION: 95
WAF1□ □□ □□□ □□ □□□ □□□□ □□□.
□□□□ □□ □□□ □□□□□ □□□.
□□□ □□ □□□?
A. Bot Manager 1.1 □□ □□□ □□□□□.
B. Azure □□□ □□□□.
C. □□□ □□ □□□ □□□□□.
D. Azure□□ □□□□ DRS□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 96
Azure Key Vault□ SQL1□□□ Azure SQL □□□□□□□ □□□ Azure □□□ □□□□.
Key1□□□ □□ □□□□□.
Key1□ □□□□ SQL1□ □□ TDE(□□ □□□ □□□)□ □□□□□ □□□.
Key1□□ □□ □ □□ □□□ □□□□ □□□? □□□ □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.



Answer:

Explanation:



NEW QUESTION: 97

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

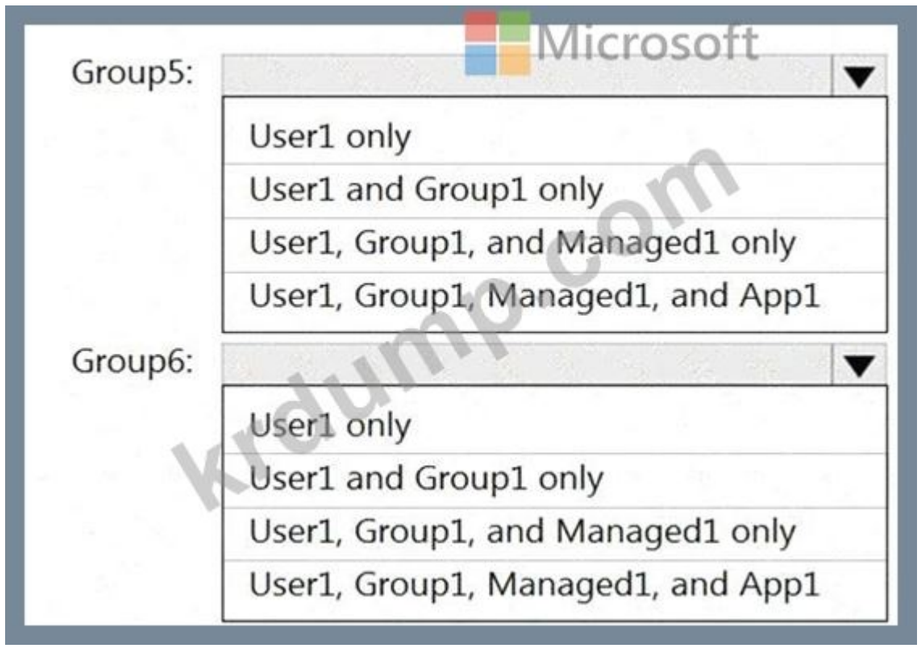
Name	Description
User1	User
Group1	Security group that has a Membership type of Dynamic Device
Managed1	Managed identity
App1	Enterprise application

□□ □□ □□□ □□□ □□□□.

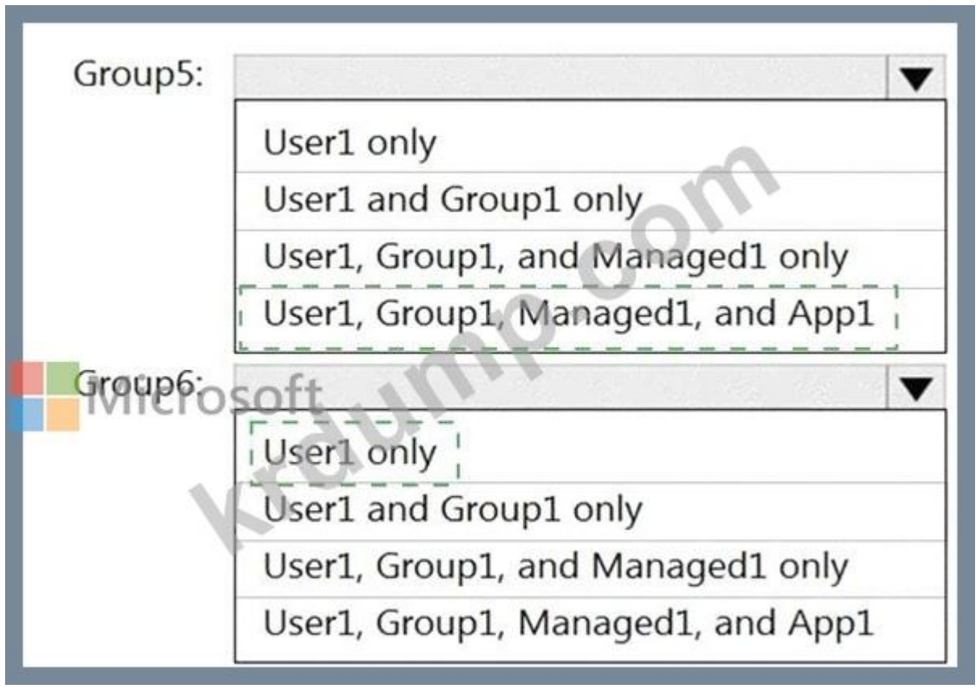
Name	Description
Group5	Security group that has a Membership type of Assigned
Group6	Microsoft 365 group that has a Membership type of Assigned

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

□□: □□ 1□□ 1□□□□.

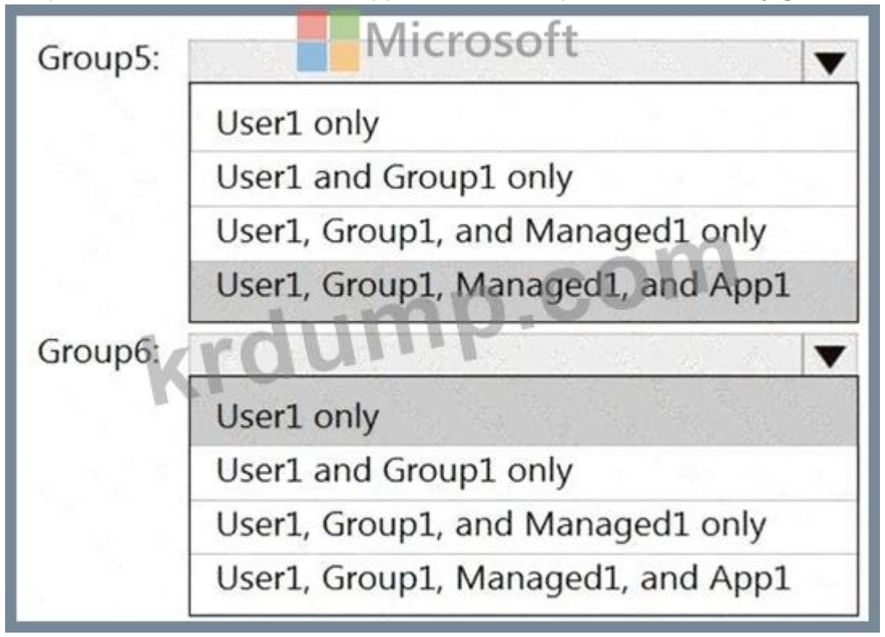


Answer:



Explanation:

Graphi cal user interface, text, application Description automatically generated

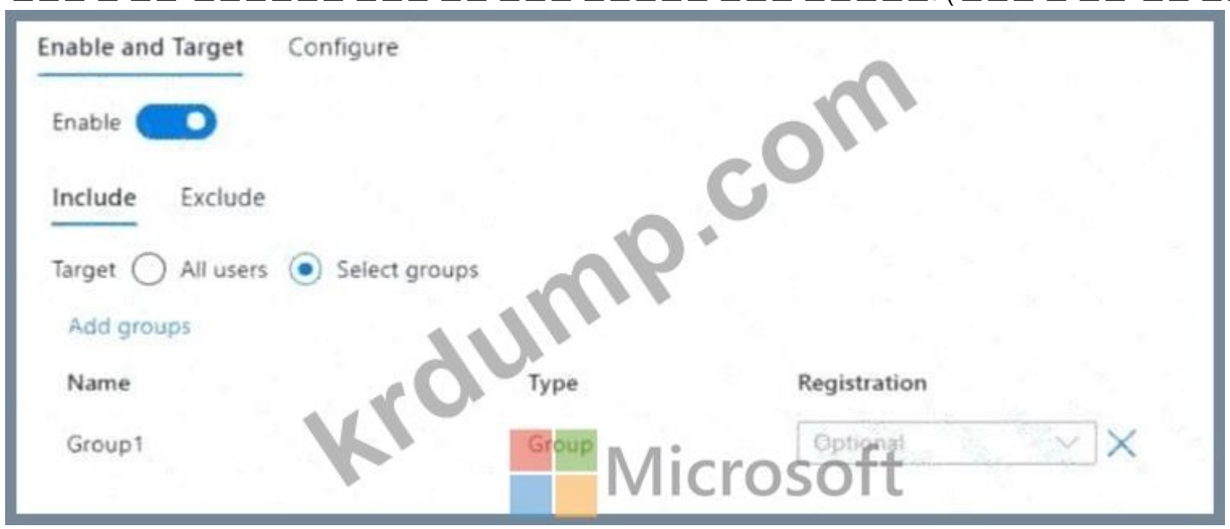


NEW QUESTION: 98

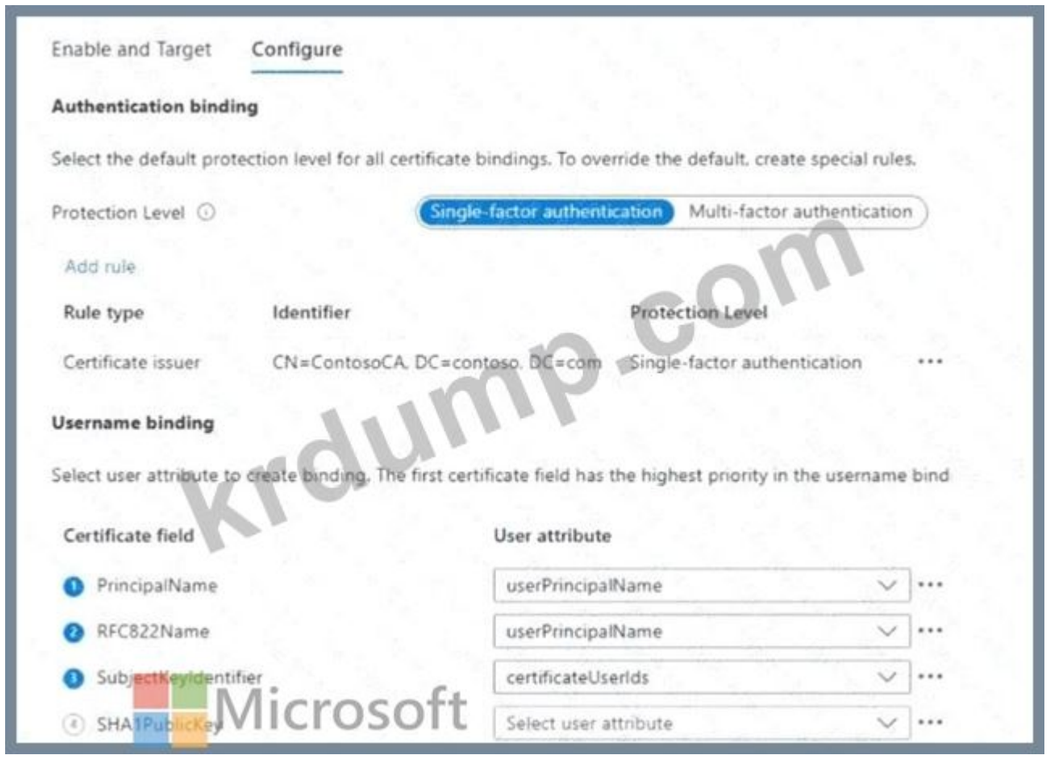
□□ □□ □□□ □□□□ □□□ Microsoft Entra □□□□ □□□□.

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

□□ □□□□ ContosoCA□□ □□ □□(CA)□□ □□□ □□□□ □□□ □□□ □□□ □□□□.
□□ □□□ □□□□ □□□ □□□ □□□ □□□□.
* □□: CAPoltcy1
* □□
o □□□ □ □□: Group1
o □□ □□
* □□: □□ □□□□ □
o □□ □□
* □□□ □□: □□ □□ □□ □□
o □□ □□□: □□
'□□□ □ □□' □□□□□□ □□□ □□ □□□ □□□□□ □□□ □□□□□. ('□□□ □ □□' □□ □□□□□.)



□□ □□□ □□□ □□ □□□ □□ □□□ □□□□□. ('□□' □□ □□□□□.)



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

Answer Area

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

Answer:

Explanation:

NEW QUESTION: 99

SQL1□□□ Azure SQL □□□□□□□ □□□ Azure □□□ □□□□. SQL1□□ □□ □□ □□□ □□ □□□□ □□□□.

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

SQL!□ Always Encrypted□ □□□□□ □□□□□.

□□□ □□□□ □□□□ □□□.

□□ □□ □□□ □□□□ □□□□□?

A. □4

B. □3

C. □2

D. □1

Answer: (SHOW ANSWER)

NEW QUESTION: 100
□+□□□□ □□□ □□□ □□□ Azure □□□ □□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

VNet1□ VNet2□ □□ □□ □□□□ □□□ □□□□□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
* VNet1□ □□□□ □□□□ □□ □□□ Microsoft □□ □□□□□ □□□□ storage1, storage2 □ Azure AD□ □□□□□ □□□.
* VNet2□ □□□□ □□□□ □□ □□□ Microsoft □□ □□□□□ □□□□ storage1□ KeyVault1□ □□□□□ □□□.
* □□ □□□ VNet1□ VNet2 □ □□□ □□ Microsoft □□ □□□□□ □□□□ □□□.
□ □□ □□□□□ □□ □ □□ □□□ □□□□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 101

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

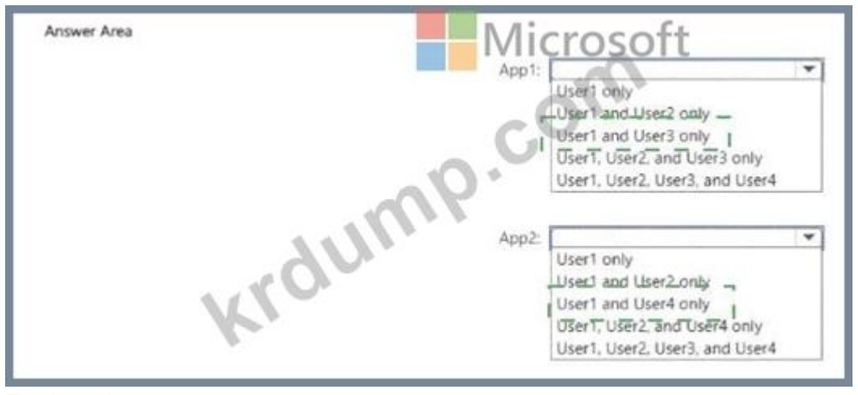
Name	Role
User1	Application Administrator
User2	Application Developer
User3	Azure DevOps Administrator
User4	Security Operator

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

Name	Owner	Users and groups
App1	User3	User4
App2	User4	User3

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

Answer:



Explanation:

NEW QUESTION: 102

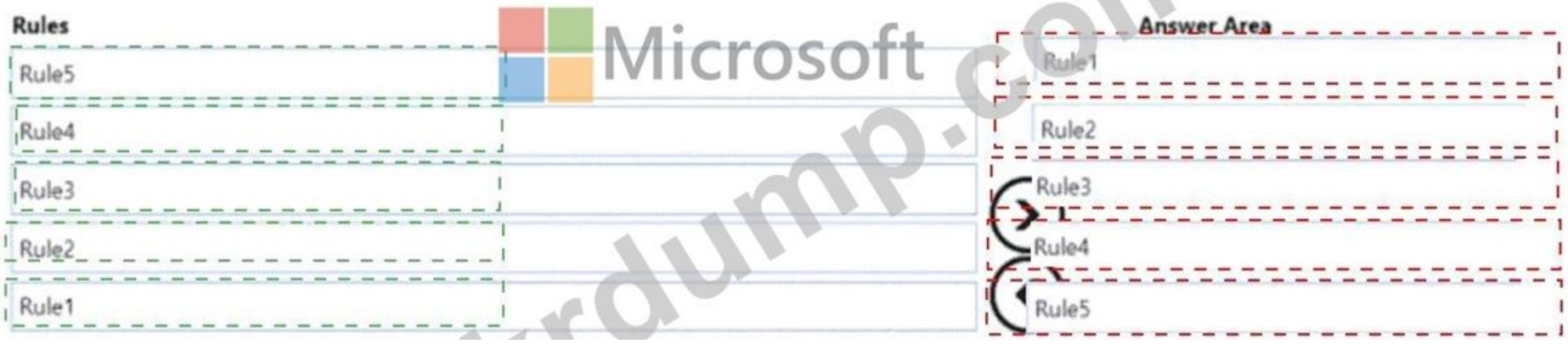
Azure □□□ □□□□.

□□ □□ □□□ □□□ □□□ Azure □□□ □□□ □□□□.

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

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

Answer:



Explanation:

The rules should be processed in the following order:

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

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

NEW QUESTION: 103

100□□ □□ □□□ □□□ Azure □□□ □□□□. □□ □□ □□□□ Azure □□□ □□□□□ □□□□.

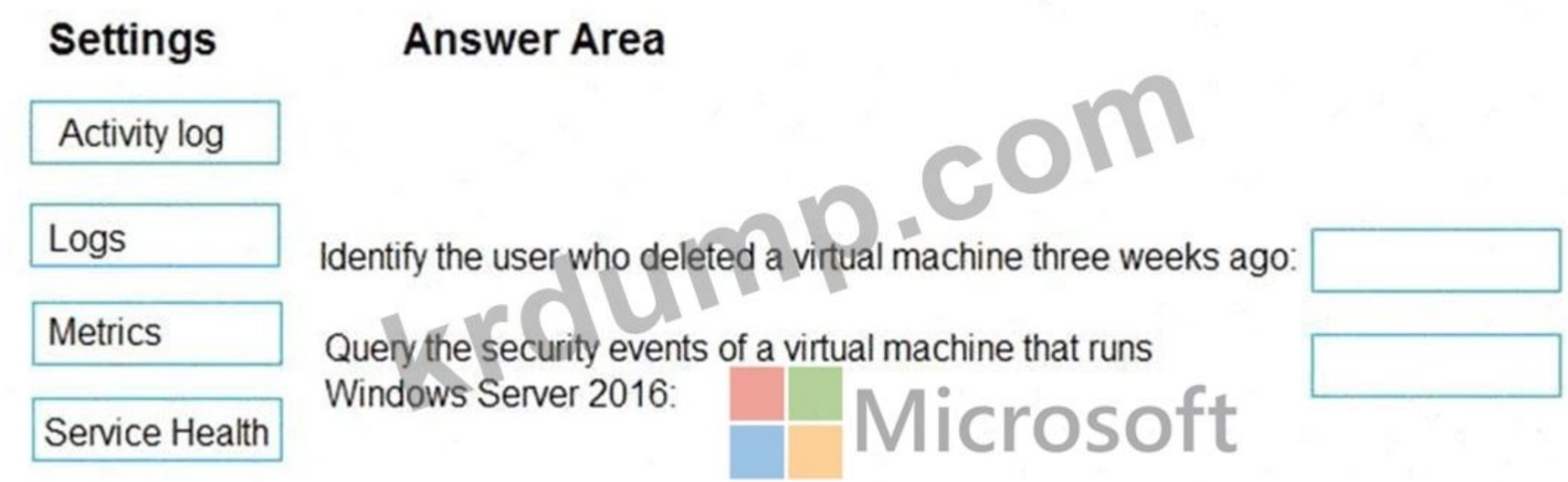
□□□□ Azure □□□ □□□□□ □□□□ □□□□.

□□ □□ □□□ □□□□ □□□.

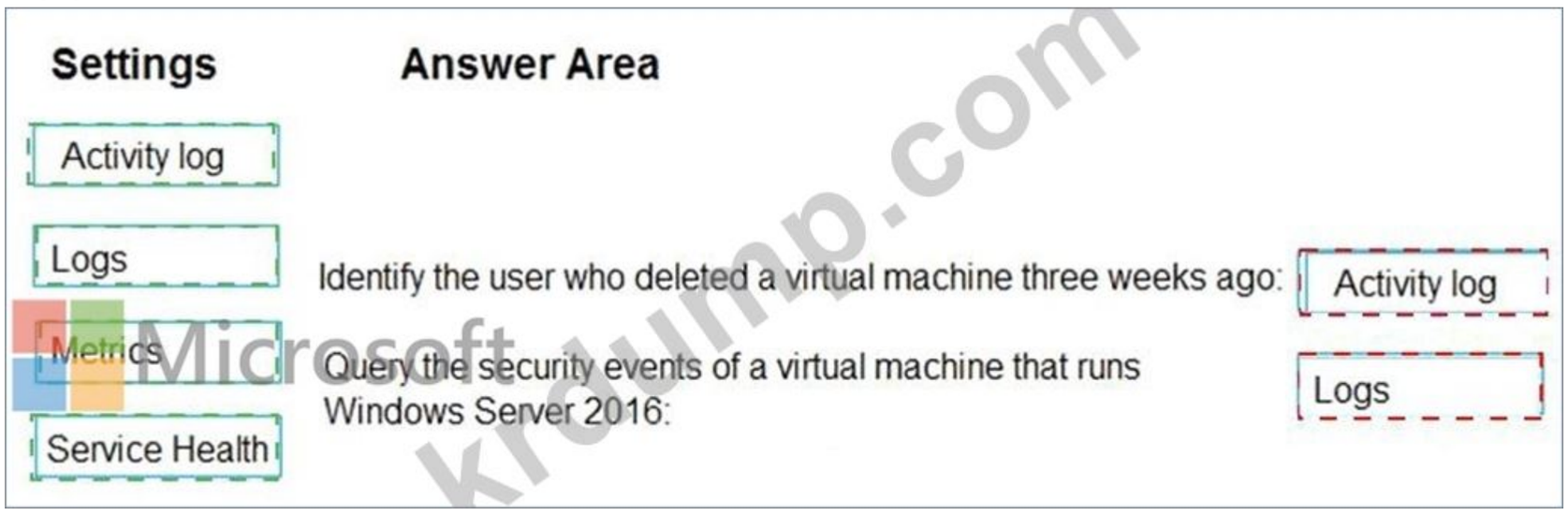
* 3□ □□ □□ □□□ □□□ □□□□ □□□□□.
* Windows Server 2016□ □□□□ □□ □□□ □□ □□□□ □□□□□.

Azure Monitor□□ □□□ □□□□ □□□? □□ □□□□ □□□ □□ □□□ □□□ □□ □□□ □□□ □□□□. □ □□ □□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□. □□□□ □□□ □ □□□ □□ □□□ □□□ □□□ □□□□□ □ □□ □□□□.

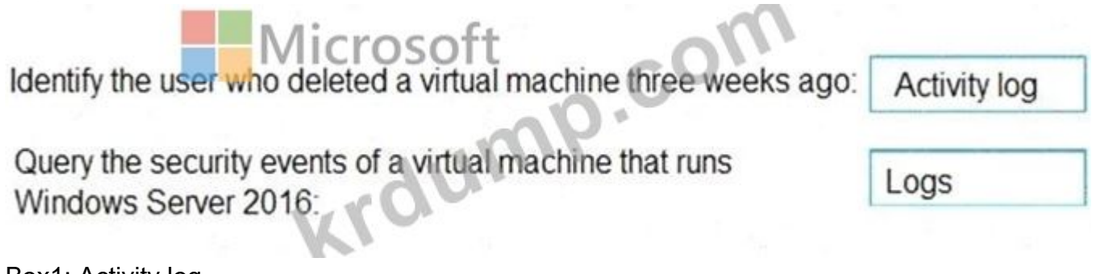
□□: □□ 1□□ 1□□□□.



Answer:



Explanation:



Box1: Activity log

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

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

Activity logs help you determine the "what, who, and when" for write operations (that is, PUT, POST, or DELETE).
Box 2: Logs
Log Integration collects Azure diagnostics from your Windows virtual machines, Azure activity logs, Azure Security Center alerts, and Azure resource provider logs. This integration provides a unified dashboard for all your assets, whether they ' re on-premises or in the cloud, so that you can aggregate, correlate, analyze, and alert for security events.
References:
https://docs.microsoft.com/en-us/azure/security/azure-log-audit

NEW QUESTION: 104
□□□ ExpressRoute □□□ □□ □□□ □□□□ □□□□ □□□. □□ □□□□ □□ □□ □□□ □□□□ □□□.
□ □□□ □□□ □□ □□ ExpressRoute □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.

Answer:

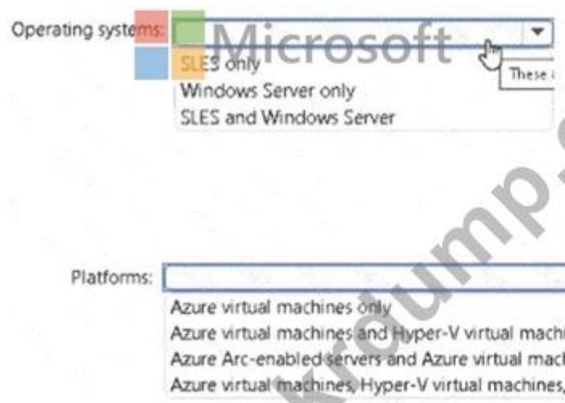
Explanation:

NEW QUESTION: 105

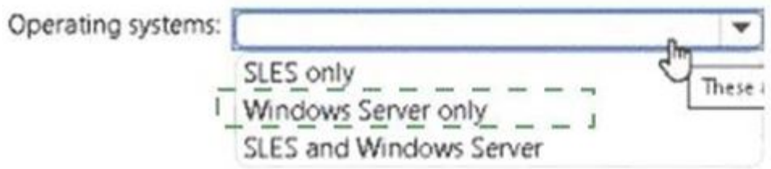
□□□□□ □□□□□□ □□ □□ □□□ □□□ □□□□ □□□□.

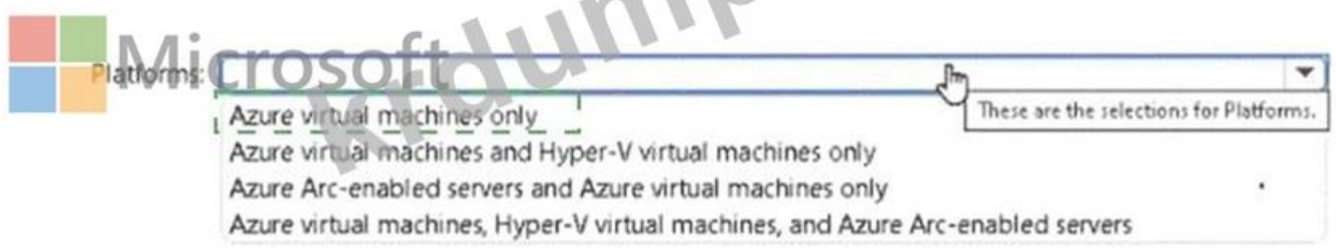
Name	Operating system	Description
Server1	Windows Server 2019	Hyper-V host hosting four virtual machines that run Windows Server 2022
Server2	Windows Server 2019	File server that has the Azure Arc agent installed
Server3	SUSE Linux Enterprise Server (SLES)	Database server that has the Azure Arc agent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

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



Answer:





NEW QUESTION: 106
Azure AD □□□□ □□□□.
□□ □□ □□□ □□□□ □□ □□ □□□□ □□□ □□□□□.
* □□ □□□ □□□□□.
* □□□ □ □□□ □□□ □□□□□.
□□□□ □□ □□ □□□ □□□□ □□□?
A. Microsoft □□□
B. FID02 □□ □
C. □□
D. □□ □□□
Answer: D (LEAVE A REPLY)

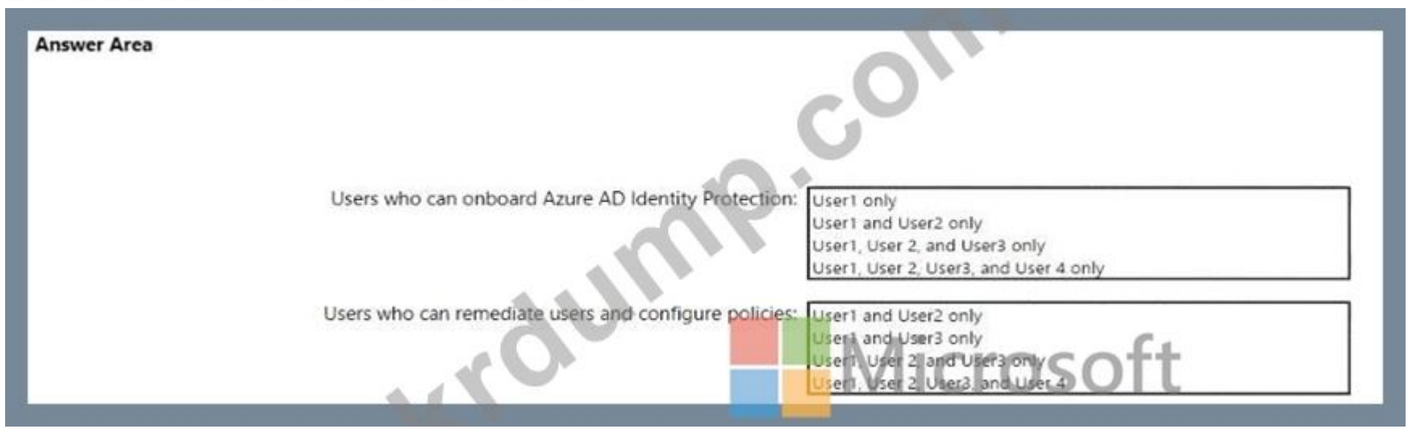
NEW QUESTION: 107
□□□ Azure DevOps□ □□□□ □□□□.
□□□ □□□ □□ □□□ □□ □□ □□□ □□□□□ □□□□ □□□ □□□□ □□□.
Azure DevOps□ □□□□ □ □□□ □□□□ □□□?
A. □□□ □□
B. □□ □□

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

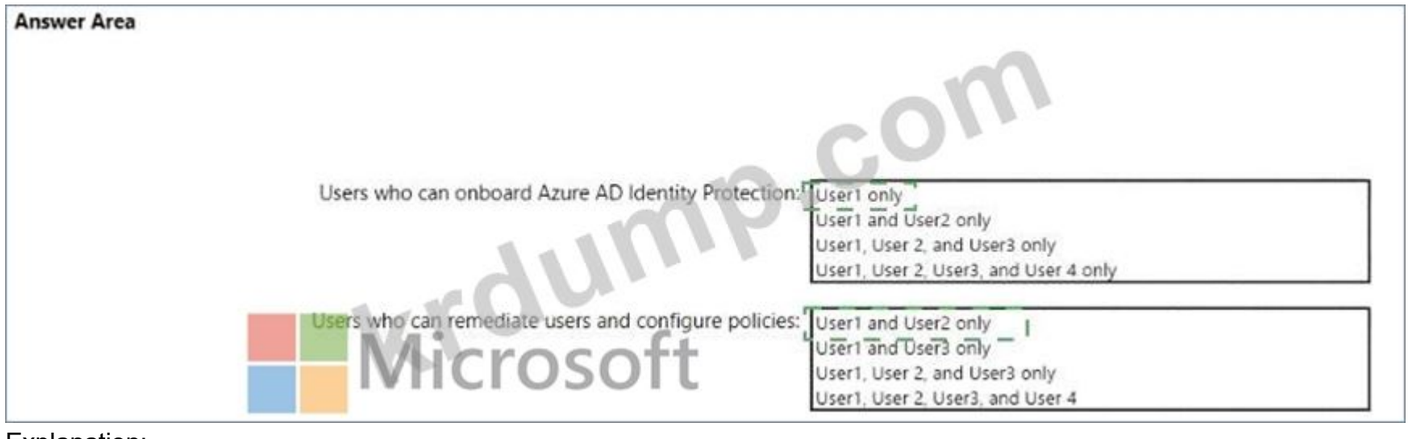
NEW QUESTION: 108
contoso.com□□□ Azure Active Directory(Azure AD) □□□□ □□□ Sub 1□□□ Azure □□□ □□□□. □□ □□□□□ □□ □□ □□ □□ □□□□ □□□□ □□□□.

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

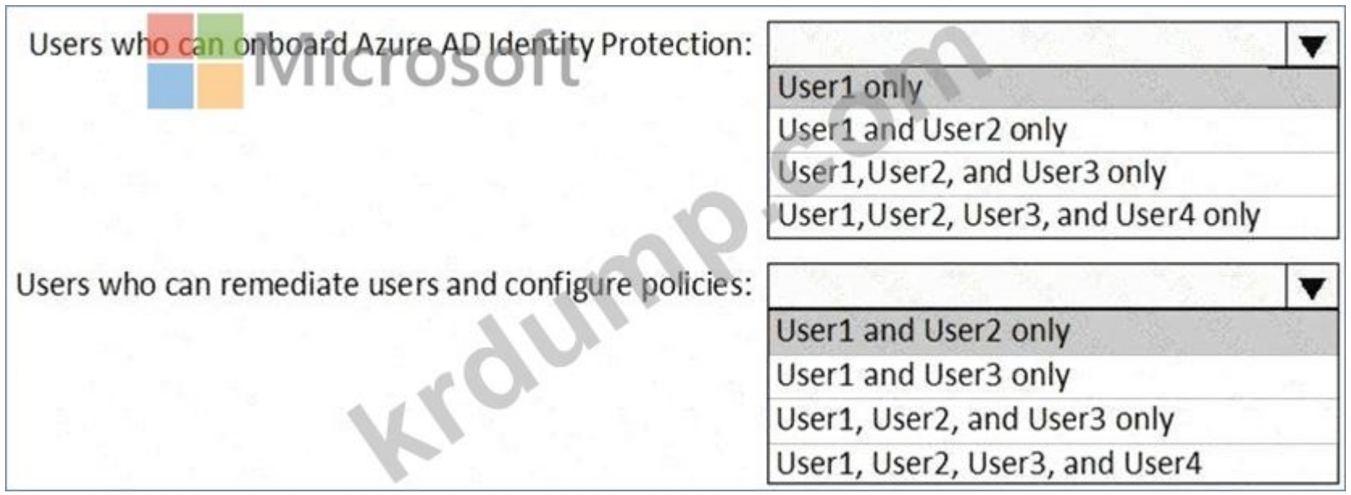
□ □□□□□ Azure AD Premium P2 □□□□□ □□□□□.
Azure AD ID □□□ □□□□□ □□□ □□□□□.
□□ □□□□ Azure AD Identity Protection□ □□□□□, □□□□ □□□□, □□□ □□□ □ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□□ □□ □□□□ 1□□ □□□ □□□□.



Answer:



Explanation:



NEW QUESTION: 109
Azure Active Directory(Azure AD) □□□□ □□ □□ □□□ □□□□.
Azure □□ 10□□ □□□ □□ □□□ □□□ □□ □□□ □□□□□.
□□ □□ □□□ □□□ Azure Blueprints □□□ □□□□ □□□.
□□ □□ □□□ □□ □□□?
A. □□ □□ □□□ Azure □□ □□□ □□□□□.
B. □□ □□ □□□ □□ □□ □□ □□□ □□(RBAC) □□ □□□ □□□□□.
C. □□□□□ □□□ ID□ □□□□□.
D. □□□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin

NEW QUESTION: 110
Azure □□ □□ Sub1□ Policy1□□□ Azure Policy □□□ □□□□ □□□□. Policy1□ □□□ □□□ □□□□.
* □□ □□: □□□ □□ □□
* □□□□ : □□□□
Policy1□ □□□□ □□ □□□□ Azure Security Center □□□□□ □□□□ □□□ □□□□ □□□.
□□ □□ □□□ □□ □□□?
A. Policy1□ □□□□□ □□ □□□ □□□□□.
B. □□□ □□ □□□□□□ Policy1□ □□□□□.
C. Policy1□ □□ □□□ Sub1□ □□□□□.
D. Sub1□ Policy1□ □□□□□.
Answer: D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/overview

NEW QUESTION: 111
ContosoAPI1□□□ Azure API Management □□□□□ □□□ Azure □□□ □□□□.
ContosoAPI1□ □□ SSL 3.0 □□□ □□□□ □□□.
Azure Portal□□ □□ □□ □□□ □□ □□□?
A. □□□□□ □□□□ □□□□□.
B. □□ □□ □□□□ □□ □□ □□□ □□□□□.
C. □□□□ + □□□□ □□□ □□□□□ □□□□□.
D. API□□ API □□□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 112
□□ □□ □□□ □□ □□□ □□□ Azure □□□ □□□□.

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

□□ □□□ □□ □□□ cosmos1□□□ Azure Cosmos DB □□□ □□□□.

Statements	Yes	No
VM1 can access cosmos1 over the internet.	○	○
VM2 can access cosmos1 over the internet.	○	○
VM3 can access cosmos1 over the internet.	○	○

Answer:

Statements	Yes	No
VM1 can access cosmos1 over the internet.	○	○
VM2 can access cosmos1 over the internet.	○	○
VM3 can access cosmos1 over the internet.	○	○

Explanation:
Yes, Yes, No

NEW QUESTION: 113
Group1□□□ □□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□. Group1□ □□□□ □□ □□ □□□ □□□□ □□□□□□ □□ □□□. □□□ □□ □□□?
A. □□□ □□ □□(CBA) □□□ □□□□□.
B. Microsoft Authenticator □□ □□ □□□ □□□□□.
C. □□□ □□ □□□ □□□□□.
D. □□□ □□□ □□□ □□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 114
Azure □□□ □□□□.
Microsoft Sentinel□ □□□□ □□ □□□ □□□ □□□□□.
□□ □□ □□□ □□□□ □□ □□□ □□□□ □□□.
* □□ 1: CEF(Common Event Format) □□□ syslog □□□□ □□□, IP □□, URL □□□□ □□□□ □□□□□□.
* □□ 2: Microsoft□ □□ □□□□□ □□□□□.
□ □□□ □□ □□ □□□ □□□ □□□□ □□□? □□ □□□□ □□□ □□□ □□□□ □□□□□.
□□: □□ 1□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 115

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

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

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

A. Vault1 □ storage1 □□

B. VM1 □□

C. VNet1, VM1, Vault1 □ storage1

D. VM1 □ storage1□ □□

E. VM1, Vault1 □ storage1□ □□

Answer: C (LEAVE A REPLY)

NEW QUESTION: 116

Azure □□□ □□□□.

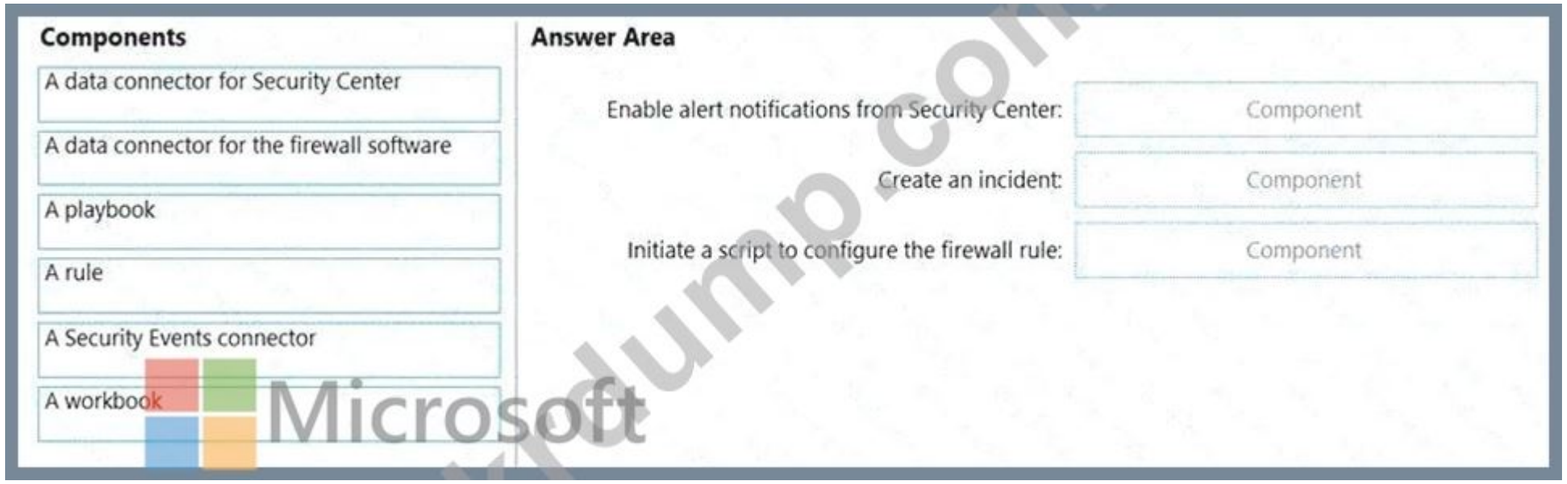
VNet1□□□ □□□ □□□ □□ □□□□□ □□□□.

VNet1□ □□□□ □□ IP □□□ □□ □□□ □ □□ App1□□□ Azure □□□ □□□ □□□□□. □□□□ □□□□ □ □□□□□ □□□□ □□□□ □□□□ □□□.

□□□ □□ □□□?

A. Azure □□□□□□ □□□□□□ □□□□.
B. Azure App Service □□□□□ □□□ □□□□.
C. □ □□□ □□ □□
D. □□ □□ □□□□ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 117
□□ □□□□ □□□ Azure □□□ □□□□.
* Microsoft □□□ □□□□□□ □□ □□□□□□ □□□□ □□ □□□□ □□□□□ □□□ □□ □□□□ □□□□□ □□□□ □□ □□□□□□(NVA)
* NVA□ □□□ □□□ □□□□ □□□□□ □□□ Azure □□
* □□ □□ □□□ □□ Azure Security Center □□ □□□ □□□□
* Azure Sentinel □□ □□
* 30□□ □□ □□
□□ □□□ □□ Security Center□□ □□ □□ □□ □□□ □□□□ Azure Sentinel□□ □□□□□ □□□ □□ NVA□ □□ □□□ □□□ □□□□ □□□□□ □□□□□ □□□□ □□□.
□□ □□□ □□□□□ Azure Sentinel□ □□□ □□□□ □□□? □□ □□□□ □□□ □□ □□□ □□□ □□ □□□ □□ □□□□□. □ □□ □□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□ □□.
□□□□ □□□ □ □□□ □□ □□□ □□□ □ □□ □□ □□□□□ □ □□ □□□□.
□□: □□ 1□□ 1□□□□.



Answer:

Explanation:

Reference:

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

https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

NEW QUESTION: 118

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

Amazon Web Services(AWS) □□□ □□□□.

□□□ AWS Elastic Compute Cloud(EC2) □□□□□ □□□ □ Microsoft Defender for Servers □□□□□ □□□□ □□□□□ □□□□ □□□.

□□ □□□ □□□□ □□□?

A. Azure Monitor □□□□

B. □□□□ □□□□ □□□

C. □□ □□ □□□□

D. □□□ □□□□ □□□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 119

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

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group2

□□ □□□ □□□□ □□□ □□□ □□□ □□□□□.

* □□: CAPolicy1

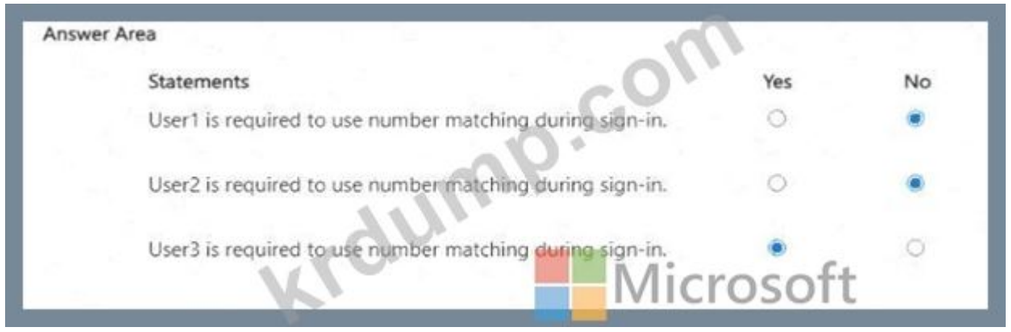
* □□
o □□□ □□ □□ ID: □□1
o □□ □□□: □□ □□□□ □
* □□ □□
o □□□ □□: □□ □□ □□ □□
□□□□ □□ Microsoft Authenticator □□□□ □□ □ □□ □□□ □□ □ □□ □□□ □□□ □□ □□□□□. (□□ □ □□ □□ □□□□□.)

□□□□ □□ Microsoft Authenticator □□□□ □□ □□□ □□ □□□ □□□ □□ □□□□□. (□□ □□ □□□□□.)

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

Answer:

Explanation:



NEW QUESTION: 120

□□□ □□ □□□□ □□□□ □□ □□□□ □□□□□.

* □□□
* □□□ □ □□□(AWS)
* □□ □□□□ □□□(GCP)

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

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

□□: □□ 1□□ 1□□□□.

Answer Area

Answer:

Answer Area

Explanation:

Answer Area

NEW QUESTION: 121

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

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

□□ □□□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Answer:

Explanation:

NEW QUESTION: 122

WAF1□□□ Azure Application Gateway □ □□□□□□ □□□(WAF)□ □□□□ □□□□.

□□□ □□ Bicep □□ □□□ □□□□.

```
resource AppGW_AppFW_Pol 'Microsoft.Network/ApplicationGatewayWebApplicationFirewallPolicies@2021-08-01' = {
  name: AppGW_AppFW_Pol_name
  location: location
  properties: {
    customRules: [
      {
        name: 'CustRule01'
        priority: 100
        ruleType: 'MatchRule'
        action: 'Block'
        matchConditions: [
          {
            matchVariables: [
              {
                variableName: 'RemoteAddr'
              }
            ]
            operator: 'IPMatch'
            negationConditon: true
            matchValues: [
              '10.10.10.0/24'
            ]
          }
        ]
      }
    ]

    policySettings: {
      requestBodyCheck: true
      maxRequestBodySizeInKb: 128
      state: 'Enabled'
      mode: 'Detection'
    }
    managedRules: {
      managedRuleSets: [
        {
          ruleSetType: 'OWASP'
          ruleSetVersion: '3.2'
        }
      ]
    }
  }
}
```


Microsoft

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

Answer Area

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

Answer:

Answer Area

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

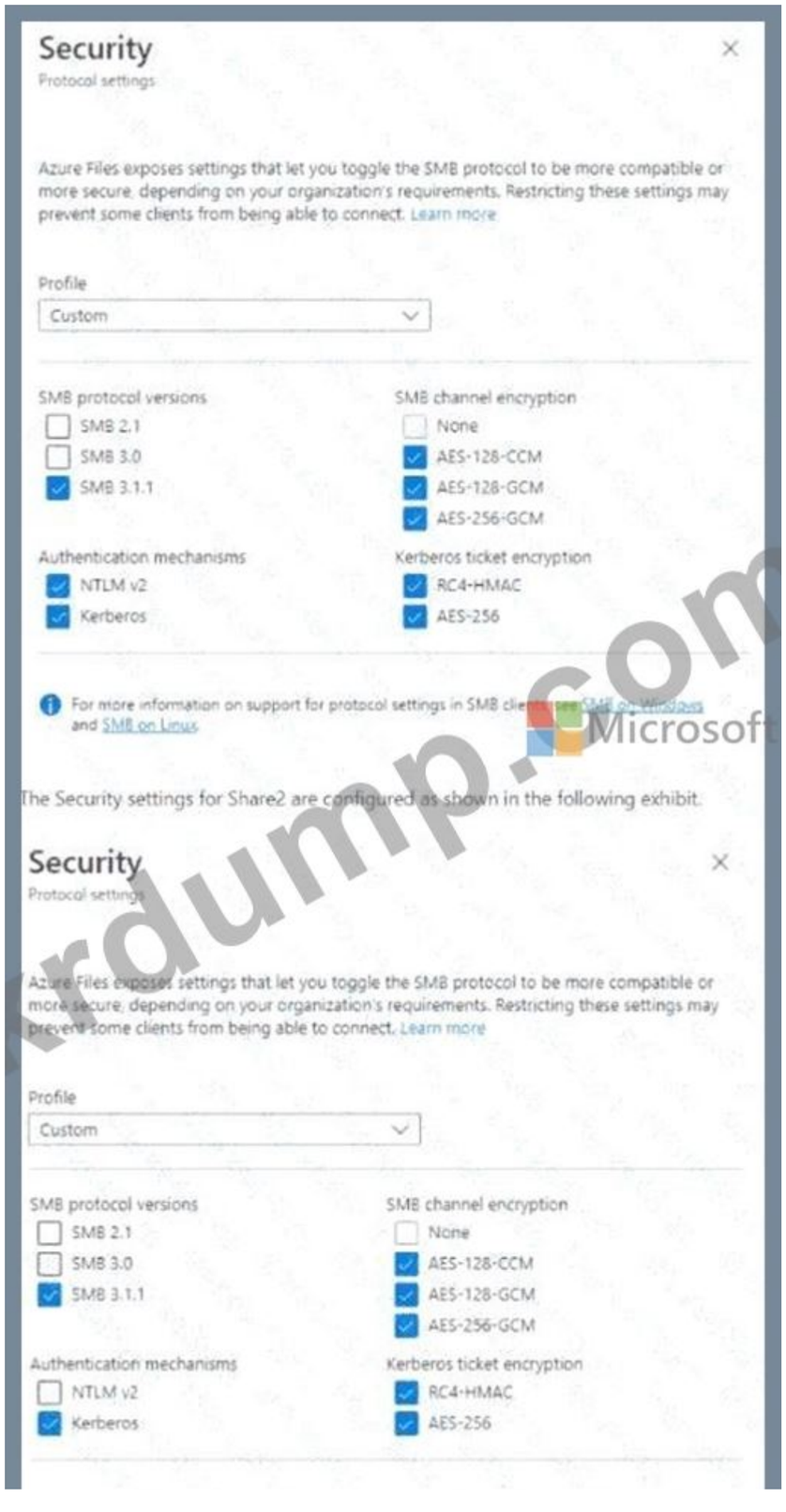
Explanation:

Answer Area

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

NEW QUESTION: 123
□□□□□ □□□□□□ Active Directory □□□ □□□(AD DS) □□□□ □□ □□ □□□ □□□ □□□□ □□□□.
User1□□□ □□□□ □□□□ □□□ □□□□□ Microsoft Entra □□□□ □□□□.

□□ □□ □□□ Azure Files □□□ □□□ Azure □□□ □□□□.
storage1□ storage2□ □□ □□ □□□ SMB □□ □□□ □□□ □□□□□□□□.
Share!□ □□ □□□ □□ □□□ □□ □□□□□.

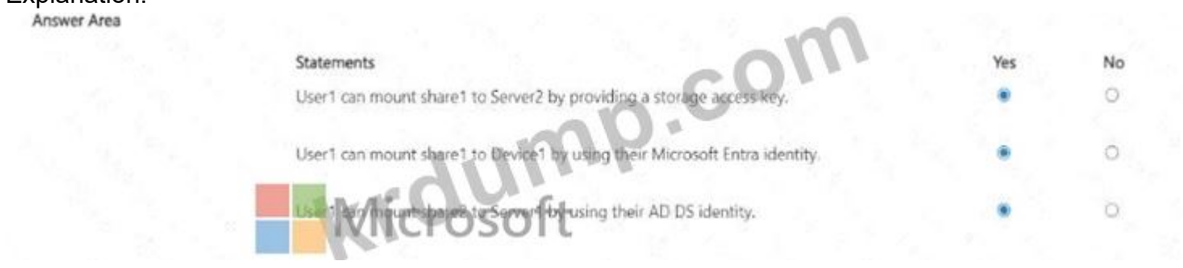


The Security settings for Share2 are configured as shown in the following exhibit.

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

Answer:

Explanation:



NEW QUESTION: 124
□□□ □□
□□□ □□ □□ □□□ □□ □□□ □□□□□.
□□□ □□□ □□□□□ □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
□□□□□ □□□□□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□ □□□□□.
Azure □□□ □□: Userl -28681041@ExamUsers.com
Azure □□□□: GpOAe4@lDg
Azure Portal□ □□□□□ □□□□□ □□□□ □□□ CTRL-K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.
□□ □□□ □□ □□ □□□□□ □□□□□.
□□□ □□□□: 28681041

□□ 6

VM1□□□ □□ □□□ □□ CPU □□□□ 15□ □□ 70%□ □□ □□ adminl@contoso.com□□□ □□□□□ □□ □□□□ □□□ □□□.

Answer:

Check below steps in explanation for Task.

Explanation:

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

* In the Azure portal, search for and select the virtual machine named VM1.
* In the left pane, select Alerts.
* Select New alert rule.
* In the New alert rule pane, enter the following information:
* Name: Enter a name for the alert rule.
* Description: Enter a description for the alert rule.
* Condition: Select Metric measurement.
* Resource: Select the virtual machine named VM1.
* Metric: Select Percentage CPU.
* Operator: Select Greater than.
* Threshold: Enter 70.
* Aggregation type: Select Average.
* Period: Select 15 minutes.
* In the Actions pane, select Add action group.
* In the Add action group pane, enter the following information:
* Name: Enter a name for the action group.
* Short name: Enter a short name for the action group.
* Email recipient: Enter the email address of the user you want to receive the alert. For example, adminl@contoso.com.
* Select OK.

NEW QUESTION: 125

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

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

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

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

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

□□□ □□ □□□ □□□□□?

A. □

B. □□□

Answer: A (LEAVE A REPLY)

NEW QUESTION: 126

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

Name	Type
User1	User
User2	User
User3	User
Group1	Security group
Group2	Security group
App1	Enterprise application

User2□ Group2□ □□□□□□.

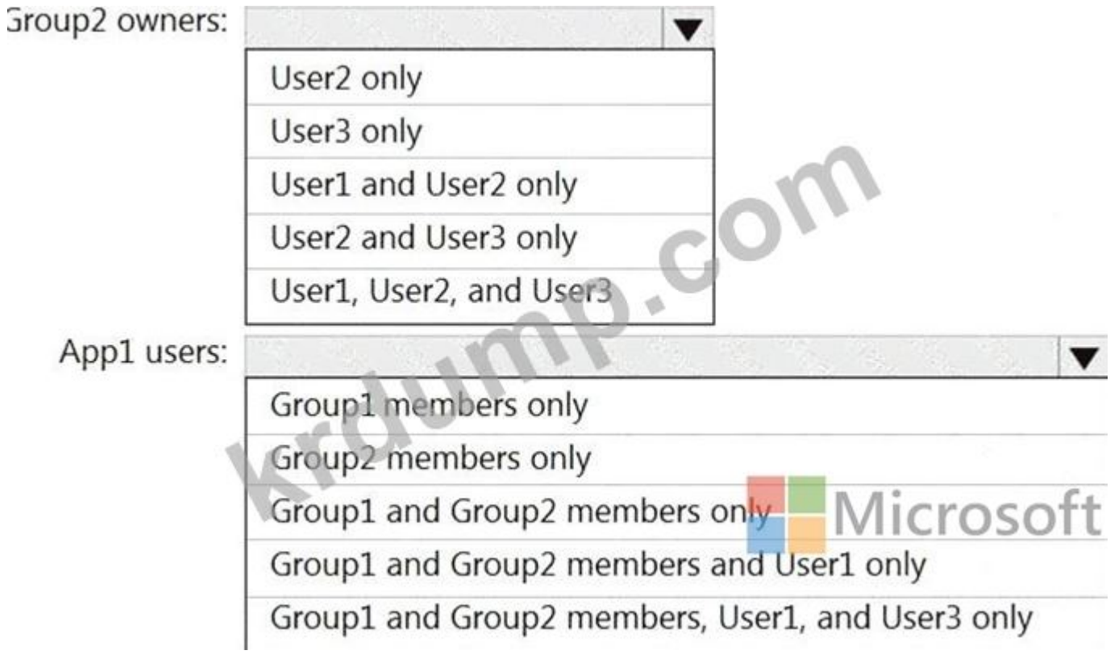
App1□ □□□ □ □□ □□□ □□ □□□ □□ □□□□□.

□□ □□□ □□ App1□ □□ □□ □□□ □□□□□□ □□□□ □□□□□□.

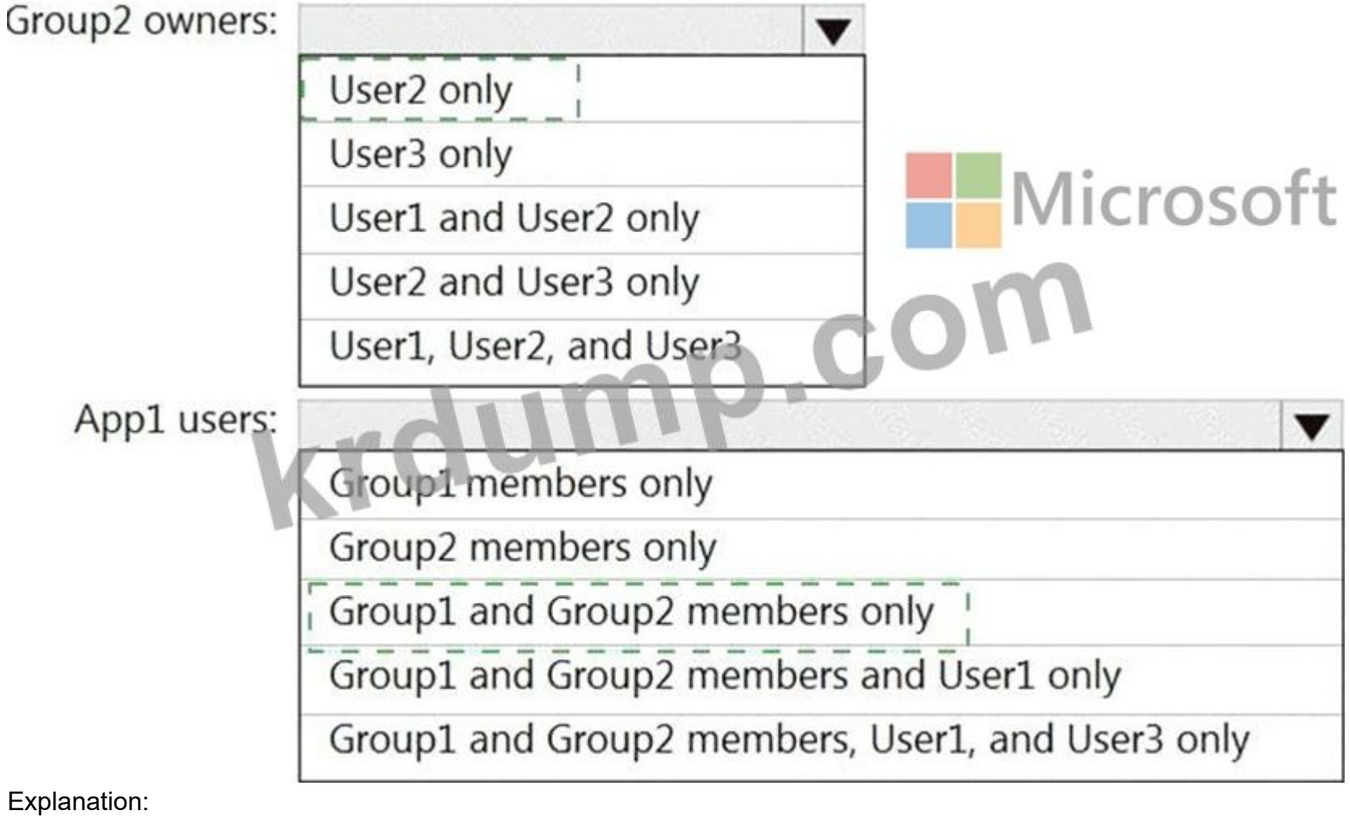
User3□ Appl□ □□ □□□□ □□□□□ □□□□□.

Group2□ □□□□ Appl□ □□□□ □□□□ □□□.

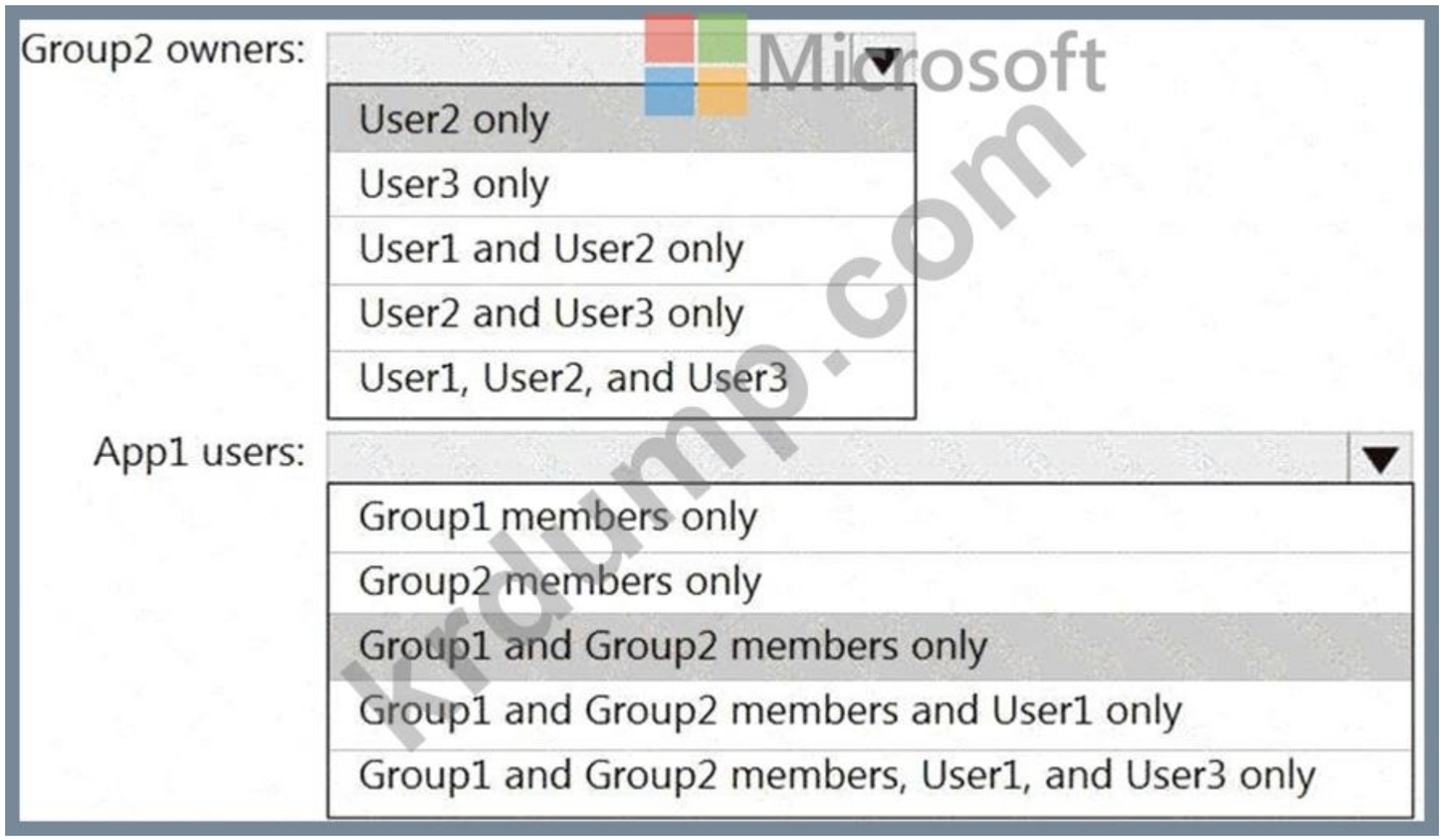
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.



Answer:



Explanation:



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

NEW QUESTION: 127
□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

Name	Type
User1	Azure Active Directory (Azure AD) user
User2	Azure Active Directory (Azure AD) user
Group1	Azure Active Directory (Azure AD) group
Vault1	Azure key vault

User1□ Group1□ □□□□□□. Group1□ User2□ Vault1□ Key Vault □□□ □□□ □□□□□□.
2019□ 1□ 1□□ Vault1□ □□□ □□□□□. □□□ □□□ □□ □□□□□. ('□□' □□ □□□□□.)

User2□□ Vault1□ □□ □□□ □□□ □□□□□□□. □□ □□□ □□□ □□□ □□□□.

* □ □□ □□: □□□□, □□ □ □□
* □□□ □□: □ □□□ □ □□
* □□ □□ □□: □□□□, □□ □ □□

□□1□ Vault1□ □□ □□□ □□□ □□□□□□□. □□ □□□ □□□ □□□□.

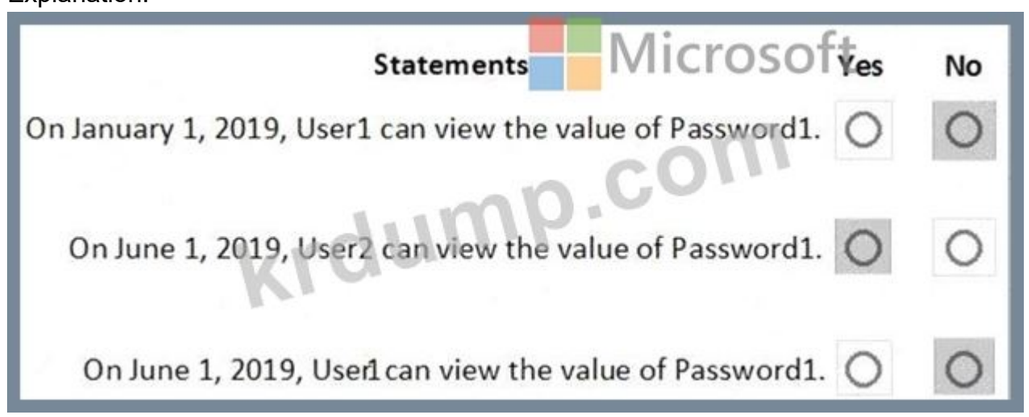
* □ □□ □□: □□□□ □ □□
* □□ □□ □□: □□, □□ □ □□

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

Statements	Yes	No
On January 1, 2019, User1 can view the value of Password1.	○	○
On June 1, 2019, User2 can view the value of Password1.	○	○
On June 1, 2019, User1 can view the value of Password1.	○	○

Answer:

Explanation:



NEW QUESTION: 128

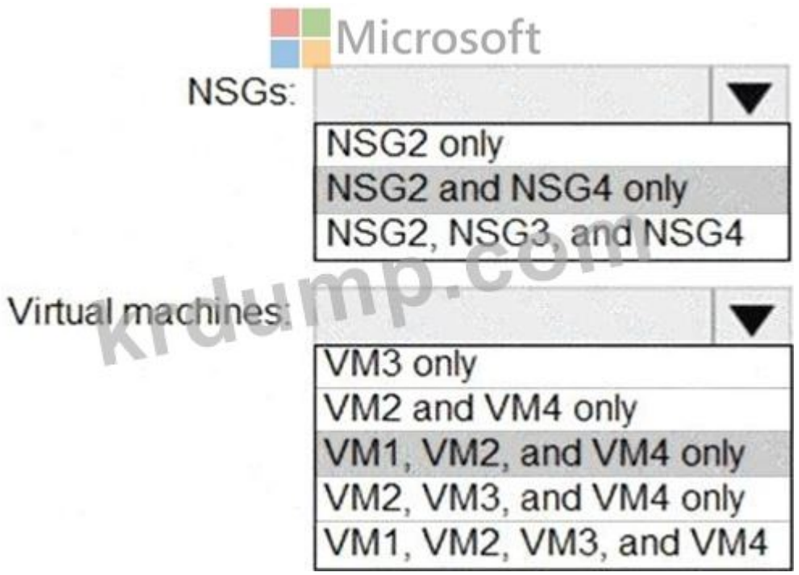
ASG1□ ASG2□ □□ □□□ □□ □□□ □□□□□.

□□ NSG□□ ASG1□ □□□ □ □□□? □□□ □□ □□ □□□ □□□□ □□□□□□ ASG2□ □□□ □ □□□?

Answer:

Explanation:

Graphical user interface, text, appli cation, chat or text message Description automatically generated



Topic 4, Fabrikam, Inc.

Case Study

Overview

Existing Environment

Network Environment

Cloud Environment

Sub1 Resources

Fabrikam, Inc. is a consulting company. The company has a main office in New York City and branch offices in Amsterdam and Singapore.

The on-premises network contains a datacenter in each office.

Fabtikam has two Azure subscriptions named Sub1 and Sub2 and a Microsoft 365 subscription that includes Microsoft 365 E5 licenses.

All the subscriptions are linked to a Microsoft Entra tenant named fabrikam.com that contains the identities shown in the following table.

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

The tenant contains the groups shown in the following table.

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

All devices are enrolled in Microsoft Intune.

Sub2 Resources

Sub1 contains a resource group named RG1 that contains the resources shown in the following table.

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

SQLServer1 uses Microsoft SQL Server authentication.

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

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

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

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

Planned Changes and Requirements

Planned Changes

Sub2 contains a resource group named RG2.

Fabtikam plans to implement the following changes:

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

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

* For RG1. create a new Privileged Identity Management (PIM) eligible role assignment that assigns the Contributor role to supported groups.

Technical Requirements

Fabrikam has the following technical requirements:

* If VM1 is deleted, the permissions for VM1 must be removed automatically.
* The AKS1 managed identity must only be able to pull images from Registry1.
* The ID1 managed identity must be able to push images to and pull images from Registry 1.
* All the data in the storage accounts must be encrypted by using Fabrikam-managed keys.
* All outbound traffic from the function apps to the on-premises network must use ExpressRoute circuits.
* ExpressRoute connectivity between the on-premises network and the Azure environment must be encrypted by using Layer 2 or Layer 3 encryption.

NEW QUESTION: 129

Azure □□□ Sentinel 1□□□ □□□ Microsoft Sentinel □□ □□□ □□□□. Sentinel!□ Microsoft 365□ □□ □□ □□ □□□□ □□□□□ □□□□□.
Sentinel 1□□ □ □□□□□ □□□□ □□□. □□□□ □□□ □□ □□□ □□□□ □□□.
□□ □□□ □□□□□ □□□□ □□□?

A. □□□ □□□□ □□□ □□□□
B. □□□□ □□□ □□ □□ □□□□ □□□ □□□□
C. □□□□ □□□□ □□ □□□□
D. □□ □□□ □□ □□□ □□□□ □□□ □□□□
E. □□ □□□□ □□ □□□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 130

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □ □ □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□□ □□□□.
Azure Security Center□ □□□□ □ □□ Azure □□□ □□ □□ □□□ □□ □□□ □□□□□.
□□□ □□□ □□□□□ □□ □□ □□ □□□ □□□□□.
□ □□ □□ □□□ □□ □□□ □□□□ □□□□ □□□.
□□ □□: □□□ □□ □□ □□ □□□ □□□ □□□ □□□□□□ □□□ □□□□.
□□□ □□□ □□□□□?

A. □
B. □□□

Answer: (SHOW ANSWER)

Reference:

https://docs.microsoft.com/en-us/azure/governance/policy/overview
https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management- groups/

NEW QUESTION: 131
contoso.com□□□ Azure AD □□□□ □□ Azure AD Premium P1 □□□□□ □□□□.
□□□ □□ □□□ □□□ Group1□□□ □□□ □□□□ □□□.
□□1□ □□□□ □□ □□□ □□□□ □□, □□ □□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□□ □□ □□□□ 1□□ □□□ □□□□.

Answer:

Explanation:

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

NEW QUESTION: 132

□□ □□ □□□ □□□ □□□□ KeyVault1□□□ Azure □ □□ □□ □□□ □□□□.

Name	Type
Item1	Key
Item2	Secret
Policy1	Access policy

KeyVault□□□ □□ □□□□ □□□□ □□□□□.

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

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

□□: □□ 1□□ 1□□□□.

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

Answer:

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

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

NEW QUESTION: 133
□□ □□ □□□ Azure Log Analytics □□ □□□ □□□ Azure □□□ □□□□.

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

□□ □□ □□□ □□ □□□ □□□□□.

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

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

NEW QUESTION: 134
Azure Active Directory(Azure AD) □□□□ User1□□□ □□□□ □□□ Azure □□□ □□□□.
□□□□ □□ □ □□ □□□ □□ □□ □□□ □□ □□□□□.

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

NEW QUESTION: 135
RG1□□□ □□□ □□□ Azure □□ □□□ 15□ □□□□.
□□ □□ □□□ □□□ □□□□□□□ □□□□□.
□□ □□□□ □□□□ □□ □□□□□□□ □□□□ □□□□ □□ □□□□ □□□.
□□□ □□ □□□?
A. Azure Active Directory(Azure AD) ID □□□ □□□□□.
B. Microsoft Defender for Cloud□□ □□□ □□□□□□ □□□ □□□□□.
C. RGI□ Azure □□□ □□□□□.
D. RGI□ □□□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)
Microsoft Defender for Cloud helps you prevent, detect, and respond to threats. Defender for Cloud gives you increased visibility into, and control over, the security of your Azure resources. It provides integrated security monitoring and policy management across your Azure subscriptions. It helps detect threats that might otherwise go unnoticed, and works with a broad ecosystem of security solutions.
Defender for Cloud helps you optimize and monitor the security of your virtual machines by:
* Providing security recommendations for the virtual machines. Example recommendations include:
apply system updates, configure ACLs endpoints, enable antimalware, enable network security groups, and apply disk encryption.
* Monitoring the state of your virtual machines.
https://learn.microsoft.com/en-us/azure/security/fundamentals/virtual-machines-overview

NEW QUESTION: 136
□□ □□ □□□ □□ □□□□□ □□□ Azure □□□ □□□□.

Name	Region	Subnet
VNET1	West US	Subnet11 and Subnet12
VNET2	West US 2	Subnet21
VNET3	East US	Subnet31

□□□□ □□ □□ □□□ □□ □□□ □□□□ □□□□.

Name	Network interface	Connected to
VM1	NIC1	Subnet11
VM2	NIC2	Subnet11
VM3	NIC3	Subnet12
VM4	NIC4	Subnet21
VM5	NIC5	Subnet31

NIC1□□ ASG1□□□ □□□□□□ □□ □□□ □□□□□.
□□ □□ □□□□ □□□□□□□ ASG1□ □□□ □ □□□?
A. NIC2□
B. NIC2, NIC3, NIC4 □ NIC5
C. NIC2 □ NIC3□ □□
D. NIC2, NIC3 □ NIC4□ □□
Answer: (SHOW ANSWER)
Only network interfaces in NVET1, which consists of Subnet11 and Subnet12, can be configured in ASG1, as all network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in.
Reference:
https://azure.microsoft.com/es-es/blog/applicationsecuritygroups/

NEW QUESTION: 137
Vault1□□□ Azure Key Vault□ VM1□□□ □□ □□□ □□□ Azure □□□ □□□□.
VM1□ VNet1□□□ □□ □□□□□ □□□□□.
VM1□□□ Vault1□ □□ □□□□ □□□□ □□□.
Vault1□ □□□□ □□□□ □□□ □□ □□□?
A. □□□ □ □□ □□□□ □□□ VNet1□ □□□□□.
B. □□□ □ □□ □□□□ □□□ Vault1□ □□ □□□ □ □□ Microsoft □□□□ □ □□□□ □□□□□ □□□ □□ □□□□□.
C. □□ □□□□□ □□ □□□ VM1□ □□ □□ □□□□□□ □□□□.
D. □□□ □ □□ □□□□ □□□ VM1□ IP □□□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 138
□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

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

□□ □□ □□□ □□ □□□ □□□ □□□□□.

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

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

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

Answer: (SHOW ANSWER)

We have two different sets of required permissions. VM1 and VM2 have the same permission requirements.
VM3 and VM4 have the same permission requirements.
A user-assigned managed identity can be assigned to one or many resources. By using user-assigned managed identities, we can create just two managed identities: one with the permission requirements for VM1 and VM2 and the other with the permission requirements for VM3 and VM4.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

NEW QUESTION: 139

Azure □□□ □□□□. □□□□ Windows Server□ □□□□ Azure □□ □□□ □□□□ □□□□.
2016□

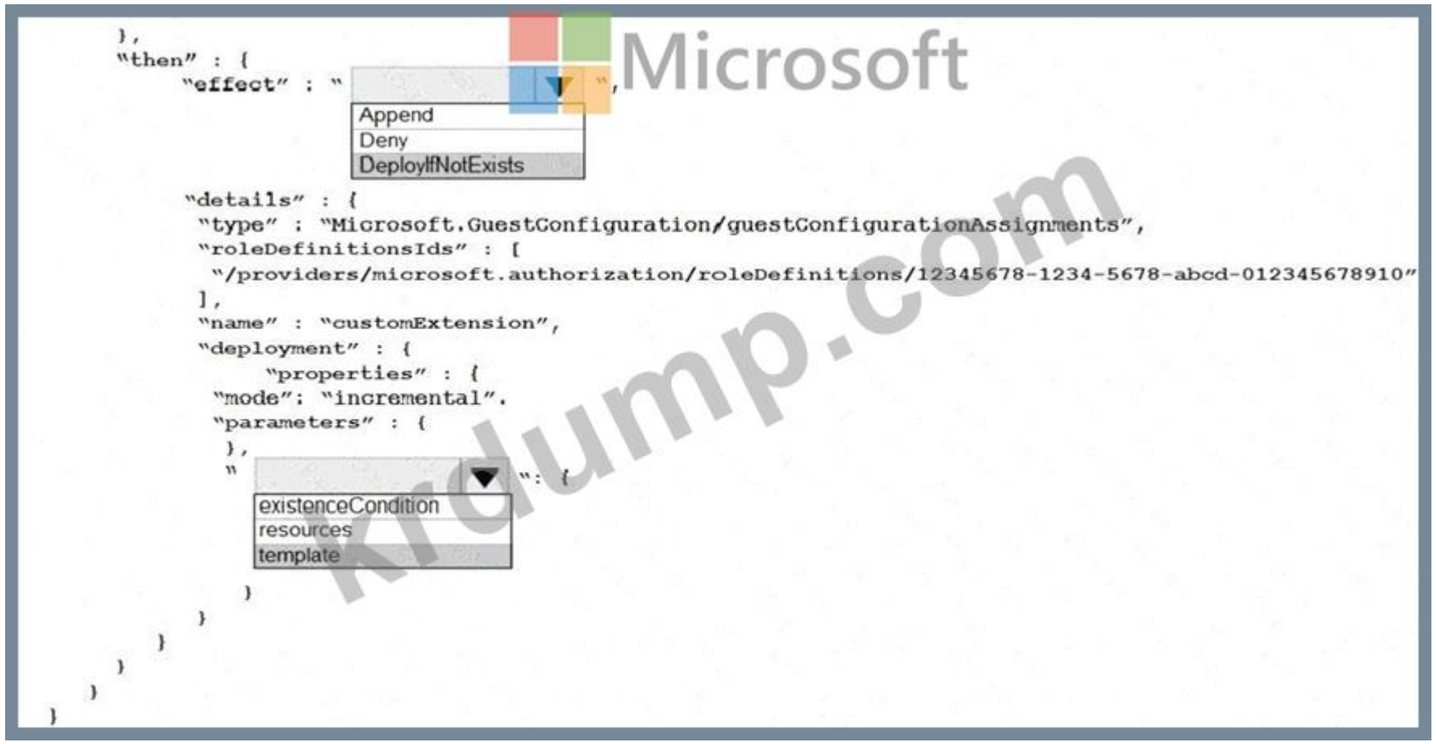
□ □□ □□□ □□□ □□ □□□ □□ □□ □□ □□ □□□□□ □□□□□ □□□ □□□□ □□□.
□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.

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

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


Answer:

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

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

Explanation:



Box 1: DeployIfNotExists

DeployIfNotExists executes a template deployment when the condition is met.

Box 2: Template

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

Deployment [required]

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

/deployment

References:

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

NEW QUESTION: 140

WebApp1□□□ Azure □□□ □□□□.

WebApp1□ □□□□ □□□□□□.WebApp1□ □ □□□□ □□□□ □□□ □

□□□ □□ □□□ .

□□□ □□ □□□?

A. WebApp1□ □□□□ □□□ □□ ID□ □□□□□.

B. WebApp1 □□□ □ □□□ □□□□□.

C. WebApp1□ □□ □□□□□ □□□ □□ ID□ □□□□□□.

D. WebApp1□ □□ TLS/SSL □□□□ □□□□□.

Answer: (SHOW ANSWER)

Reference:

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

NEW QUESTION: 141
WebApp1□□□ □ □□ □□□□.
□ □□□□□□ □□□(WAF) □□□ WAF1□□□ □□□□ □□□□□.
WebApp1□ WAF1□ □□□□ □□□□ □□□.
□□□ □□ □□ □□□?
A. Azure □□□□ □□□□□.
B. WebApp1□ □□ □□□ □□□□□.
C. Azure Front Door□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 142
VM1□□□ □□ □□□ □□□ Azure □□□ □□□□.
□□ □□□ □□ Azure Key Vault□ □□□□.
* □□: Vault5
* □□: □□ □□
* □□□ □□: RG1
VM1□□ Azure Disk Encryption□ □□□□□□ Vault5□ □□□□ □□□. □□□□ Azure Backup□ □□□□ VM1□ □□□ □ □□□ □□□.
□□ □ □□□ □□□ □□□□ □□□?
A. □□□ □□
B. □□
C. □
D. □□ □□
Answer: (SHOW ANSWER)
References:
https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

NEW QUESTION: 143
□□ □□ □□ □□ Azure Firewall □□□ □□□ Azure □□□ □□□□.

Name	Type
Policy1	Standard
Policy2	Premium

□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	Tier	Policy
FW1	Premium	Policy2
FW2	Premium	Policy1

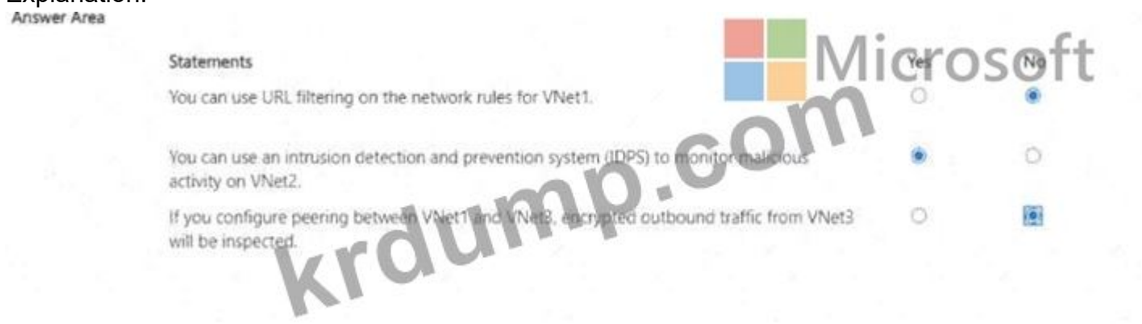
□□□□ □□ □□ □□□ □□ □□□□□ □□□□ □□□□.

Name	Firewall
VNet1	FW1
VNet2	FW2
VNet3	*None*

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

Answer:

Explanation:



NEW QUESTION: 144

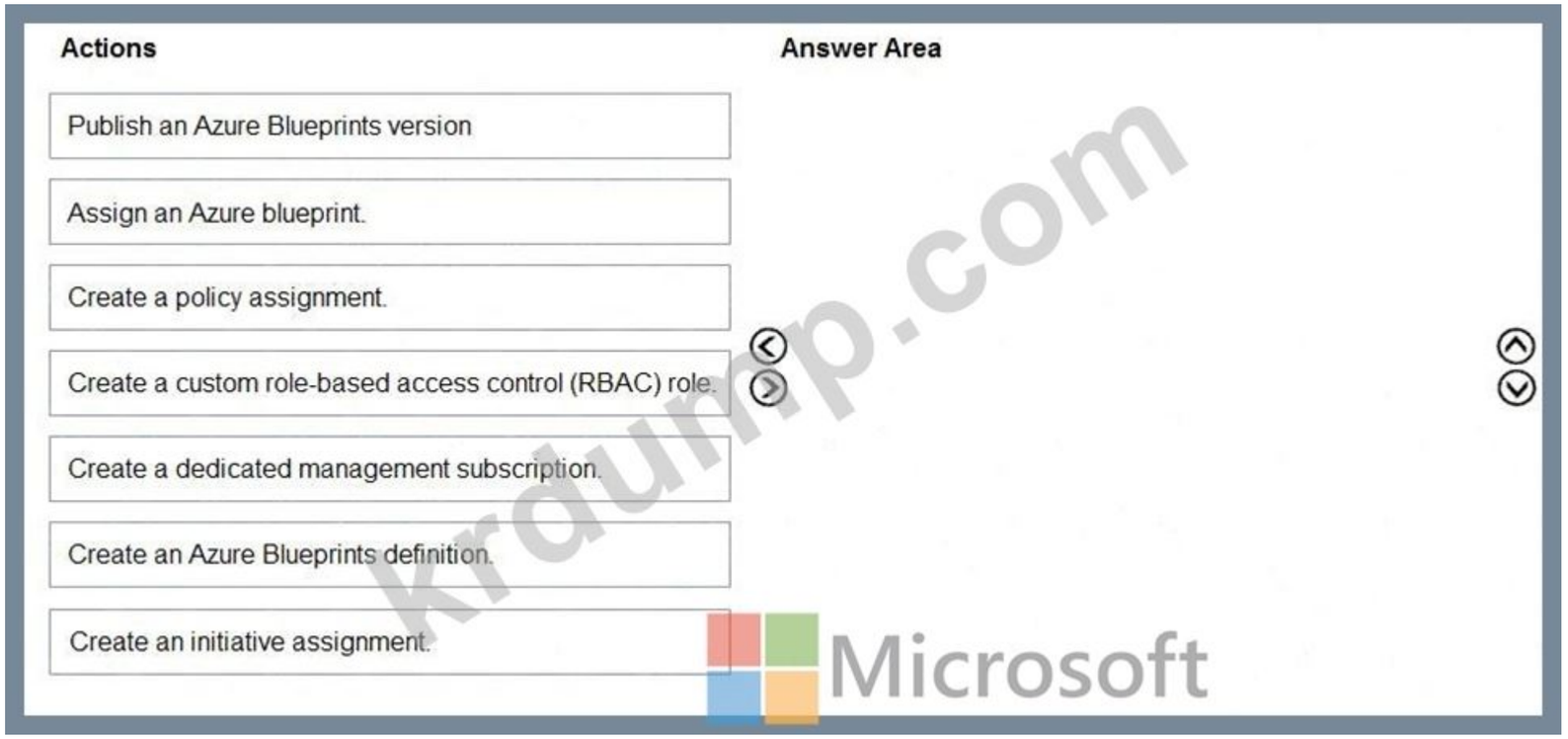
□□ Azure Active Directory(Azure AD) □□□□ □□□ Azure □□□ 5□ □□□□.

SecurityPolicyInitiative1□□□ Azure Policy □□□□□□ □□□□.

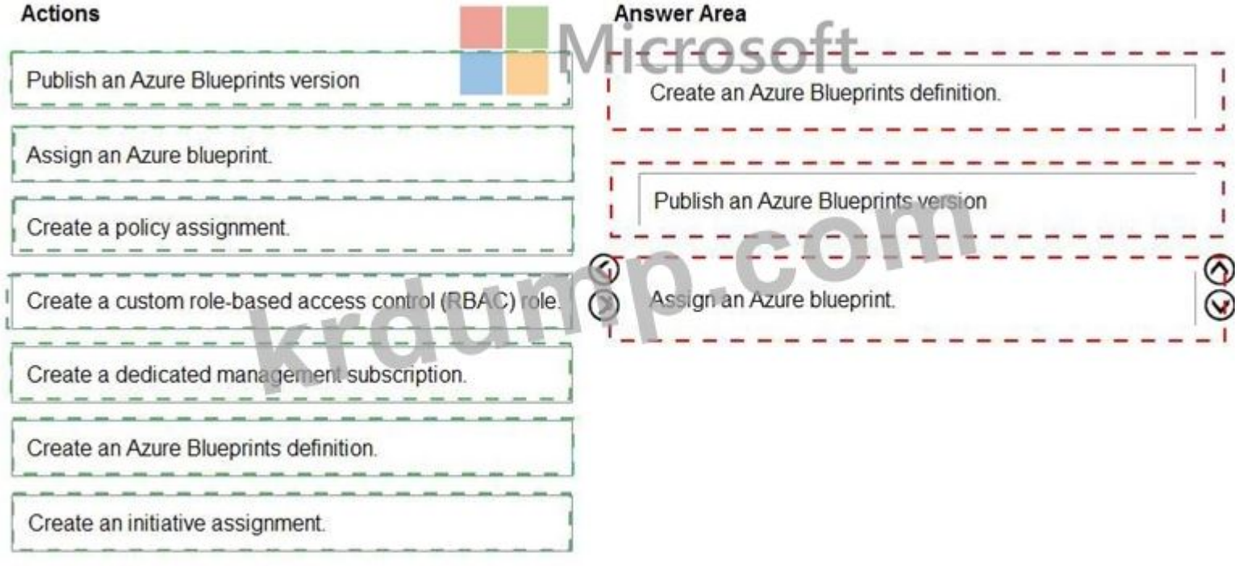
□□ □ □□□ □□□□ □□ □□ □□ □□□ □□□□ □□□ □□□□□.

□ □□□ □□□ □□□□ SecurityPolicyInitiative1□ □□ □□□ □□□□ □□□.

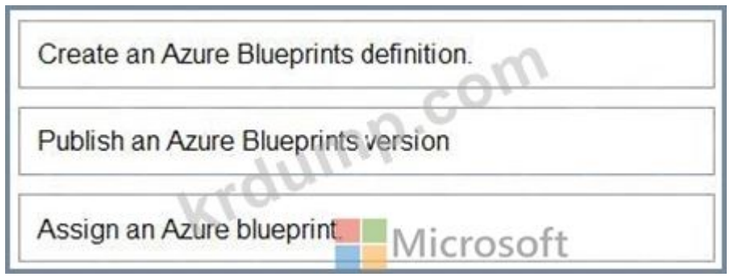
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□□ □□ □□□□ □□ □□□ □□ □□□□ □□ □□□ □□□□ □□□□□.



Answer:



Explanation:



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

NEW QUESTION: 145
VNetwork1□ □□ □□ □□ □□□ □□□□ □□□.
□□ □□ □□□ □□ □□□?
A. VNetwork1□ □□□ □□□□ □□□□.
B. Subnet11 □ Subnet13□□ NSG□ □□□□□.
C. NSG□ Subnet12□ □□□□□.
D. VNetwork1□ □□ DDoS □□□ □□□□□.
Answer: (SHOW ANSWER)
From scenario: Deploy Azure Firewall to VNetwork1 in Sub2.
Azure firewall needs a dedicated subnet named AzureFirewallSubnet.
References:
https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal

NEW QUESTION: 146
100□□ □□ □□□ □□□ Azure □□□ □□□ Azure Security Center□ □□□□□ □□□□. □□ □□□ □□□□□ □□□□.
□ □□ □□□ □□□ □□□ □□□ □□□□□.
Azure Resource Manager □□□□ □□□□ □□□ □□□ □□□ □□ □□□ □□□□ □□□.
□□ □□□ □□ □□□□□ □□□□ □□□□□ □□□ □□ □ □□ □□□□ □□□? □ □□□ □□□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.
A. □□□□□ □□□ □□ ID
B. Key Vault □□ □□□□ □□ □
C. Azure Active Directory(Azure AD) ID
D. □□□□□ □□□ □□ ID
E. □□ □□ □
F. □□ □□ ID
Answer: A,C (LEAVE A REPLY)
https://docs.microsoft.com/en-us/azure/azure-arc/servers/onboard-service-principal

NEW QUESTION: 147
□□ □□ □□ □□ □□□ □□□ □□□□ Sub1□□□ Azure □□□ □□□□.

Name	Location
RG1	West US
RG2	East US

□□ □□□ □□□ Azure Policy □□□ □□□□.

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

Sub1□ □□□ □□□□□.

□□ □□ □□□ □□□□ □□ □□□□□.

Name	Type	Location	Resource group
IPobject1	Public IP address	East US	RG2
obj1	Resource group	West US	*Not applicable*
OBJ3	Virtual network	West US	RG1

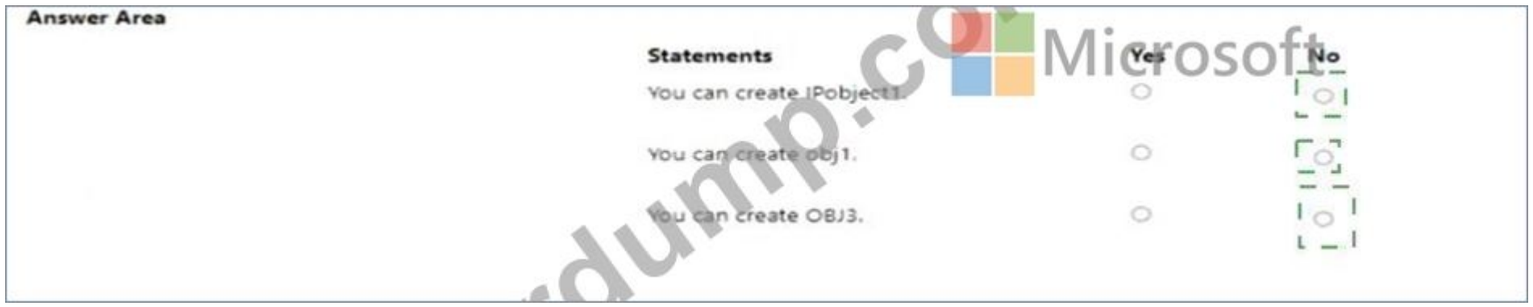
□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.

□□: □□ 1□□ 1□□□□.

Answer Area

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

Answer:



Explanation:

NEW QUESTION: 148

Azure □ □□ □□ □□□ □□□□.

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

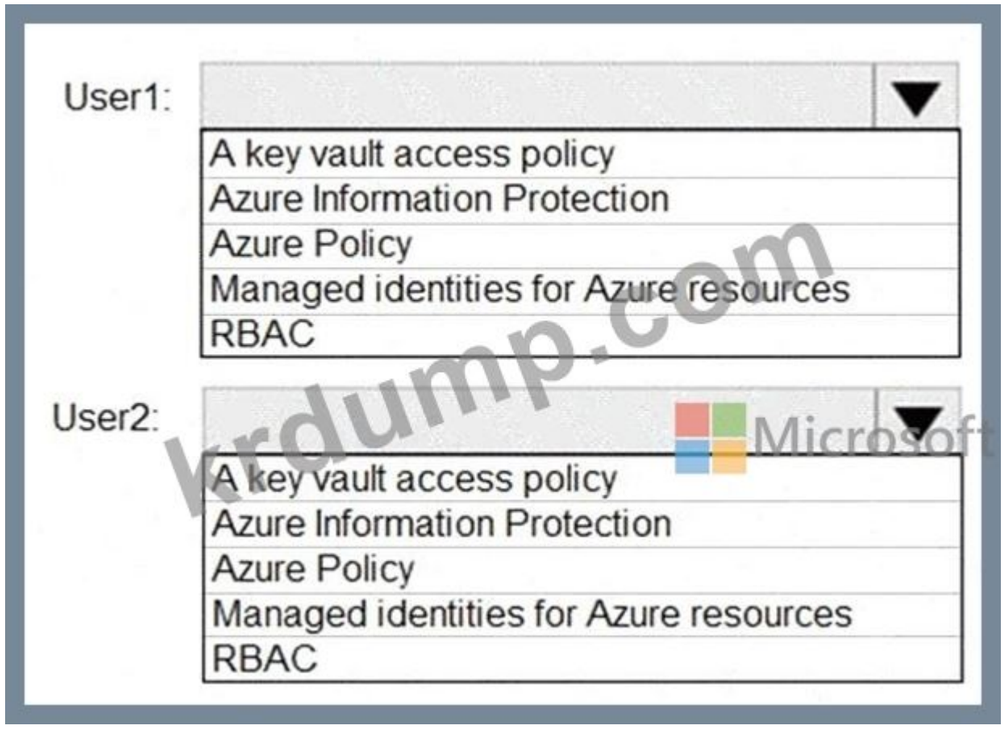
* □ □□□□ □□ □□ □□□ □□□ □□□ □ □□ □□□ User1□□□ □□□□□ □□□□□.

* □ □□□□□ □□□□ □□□□ □□□ □ □□ □□□ User2□□ □□□□□ □□□□□.

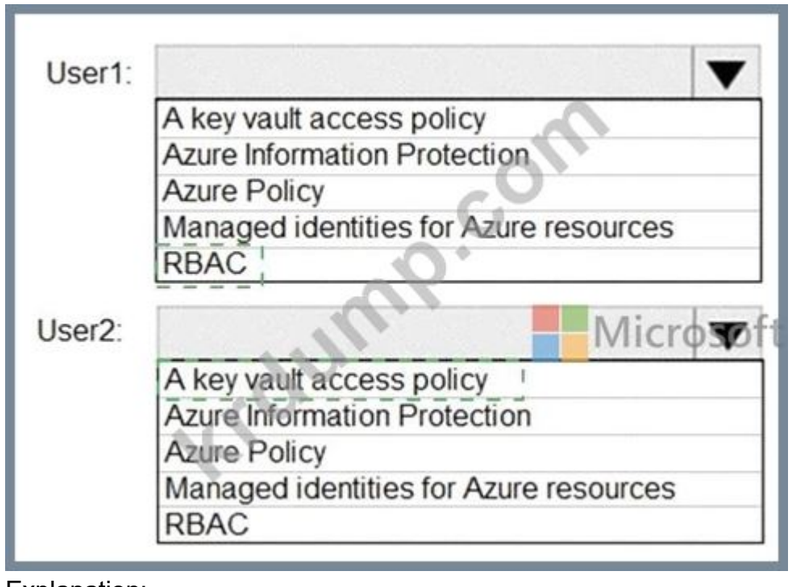
* □□ □□□ □□□ □□□□□.

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

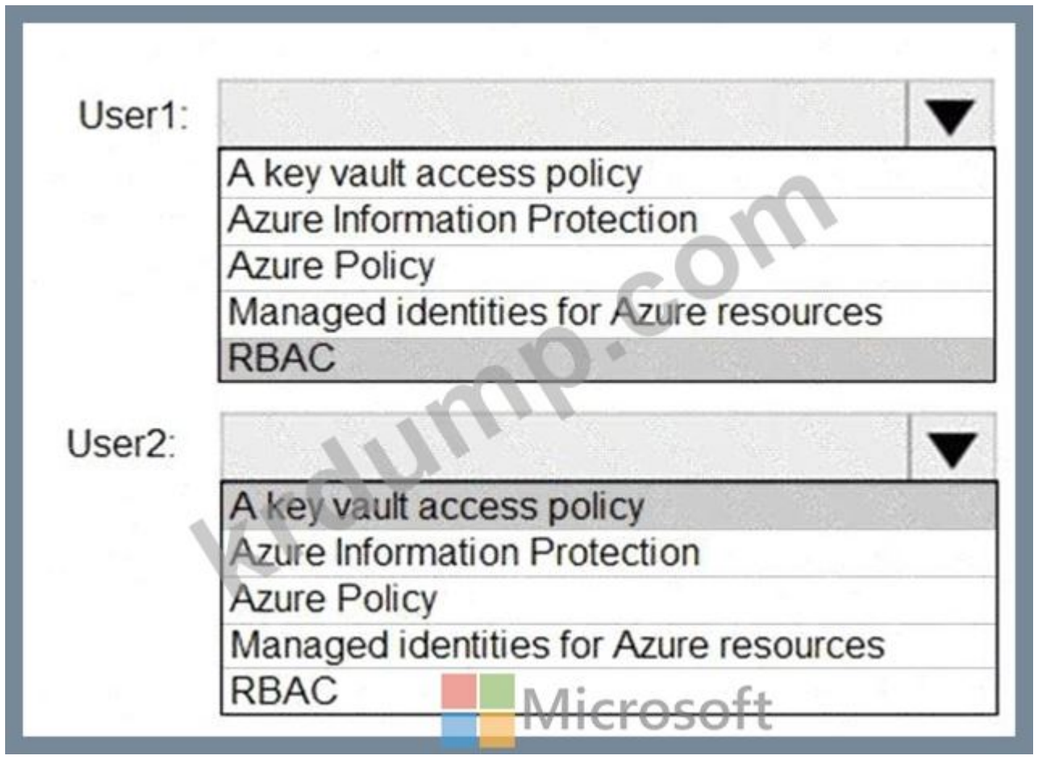
□□: □□ 1□□ 1□□□□.



Answer:



Explanation:



User1: RBAC

RBAC is used as the Key Vault access control mechanism for the management plane. It would allow a user with the proper identity to:

* set Key Vault access policies
* create, read, update, and delete key vaults
* set Key Vault tags

Note: Role-based access control (RBAC) is a system that provides fine-grained access management of Azure resources. Using RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs.

User2: A key vault access policy

A key vault access policy is the access control mechanism to get access to the key vault data plane. Key Vault access policies grant permissions separately to keys, secrets, and certificates.

References:

https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

NEW QUESTION: 149

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

* Azure □□
* □□ □□□□ □□□(GCP) □□□□
* □□□ □ □□□(AWS) □□

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

A. □□□ □□ □□(CIS)

B. NIST 800-53

C. ISO 27001

D. □□□ □ □□ □□(SOC) 2 □□ 2

Answer: C (LEAVE A REPLY)

NEW QUESTION: 150
share1□□□ Azure Files □□□ User1□□□ □□□□ □□□ Azure □□□ □□□□.
share1□ □□ ID □□ □□□ □□□□□□□.
User1□ SMB□ □□□□ Windows 10 □□□□ share1□ □□□□□□ □□□□□.
Azure Files□□□ □□□ □□□□ □ □□ □□□ □□□ □□□□□?
A. OAuth 20
B. JSON Web Token (JWT)
C. Kerberos
D. SAML
Answer: C (LEAVE A REPLY)
https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-domain-service-enable?tabs=azure-portal

NEW QUESTION: 151
LAW1□□□ Azure Log Analytics □□ □□□ □□□□ Sub1□□□ Azure □□□ □□□□.
Windows Server 2012 R2 □ Windows Server 2016□ □□□□ □□□□□ □□ 100□□ □□□□. □ □□□□ LAW1□ □□□□□. LAW1□ □□□ □□□□ □□ □□ □□ □□□□ □□□□□ □□□ □ □□□□.
LAW1□□ □□□ □□□□ □□□□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
* □□ □□□ □□□ □□□□ □□□.
* □□ □□□ □□□ □□□ □□□□□ □□□.
* □□ □□□ □□□ □□□ □□ □□□ □□□ □ □ □□ □□□□□ □□□.
* □□□.
□□ □□□ □□ □ □□ □□ □□□ □□□□ □□□?
A. □□
B. □□(□□□ □□)
C. □□□
D. □□ □□
Answer: C (LEAVE A REPLY)
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: 152
Azure Sentinel □□ □□□ □□□ Azure □□□ □□□□.

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

Answer:

Explanation:

Reference:

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

NEW QUESTION: 153

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

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

□□ JSON □□□ □□□□ Azure □□□ □□□□.

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

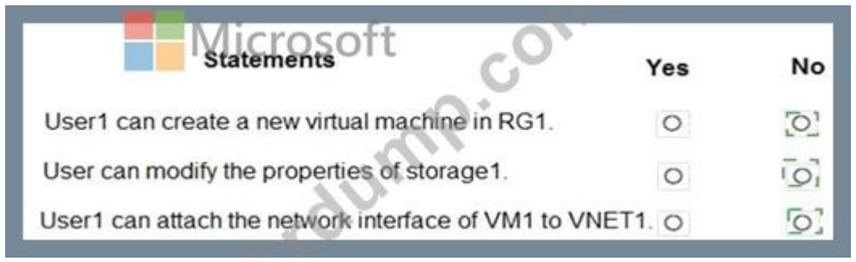
RG1□ □□ User1□ Role1□ □□□□□.

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

□□: □□ 1□□ 1□□□□.

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

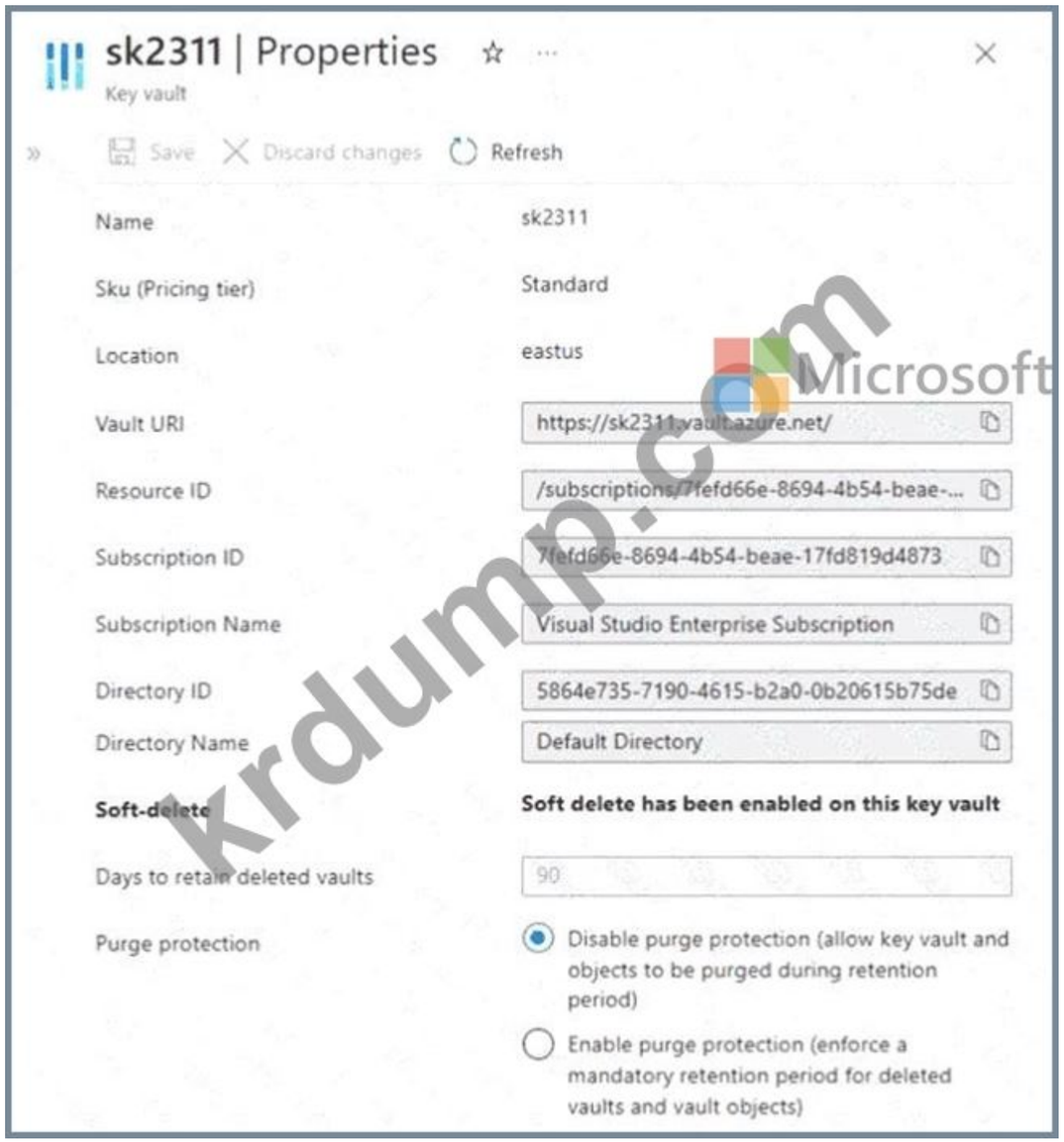
Answer:



Explanation:
NO
NO
NO
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#compute

NEW QUESTION: 154
Azure □□ 1□ □□ □□ VM1□ □□□ Azure □□□ □□□□.
VM1□ Microsoft SQL Server□ □□□□ VNet1□□□ □□ □□□□□ □□□□ □□□□. App1, VM1, Vent□ □□ □□ Azure □□□ □□□□.
App1□ VM1□ □□□ □ □□□ □□□□ □□□. □□□□ □□□ □□□□□ □□□.
A. Azure Application Gateway □□
B. Azure □□
C. □□ □□ □□□□ □□
D. NAT □□□□□ □□
E. □□□□□□ □□□ □□ □□□□ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 155
□□ □□□ □□ sk2311□□□ Azure Key Vault□ □□□□ □□□□.



Sk2311□□ □□ □□ □□□ □□□ □□□□ □□□□.

Name	Type
Item1	Key
Item2	Secret
Policy1	Access policy

sk2311□□□ □□ □□□□ □□□□ □□□□□.

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

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

□□: □□ 1□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 156
UseR1□□□ □□□□ □□□ Azure □□□ □□□□. UseR1□ □□ □□□ □□□ □ □□□ □□□□ □□□.
* □□□ □□□□.
* □□ □□□ □□□ □□□ □□ □□□ □□□ □□□□□.
* □□□ Azure AD □□□ □□□□□.
□ □□□□ □□ □□ □□□ □□□□ □□□. User1□□ □□ □□□ □□□□ □□□?
A. □□□ □□ □□ □□□
B. □□ □□□
C. ID □□□□ □□□
D. □□ □□□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 157
VM1□ storage1□ □□□□□□ □□□ □□ □□□ □□□□ □□□.

□□□□ □□□ □□ □□□ □□□□ □□□.
□□ □□ □□□ □□ □□□?
A. storage1□ □□ □□ □□□ □□□□□.
B. VM1□□ □□□□ □□□ □□ ID□ □□□□□.
C. ID1□ □□ □□□□□ ID □□ □□□ □□□□□.
D. □□□ 1□ □□□ Blob □□□ □□ □□□ □□□□□.
E. VM1□ ID1□ □□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 158
□□□□□□ Microsoft Entra □□□□ □□□□□ adatum.com□□□ □□□□□ Active Directory □□□□ □□□□ □□□□.
Microsoft Entra □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

□□ □□□ □□ adatum.com□ □□ Microsoft Entra □□ □□ □□□ □□□□□.

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

Answer Area

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

Answer:

Answer Area

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

Explanation:

Answer Area

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

NEW QUESTION: 159

□□□ □□

□□ 6

VNET01 □□ □□□□□ Subnet0 □□□□□□ □□□ □□□□□ Web3l 330471□□□ Microsoft SQL □□□ □□□□ □□□.

Answer:

see the task answer with step by step below:

* Configure the firewall settings for the SQL server. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to add a firewall rule that allows inbound traffic from the IP address range of the Subnet0 subnet. You also need to disable the option to allow Azure services and resources to access this server.

* Configure the network settings for the SQL server. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to enable service endpoints for SQL Server on the Subnet0 subnet.

You also need to add a virtual network rule that links the SQL server to the Subnet0 subnet.

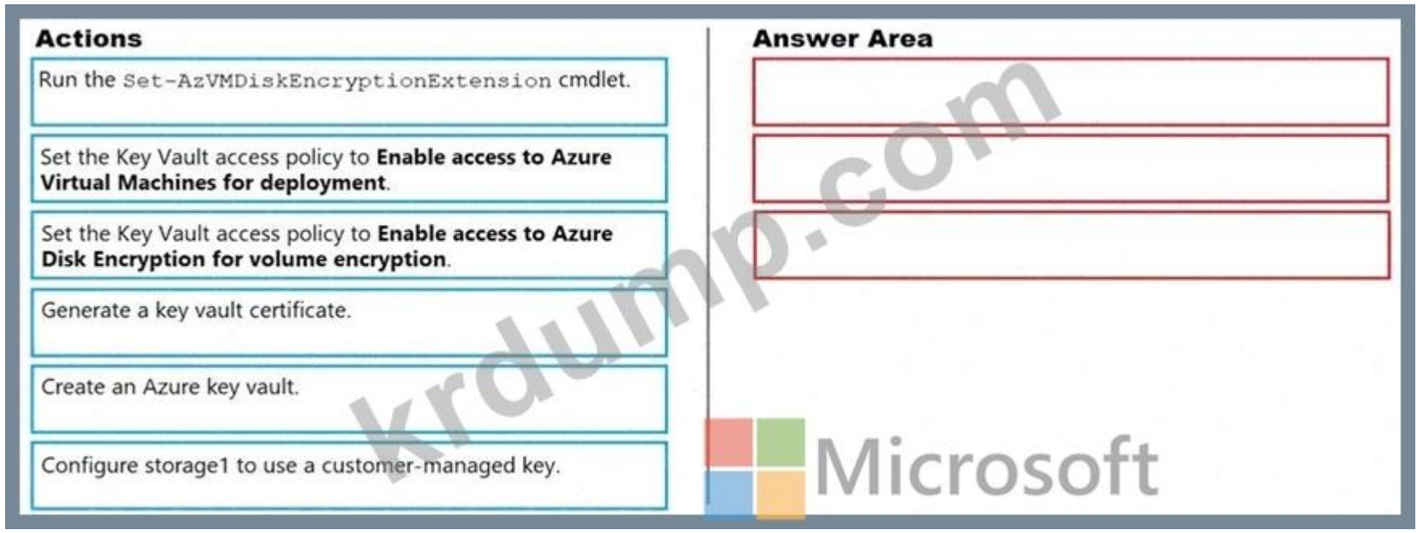
* Configure the connection settings for the SQL server. You can use SQL Server Management Studio or Transact-SQL to do this. You need to enable remote server connections and specify a TCP port for

listening. You also need to configure SQL Server Authentication or Azure Active Directory Authentication for connecting to the SQL server.

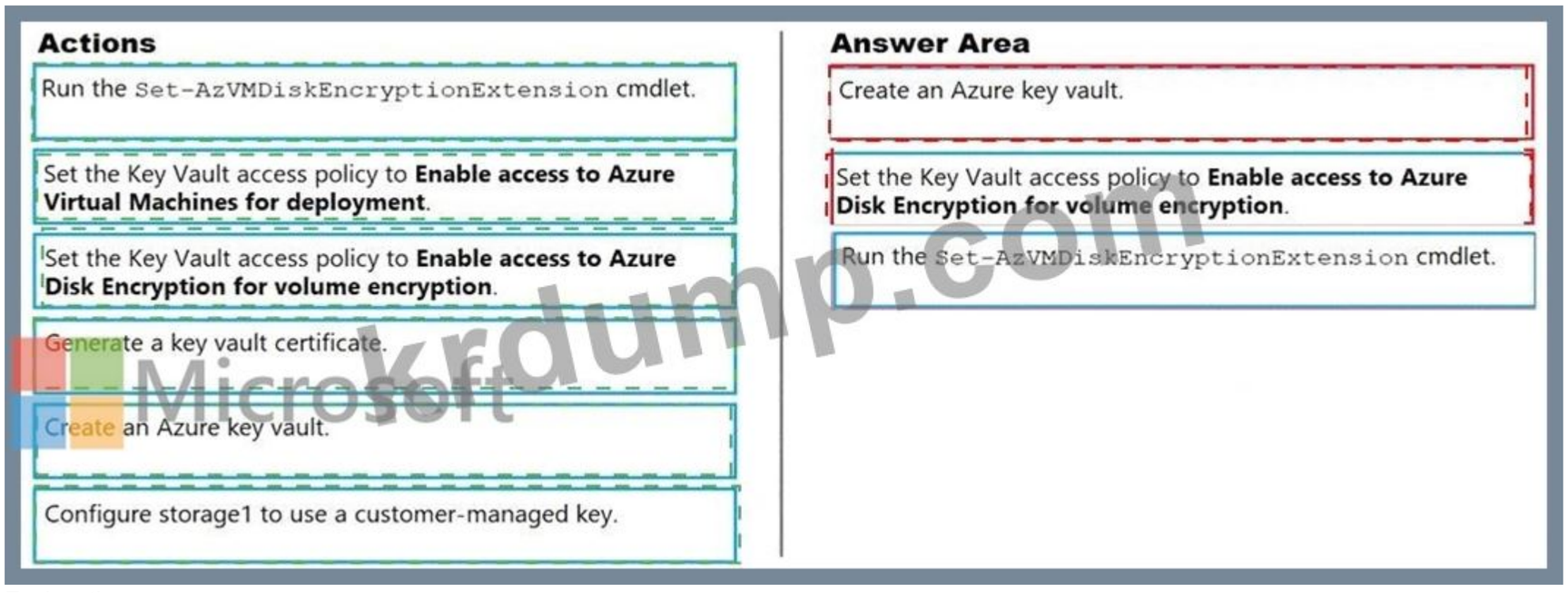
NEW QUESTION: 160
sql1□□□ Azure SQL □□□□□□□ □□□ Azure □□□ □□□□.
sql1□ □□□ □□□□□.
□□ □□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
* Kusto □□ □□□ □□□□ □□□ □□□ □□□□□.
* □□□ □□□ □□□□□□.
□□□ □□□□ □□□?
A. □□□ □□
B. □□ □□
C. Log Analytics □□ □□
Answer: C (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/tutorial-log-analytics-wizard

NEW QUESTION: 161
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □ □ □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□□ □□□□.
Azure Security Center□ □□□□ □ □□ Azure □□□ □□ □□ □□□ □□ □□□ □□□□□.
□□□ □□□ □□□□□ □□ □□ □□ □□□ □□□□□.
□ □□ □□ □□□ □□ □□□ □□□□ □□□□ □□□.
□□□: □□ □□□ □□□ □□□ □□□□□□ □□□ □□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: A (LEAVE A REPLY)
References:
https://docs.microsoft.com/en-us/azure/governance/policy/overview

NEW QUESTION: 162
storage1□□□ Azure Storage □□□ VM1□□□ Azure □□ □□□ □□□□. VM1□□ □□□□ SSD □□ □□□□ □□□□.
VM1□ □□ Azure Disk Encryption□ □□□□□ □□□.
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□□ □□ □□□□ □□ □□□ □□ □□□□ □□ □□□ □□□□ □□□□□.



Answer:



Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

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

NEW QUESTION: 163
User1□□□ □□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□.
User1□ □□ □□□ □□□□ □□□ □ □□□ □□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
User1□□ □□ □□□ □□□□ □□□?
A. □□□□□ □□□
B. □□□ □□ □□ □□□
C. □□□ □□□
D. □□ □□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 164
Azure Active Directory(Azure AD)□ □□□ Azure □□□ □□□□. □□ □□□□□ □□ □□ □□ □□ □□□□ □□□□ □□□□.

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

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

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

□□ □□ □□□ □□ Vault1□ □□ □□ □□□ □□□□.

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

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

Answer Area

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

Answer:

Answer Area

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

Explanation:

Answer Area

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

NEW QUESTION: 165
Azure AD Privileged Identity Management(PIM)□ □□□□ Azure □□□ □□□□.
User1□□□ □□□□ □□ □□□ □□□ □□□ □ □□□□.
□□ □□□ □□ 2□□ □□□ □□□ □ □□□ □□ □□□.
□□□ □□ □□□?
A. □□□ □□ □□□ □□□□□.
B. □□ □□□ □□□ □□□□□.
C. □□□ □□□ □□ □□□ □□□□□□□.
D. □□ □□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 166
Azure □□□ □□□□.
CAPolicy1□□□ □□□ □□□ □□□ □□□ □□□ □□□□□.
What If □□□ □□□□ CAPolicy1□ uter1□ □□□ □□□ □□□□ □□□. □□□□ CAPolicy1□ □□□□□ □□□ □□□ □□□□□ □□□.
CAPolicy1□ □□ Enable □□ □□□ □□□□ □□□□ □□□?
A. □□
B. □□
C. □□□ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 167
□□□□□ 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: 168

□□ □□ □□□ □□ East US2 □□□ □ □□ Azure □□ □□□ □□□□.

Name	Operating system	Type	Tier
VM1	Windows Server 2008 R2	A3	Basic
VM2	Ubuntu 16.04-DAILY-LTS	L4s	Standard

Azure Key Vault□ □□□□ □□□□□.

VM1□ VM2□□ Azure Disk Encryption□ □□□□ □ □□□ □□□□ □□□.

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

□□: □□ 1□□ 1□□□□.

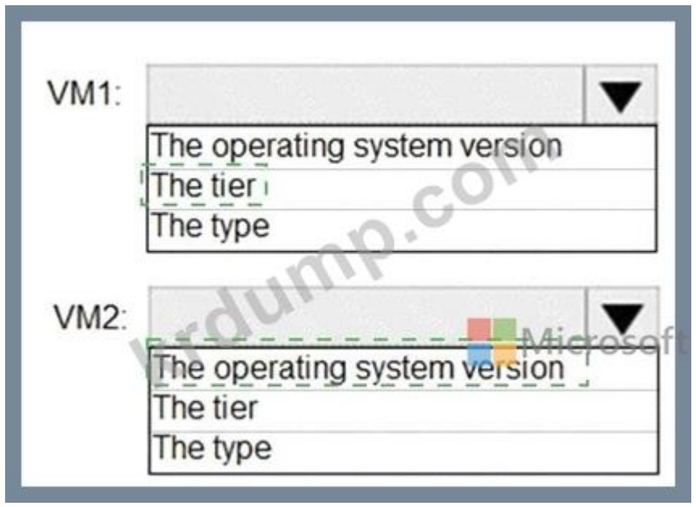
VM1:

- The operating system version
- The tier
- The type

VM2:

- The operating system version
- The tier
- The type

Answer:



Explanation:

VM1: The Tier

The Tier needs to be upgraded to standard.

Disk Encryption for Windows and Linux IaaS VMs is in General Availability in all Azure public regions and Azure Government regions for Standard VMs and VMs with Azure Premium Storage.

VM2: the operating system

References:

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/generation-2#generation-1-vs-generation-2-capabilities

NEW QUESTION: 169

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

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

□□□ □□□□ □□□?

A. Azure Monitor □□ □□

B. PostgreSQL Audit □□(pgAudit)

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

D. Azure Monitor □□ □□

Answer: C (LEAVE A REPLY)

NEW QUESTION: 170

Sub1□□□ Azure □□□ □□□□.

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

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

WF1□ □□□□□ □□□ □□□□ □□□?

A. Azure □□□□□□ □□□□

B. Azure □□□

C. Azure Logic Apps □□□□

D. Azure DevOps

Answer: (SHOW ANSWER)

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

NEW QUESTION: 171
Adminl1□□□ □□□□ VM1□□□ □□ □□□ □□□ Azure □□□ □□□□.
VM1□ Windows Server 2019□ □□□□ Azure Resource Manager □□□□ □□□□ □□□□□□□. VM1□ □□ Azure □□ □□ □□ □□□ □□□ □□ □□□□.
Admin1□ VM1□ Azure Security Center□ Just in time VM □□□ □□□□□□ □□□□ □□□□ □□□□ □□□ □□□□□.
Admin1□ VM1□ □□ JIT(Just-In-Time) VM □□□□ □□□□ □ □□□ □□□□ □□□.
□□□ □□ □□□?
A. VM 1□ □□ □□ □□ IP □□□ □□□ □□□□□.
B. □□ □□ □□ □□□ Azure □□ □□ □□ □□□ □□□□□.
C. Admin1□ Azure Active Directory Premium Plan 1 □□□□□ □□□□□.
D. □□□□ □□ □□(NSG)□ □□□□ □□□□□.
Answer: D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time?tabs=jit-config-asc%2Cjit- request-asc

NEW QUESTION: 172
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □ □ □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□□ □□□□.
Azure Security Center□ □□□□ □ □□ Azure □□□ □□ □□ □□□ □□ □□□ □□□□□.
□□□ □□□ □□□□□ □□ □□ □□ □□□ □□□□□.
□ □□ □□ □□□ □□ □□□ □□□□ □□□□ □□□.
□□ □□: □□□ □□□ □□□ □□□ □□ □□□ □□□ □□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)
References:
https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-groups/

NEW QUESTION: 173
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □ □ □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□□ □□□□.
Azure □□□ □□□□. □ □□□□ Windows Server□ □□□□ 50□□ □□ □□□ □□□□ □□□□.
2012 R2 □□ Windows Server 2016.
□□ □□□ Microsoft Antimalware□ □□□□ □□□.
□□ □□: □ □□ □□□ □□□□ Windows □□□ □□□□□.

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: B (LEAVE A REPLY)

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

References:

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

NEW QUESTION: 174

Azure Portal□□ Azure □□□ □□□□ □□□□.

DeployIfNotExist, AuditIfNotExist, Append □ Deny □□□ □□□□ □□□ □□□ □□□□□.

□□ □□□ □□□ □□ □□□□ ID□ □□□□□?

A. □□□□ □□□ □□

B. □□

C. □□□□ □□□ □□

D. □□

Answer: (SHOW ANSWER)

When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity.

References:

https://docs.microsoft.com/bs-latn-ba/azure/governance/policy/how-to/remediate-resources

NEW QUESTION: 175

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

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

Sub1□□□ Azure □□□ □□□□.

RG1□□□ □□□ □□□ Sa1□□□ Azure Storage □□□ □□□□.

□□□□ □□□□□□□ □□ □□ □□ □□□ □□(SAS)□ □□□ □□□ □□□ □□□□ Sa1□ Blob □□□□ □□ □□□□ □□□□□□.

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

Sa1□ □□ □□ □□ □□□ □□□□ □□□.

□□□: Sa1□ □□□ □□□□□.

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: B (LEAVE A REPLY)

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

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

References:

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

NEW QUESTION: 176

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

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

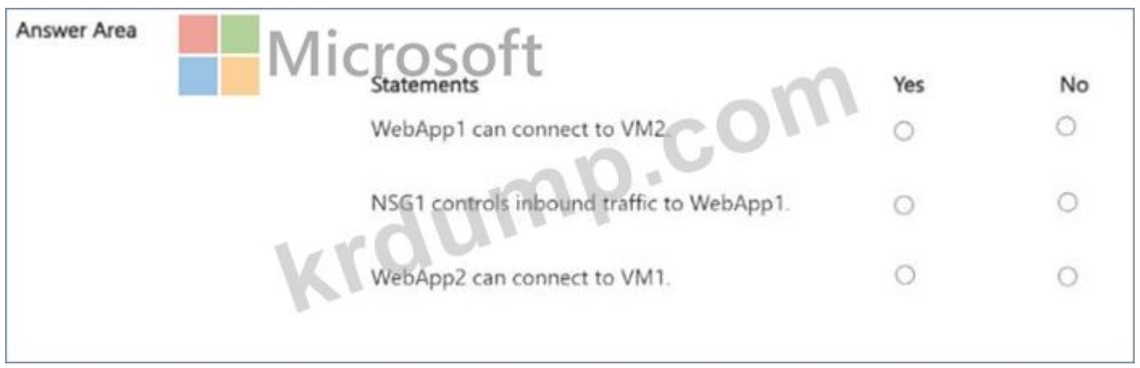
NSG1□ NSG2□ □□ □□ □□□ □□□ □□□□.
□□□□ □□ □□ □□□ □□ □□□ □□□□ □□□□.

Name	Connected to
VM1	Subnet1
VM2	Subnet2

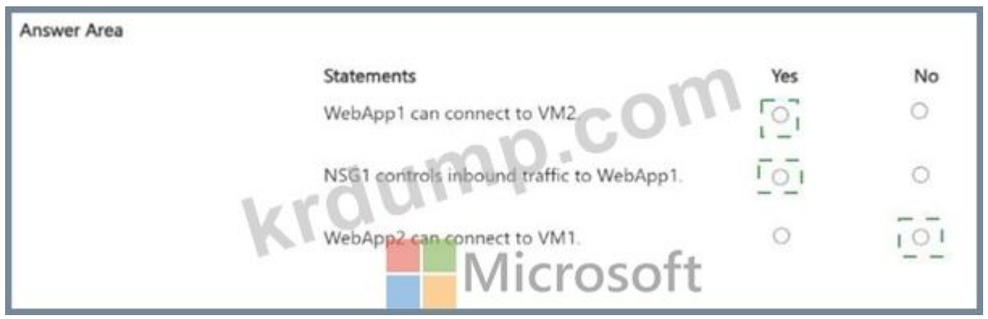
□□□□ □□ □□ □□□ □ □□□ □ □□ □□□□ □□□□.

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

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



Answer:

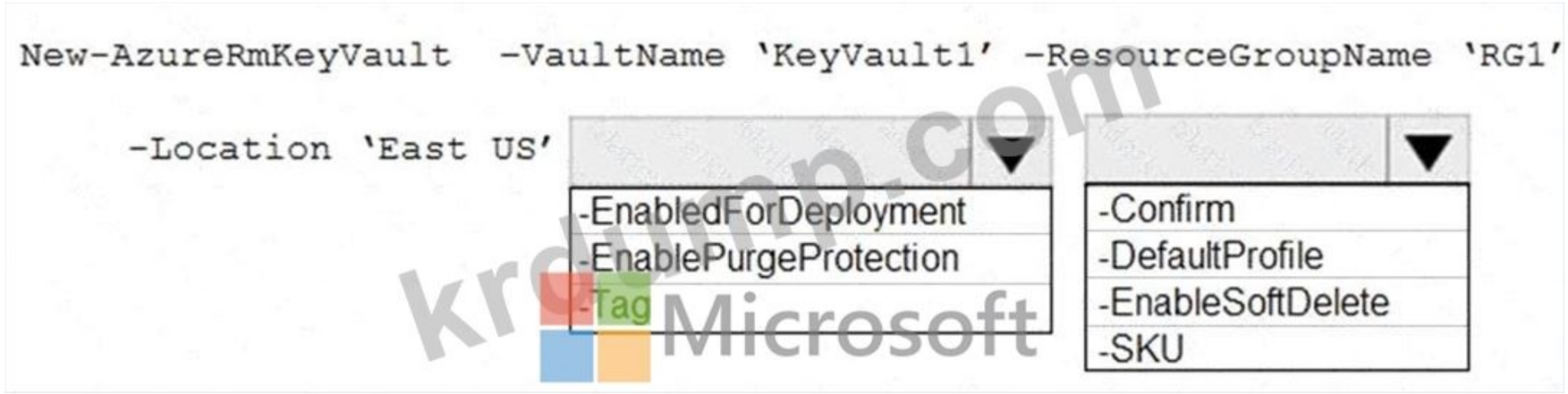


Explanation:

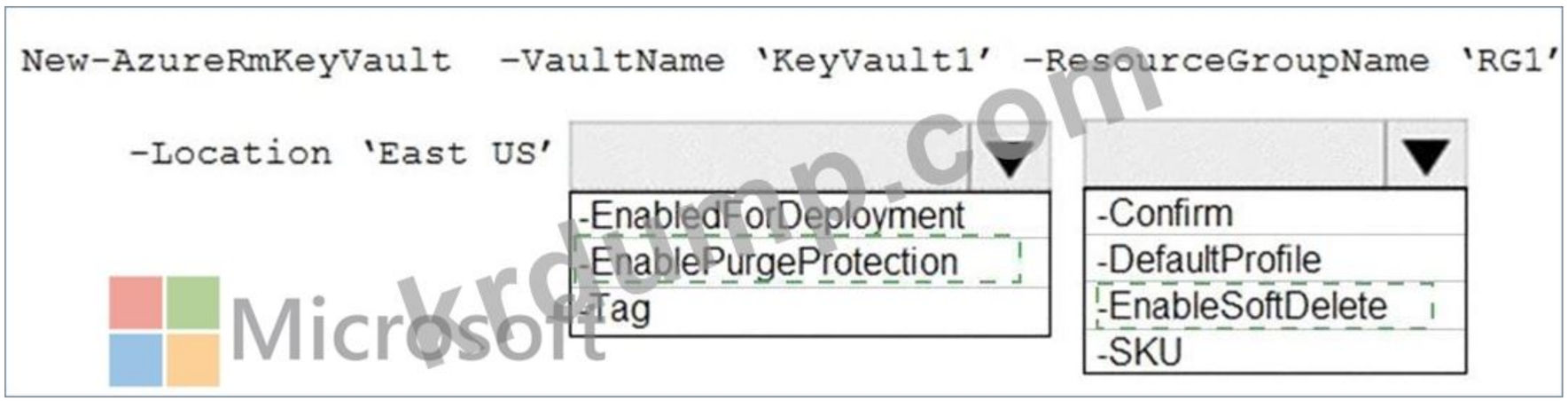
NEW QUESTION: 177
Azure □□□ □□□□.
Microsoft Defender for Cloud□□ □□ □□□□ □□□□ □□□□ □□□□ □□□□ □□ □□□□□.
□□ □□ □□□ □□□□ □□□?
A. □□□ □□
B. □□□□ ID
C. □□ □□
D. Azure □□ □
E. Azure □□ □
Answer: D (LEAVE A REPLY)

NEW QUESTION: 178
□□ □□ □□ □□□ □□□ □ □□□ □□□□ □□□.
□□ □□ □□□ □□ □□□?
A. □□ □□□□ □□ □□□□□□ □□□.
B. Security Center□ Microsoft Cloud App Security□ □□□□□.
C. Security Center□ □□ □□ □□□ Standard□ □□□□□□□□.
D. □□ □□ □□ □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
The Standard tier extends the capabilities of the Free tier to workloads running in private and other public clouds, providing unified security management and threat protection across your hybrid cloud workloads. The Standard tier also adds advanced threat detection capabilities, which uses built-in behavioral analytics and machine learning to identify attacks and zero-day exploits, access and application controls to reduce exposure to network attacks and malware, and more.
Scenario: Security Operations Requirements
Litware must be able to customize the operating system security configurations in Azure Security Center.
References:
https://docs.microsoft.com/en-us/azure/security-center/security-center-pricing

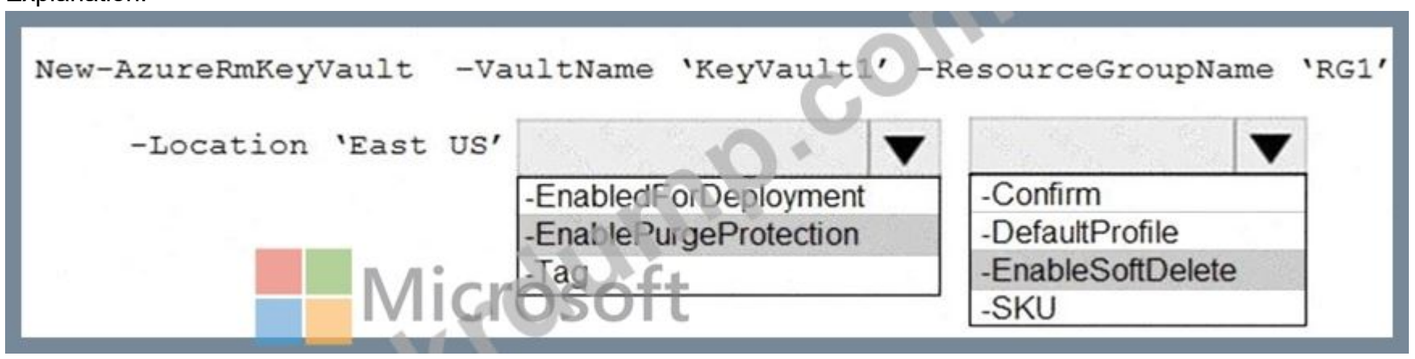
NEW QUESTION: 179
Azure Key Vault□ □□□□ □□□. □□□□ Key Vault□□ □□□ □□ □□□ 90□ □□ □□□□ □□□.
□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.



Answer:



Explanation:



Box 1: -EnablePurgeProtection

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

Box 2: -EnableSoftDelete

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

References:

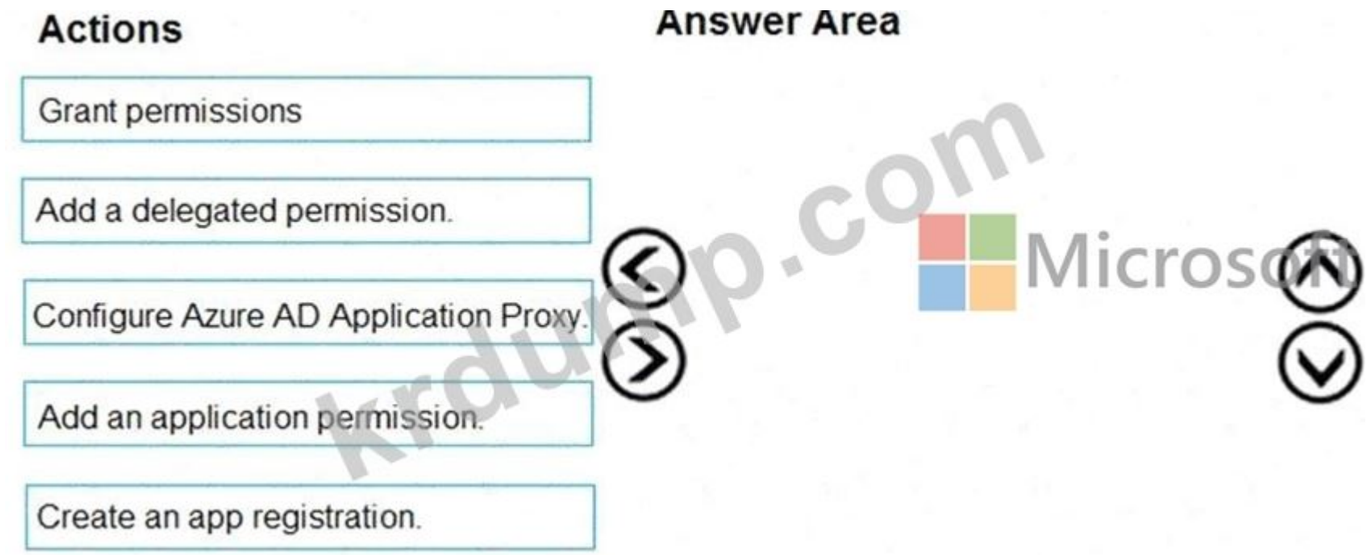
https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/new-azurermkeyvault

NEW QUESTION: 180

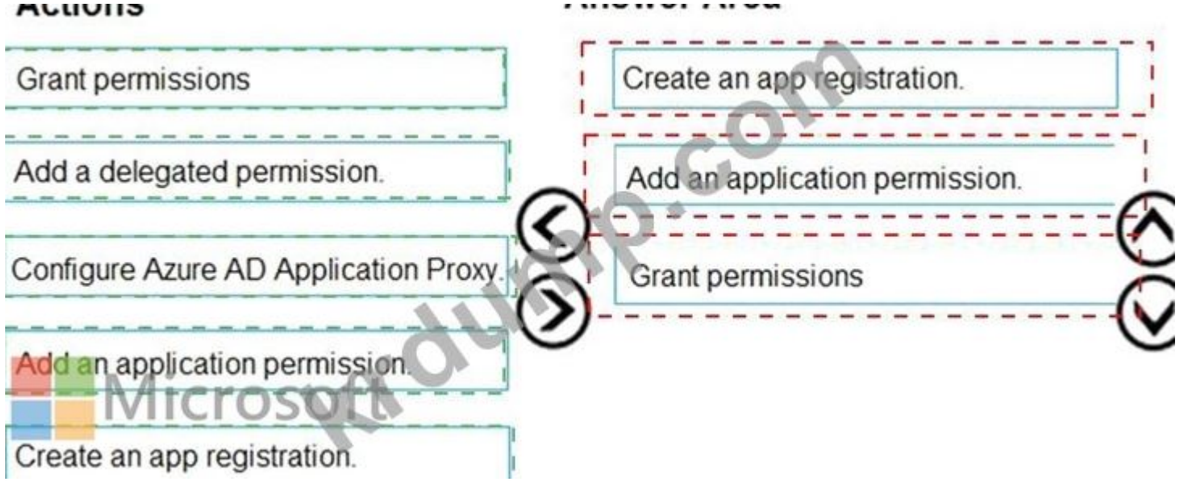
Windows Server 2019□ □□□□ VM1□ VM2□□ □ □□ □□ □□□ □□□ Azure □□□ □□□□.
Azure Automation□□ □□□□ □□□ □□□□ □□□□.
Update1□□□ □□□ □□□ □□□□ □□□ □□ □□□□□.
Update!□ □□ □□ □□□ □□□□□ □□□□ □□□.
* VM1□ VM2□ □□□□ □□□□□ □□□□□.
* □□ □□□ Windows Server 2019 □□ □□□ □□□□ Update1□ □□□□□.
□□□□ 1□ □□□ □□□□ □□□?
A. □□ □□□ □□□ □□□ □□ □□ □□
B. □□□ □□□ □□□ □□ □□ □□
C. □□ □□ □□
D. Kusto □□ □□ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 181
□□□ □□
□□ 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: 182
□□□ □□□□ contoso.com□□□ Azure Active Directory(Azure AD) □□□□ □□□□.
□ □□□ App1□□□ □□□□□□□ □□□□ □□□□. App1□ Windows Server 2016□ □□□□ □□□□ □□□□ □□□□□. App1□ contoso.com□ □□□□ Microsoft Graph□ □□□□□ □□ □□ □□□□ □□□□.
App1□ □□□ □□□□ □□□ □□□□ □□□.
Azure Portal□□ □□ □ □□ □□□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□ □□□ □□ □□□□ □□□ □□□ □□□□ □□□□□.



Answer:



Explanation:

Step 1: Create an app registration

First the application must be created/registered.

Step 2: Add an application permission

Application permissions are used by apps that run without a signed-in user present.

Step 3: Grant permissions

References:

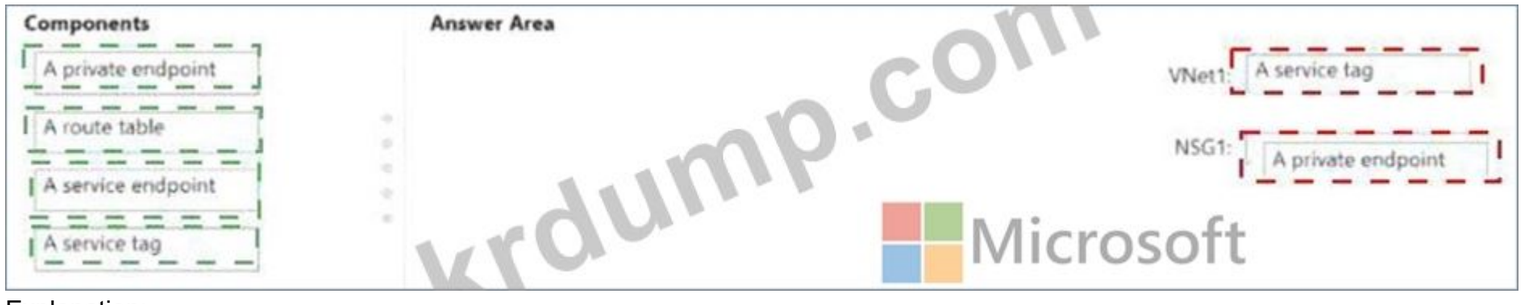
https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-permissions-and-consent

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

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

□□ □□ □□□ □□□□□ □□□□ □□□ □□□□ □□□.
* VM1□□ □□□□□ □□□ □□□□ Microsoft □□ □□□□□ □□□ □□□.
* VM1□□ □□□□□ □□□ □□ □□□□□ □□□□ □□□□□ □□□.
* □□□□ □□□ □□ □□□ □□□□□ □□□.
VNetl□ NSG1□ □□ □□□ □□□□ □□□? □□□ □□ □□ □□□ □□□ □□□□ □□□□□ □□□□. □ □□ □□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□. □□□□ □□□ □ □ □□ □□ □□□ □□□□□□ □□□□□ □ □□ □□□□. □□: □□□ □□ □□□ 1□□□□.

Answer:



Explanation:

NEW QUESTION: 184
□□ □□ □□□ □□□□ □□□ contoso.com□□□ Azure Active Directory(Azure AD) □□□□ □□□□.

Name	Member of	Multi-factor authentication (MFA) status
User1	None	Disabled
User2	Group1	Disabled
user3	Group1	Enforced

□□□□ □□ Azure AD □□ □□ ID □□(PIM)□ □□□□□□□□.
PIM□□ □□□□ □□□ □□□□ □□□ □□ □□□ □□□□.
* □□ □□□ □□(□□): 2
* □□□□□ □□□ □□ □□□ □□□: □□□□
* □□□ □ □□/□□ □□ □□ □□: □□□□
* □□□□ □□ Azure Multi-Factor Authentication□ □□□□□. □□□
* □ □□□ □□□□□□ □□□ □□□□□. □□□
* □□□ □□□: Group1
□□ □□ □□□ □□ □□□□□ □□□□ □□□ □□□ □□□□□.

Name	Assignment type
User1	Active
User2	Eligible
user3	Eligible

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

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

Answer:

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

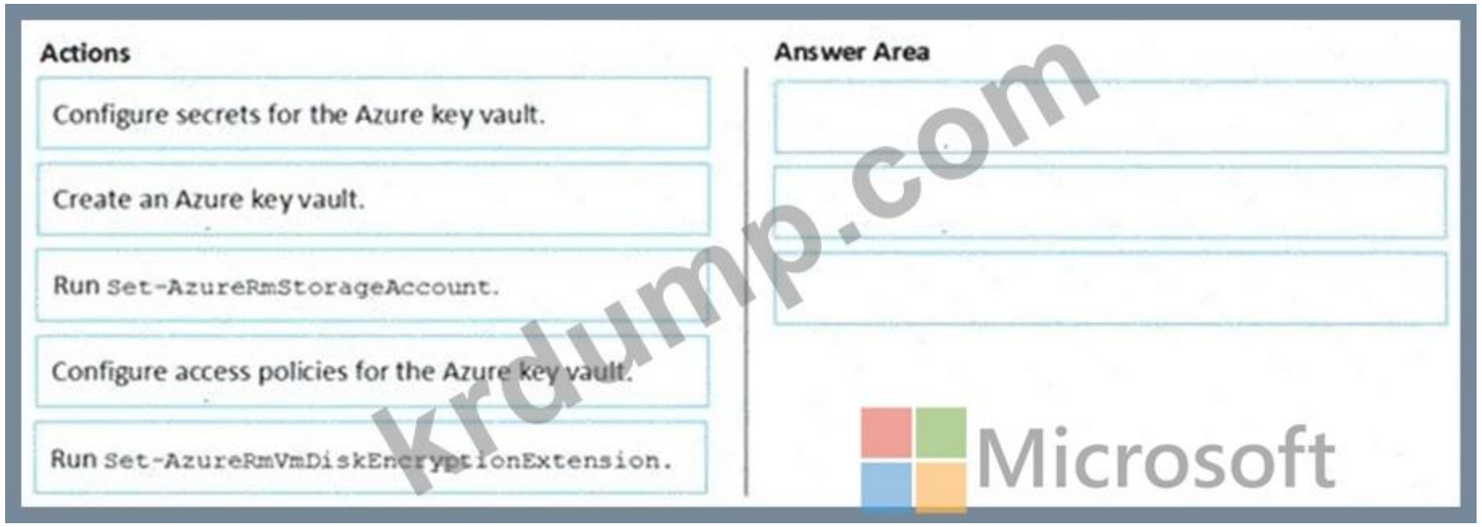
Explanation:

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

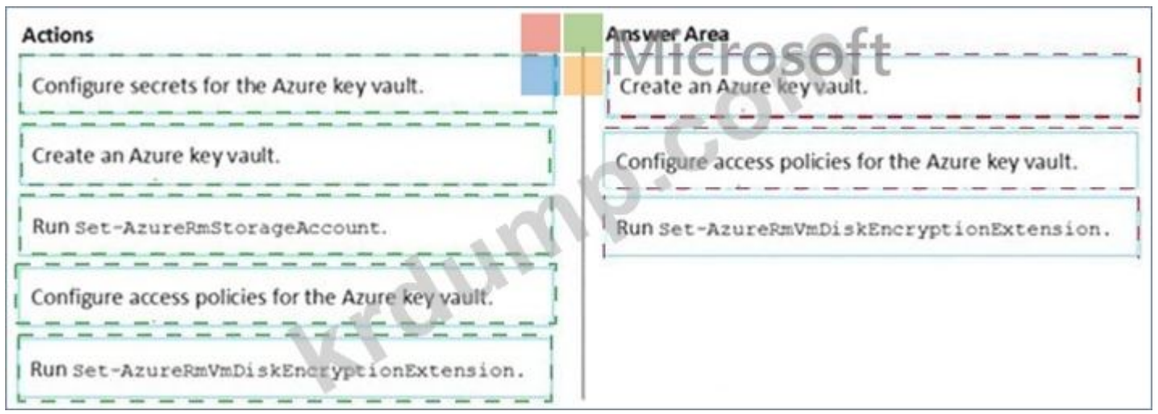
https://docs.microsoft.com/es-es/azure/active-directory/privileged-identity-management/pim-deployment-plan (Require approval section)

NEW QUESTION: 185
sa1□□□ □□□ Azure Data Lake Storage □□□ □□□ Azure □□□ □□□□.
sa1□ □□□□□ □□, □□, □□□□ □□, □□□□ □□ □□ □□□ □□□□ App1□□□ □□ □□□ □□□□□.
App1□ □□ □□□□□□ □□□□ sa1□ □□□□ □□□ □ □□□ □□□□ □□□. sa1□ □□□ □□ □□ □□□□□ □□ □□□□□?
A. 3
B. 5
C. 1
D. 4
E. 2
Answer: E (LEAVE A REPLY)

NEW QUESTION: 186
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □ □ □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□□ □□□□.
Sub1□□□ Azure □□□ □□□□. Sub1□□ Windows Server 2016□ □□□□ VM1□□□ Azure □□ □□□ □□□□ □□□□.
Azure Disk Encryption□ □□□□ VM1 □□□□ □□□□□ □□□.
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□□ □□ □□□□ □□ □□□ □□ □□□□ □□ □□□ □□□□ □□□□□.



Answer:



Explanation:

References:

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

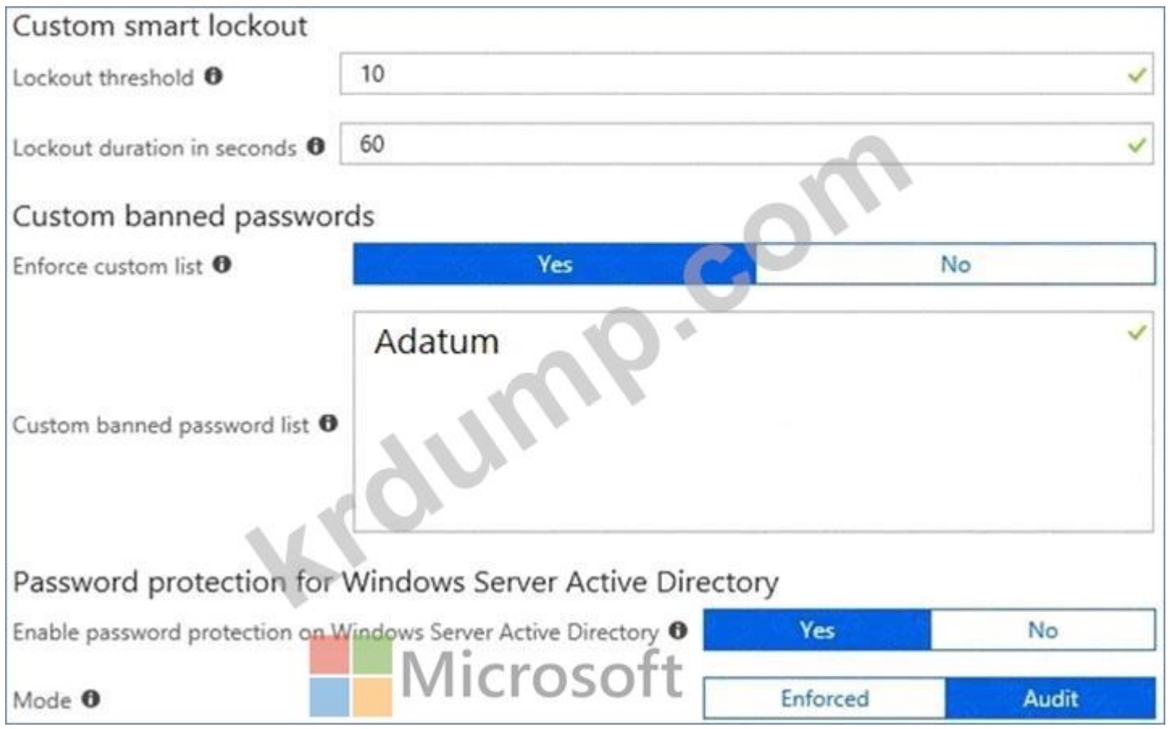
NEW QUESTION: 187

□□□□□□ Azure Active Directory(Azure AD)□ □□□□□ adatum.com□□□ □+□□□□ Active Directory □□□□ □□□□ □□□□.

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

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

□□ □□□ □□ adatum.com□ □□ □□ □□ - □□□□ □□ □□□ □□□□□.



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

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

Answer:

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

Explanation:

Text Description automatically generated

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

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

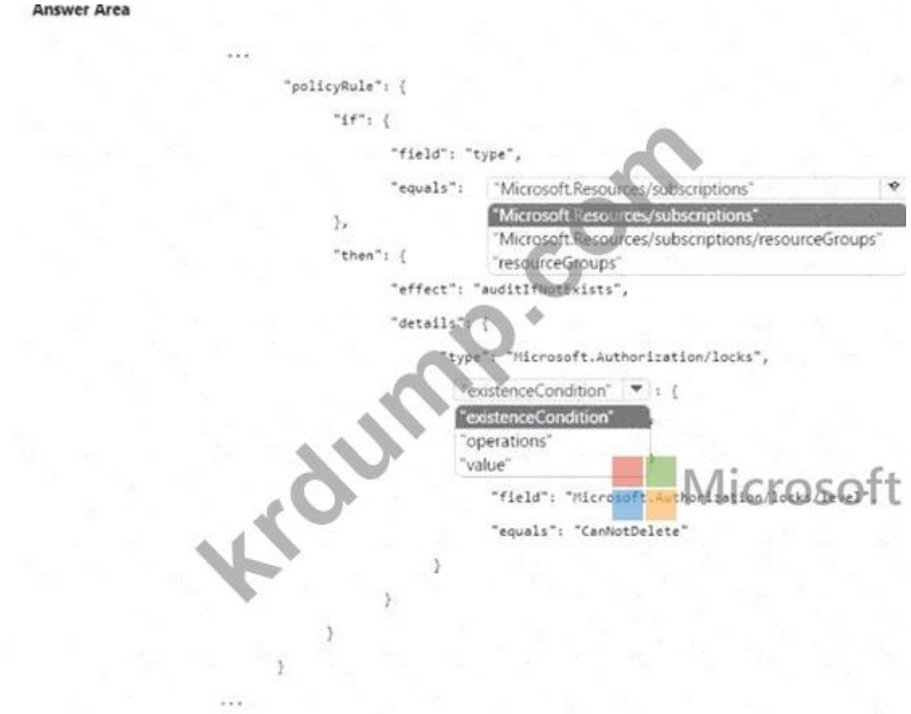
NEW QUESTION: 188
Azure □□ □□□ □□□□ □ □□□□ Azure Resource Manager □□□□ □□□□.
□□ □□ □□□□□ □□□□□□□ □□ □□□□ □□ Windows □□□ □□□□ □□□□□□ □□□.
□□□ □□□□ □□□?
A. Microsoft Intune□ □□ □□ □□ □□
B. Azure Automation □□ □□
C. □□□□□□ □□ □□
D. Azure □□□□□
Answer: (SHOW ANSWER)
You can use Azure Automation State Configuration to manage Azure VMs (both Classic and Resource Manager), on-premises VMs, Linux machines, AWS VMs, and on-premises physical machines.
Note: Azure Automation State Configuration provides a DSC pull server similar to the Windows Feature DSCService so that target nodes automatically receive configurations, conform to the desired state, and report back on their compliance. The built-in pull server in Azure Automation eliminates the need to set up and maintain your own pull server. Azure Automation can target virtual or physical Windows or Linux machines, in the cloud or on-premises.
References:
https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started

NEW QUESTION: 189
□□□□ VM0□ □□□□ □ □□□ □□ □□□. □□□□ □□□ □□ □□ □□□ □□□□ □□□.
□□□ □□ □□□?
A. VM0□ Subnet1□ □□□□□.
B. □□□□□ □□□□ □□□ □□□ □□□ □□□□□.
C. RT1□ AzureFirewallSubnet□ □□□□□.
D. □□□□□ DNAT □□□ □□□□□.
Answer: (SHOW ANSWER)
https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-dnat

NEW QUESTION: 190
Microsoft Defender for Cloud□ □□ □□□ □□ □□ □□□□□□ □□□ □□□□□.
□□ □□□ □□ □□ □□□ □□□ □□□□ □□□.
□□ □□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □□ 1□□ 1□□□□.

Answer Area



Answer:

Answer Area

Explanation:

A screenshot of a computer Description automati cally generated

Answer Area

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

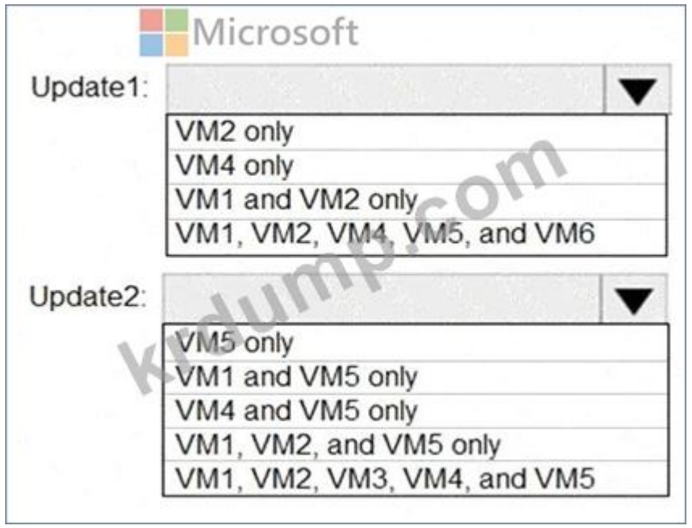
"Microsoft.Resources/subscriptions"
"Microsoft.Resources/subscriptions/resourceGroups"
"resourceGroups"

"existenceCondition"
"operations"
"value"

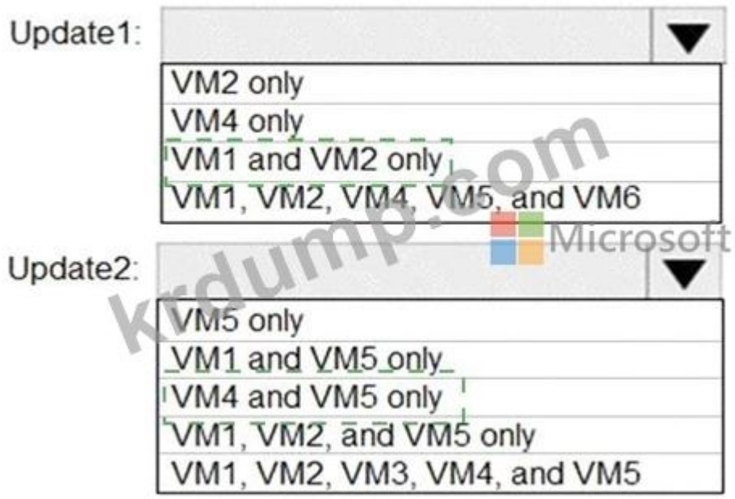
NEW QUESTION: 191
□□□□ □□□ □□□□ Azure □□ □□□ □□□□. □□ □□□ □□ □□ □□ □□□□ □□□□.

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

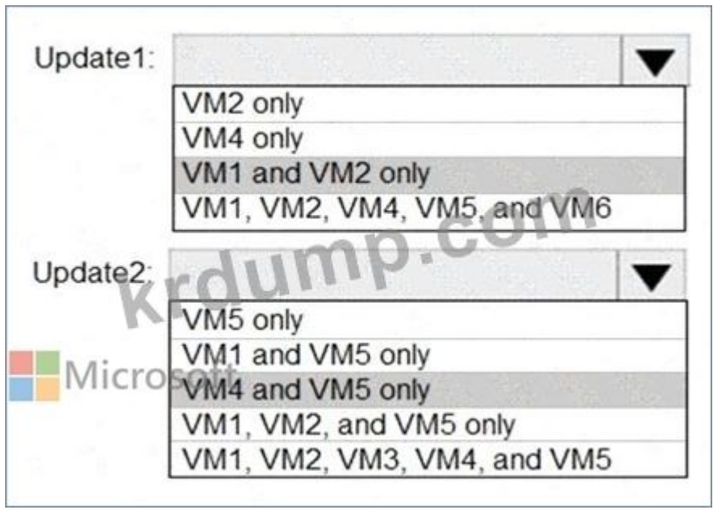
Update1□ Update2□□ □ □□ □□□□ □□□ □□□□□. Update1□ VM3□ □□□□□□, Update2□ VM6□ □□□□□□□.
□□□□ 1□ □□□□ 2□ □□□□ □□ □□ □□ □□□ □□□□□ □ □□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.



Answer:

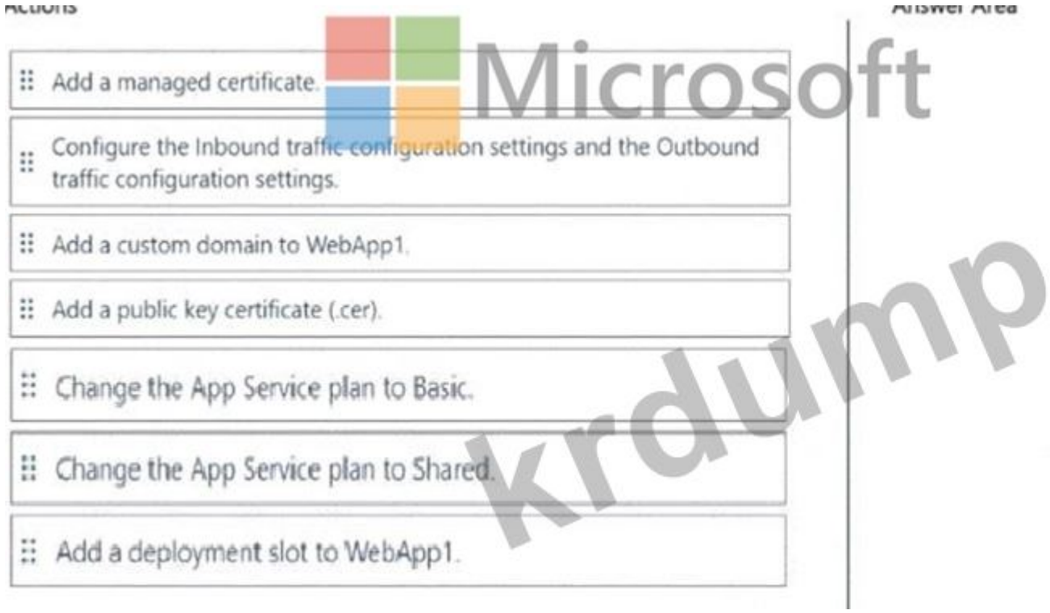


Explanation:

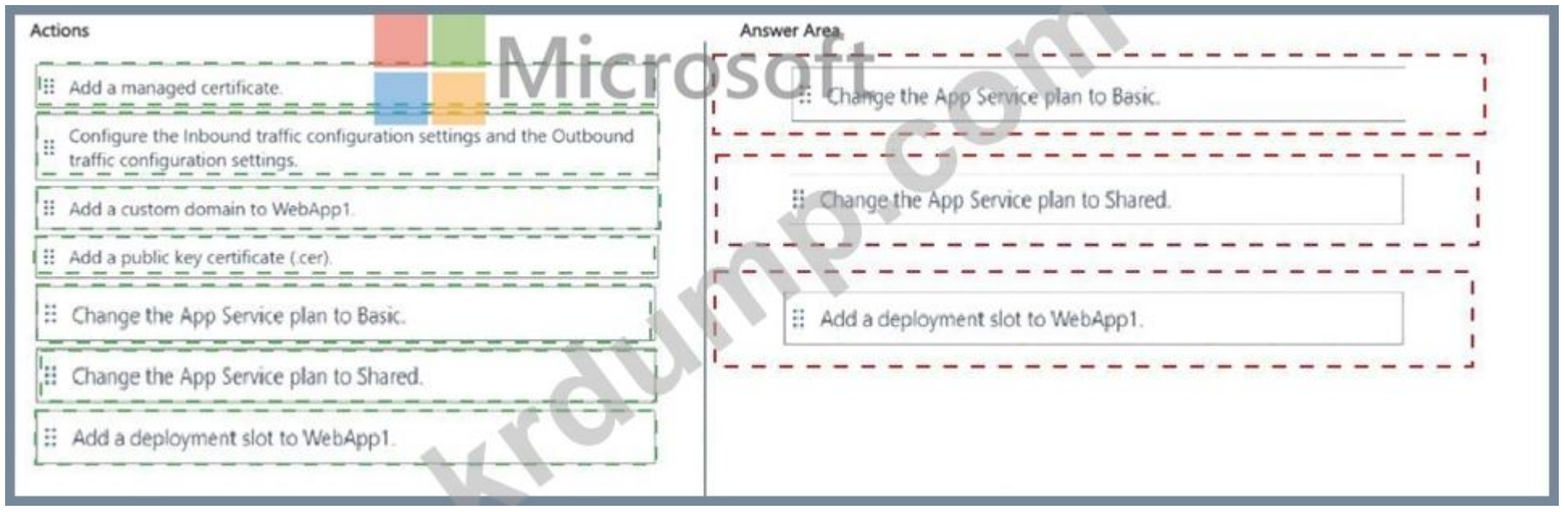


Update1: VM1 and VM2 only
VM3: Windows Server 2016 West US RG2
Update2: VM4 and VM5 only
VM6: CentOS 7.5 East US RG1
For Linux, the machine must have access to an update repository. The update repository can be private or public.
References:
https://docs.microsoft.com/en-us/azure/automation/automation-update-management

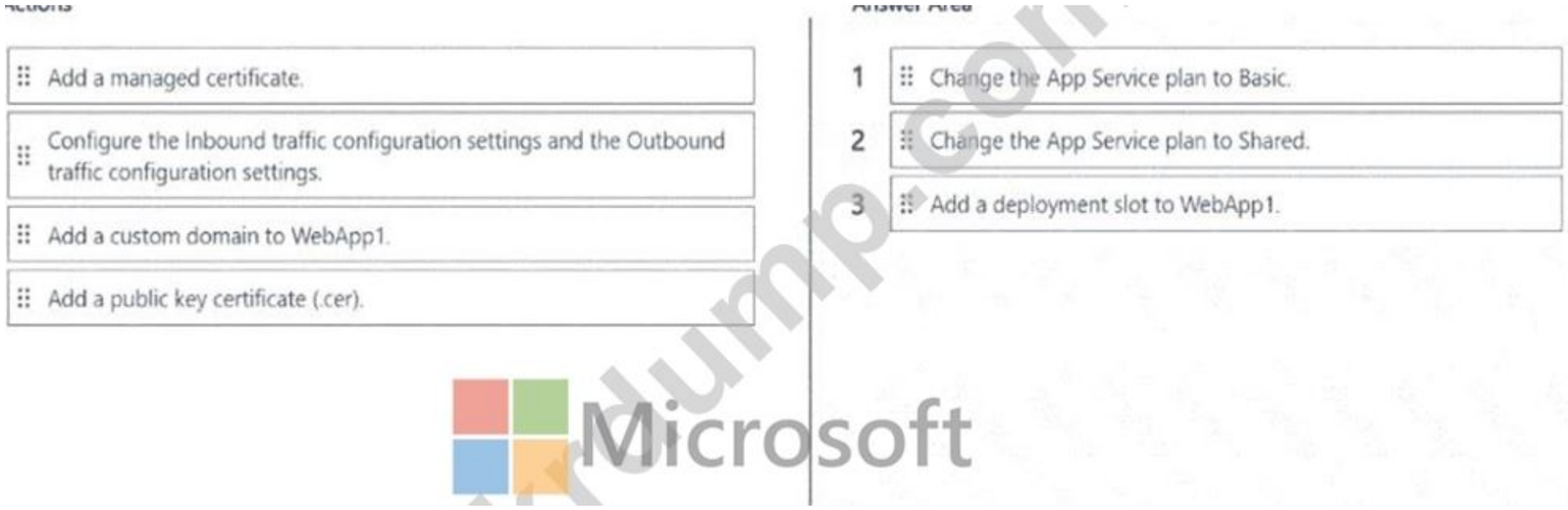
NEW QUESTION: 192
□□□□ Azure □□□□ □□□ □□ Azure App Service □ □□ □□□□ □□□□.
* □□: WebApp1
* □ □□□ □□□: □□
WebApp1□ App Service □□□ □□□□ □□□□□ □□□□ □□□. □□□□ □□□ □□□□□ □□□.
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□ □□□□□, □□ □□□□ □□□ □□□ □□ □□□ □□ □□□ □□□□ □□□□□.



Answer:



Explanation:



NEW QUESTION: 193

□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

Name	Type
storage1	Storage account
KeyVault1	Azure key vault

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

A. Add-A:StorogcAccountmanagementPolicyAction

B. -A=StorageAccount□ □□□□□.

C. Set-A;□□ □□ □□ □□

D. Add-AsKeyVaultmanageStorageAccount

Answer: D (LEAVE A REPLY)

NEW QUESTION: 194

Sub1□□□ Azure □□□ □□□□.

Azure Security Center□□ Play1□□□ □□ □□□□□ □□□□. Play1□ User1□□□ □□□□□ □□□ □□□□ □□□□ □□□□ □□□□.

□□□□□ □□□ □□ □□□ □□□ □□□□ □□□□ Play1□ □□□□ □□□.

Play1□ □□□□□ □□□ □□□□ □□□?

A. Azure DevOps

B. Azure □□□□□□ □□□□

C. Azure □□□

D. Azure Logic Apps □□□□

Answer: (SHOW ANSWER)

You can change an existing playbook in Security Center to add an action, or conditions. To do that you just need to click on the name of the playbook that you want to change, in the Playbooks tab, and Logic App Designer opens up.

References:

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

NEW QUESTION: 195
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: (SHOW ANSWER)
B: You can configure Azure DNS to host a custom domain for your web apps. For example, you can create an Azure web app and have your users access it using either www.contoso.com or contoso.com as a fully qualified domain name (FQDN). To do this, you have to create three records:
A root " A " record pointing to contoso.com
A root " TXT " record for verification
A " CNAME " record for the www name that points to the A record
F: To use HTTPS, you need to upload a PFX file to the Azure Web App. The PFX file will contain the SSL certificate required for HTTPS.
References: https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom- Domain

NEW QUESTION: 196
□□□ □□
□□□ □□ □□ □□□ □□ □□□ □□□□□.
□□□ □□□ □□□□□ □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
□□□□□ □□□□□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□ □□□□□.
Azure □□□ □□: Userl -28681041@ExamUsers.com
Azure □□□□: GpOAe4@lDg
Azure Portal□ □□□□□ □□□□□ □□□□ □□□ CTRL-K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.
□□ □□□ □□ □□ □□□□□ □□□□□.
□□□ □□□□: 28681041
□□ 1
□□□□□ VM1□□□ □□ □□□□□ RDP □□□ □□□□□ Azure□ □□□□ □□□.
□□□□ VM1□ □□ □□□ □□□□□ □□□.
Answer:
Check below steps in explanation for Task.
Explanation:
To configure Azure to allow RDP connections from the Internet to a virtual machine named VM1, you can follow the steps below:
* Create a new inbound security rule in the network security group (NSG) that is associated with the virtual network subnet that contains VM1. The rule should allow RDP traffic from the Internet to the virtual network subnet. You can use the Azure portal, Azure PowerShell, or Azure CLI to create the rule.
* Configure the network security group (NSG) to associate it with the virtual network subnet that contains VM1.

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

NEW QUESTION: 197
□□□□ Windows Server□ □□□□ □□□□□ □□□ 10□ □□□□.
□□□ Microsoft Defender for Cloud □□□ □□□ □□□ □□□□□. □□□ □□□ □□ □□□□ □□□?
A. Microsoft Configuration Manager □□□□□
B. Azure Arc Connected Machine □□□□
C. Microsoft Defender for Endpoint □□□□
D. Microsoft Sentinel□ □□ □□□ □□□ □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 198
Appl□□□ □□□ □□□ Azure □□□ □□□□. App1□ □□□□□ □□ □□□□ □□□□ □□□□□. □□□□ HTTPS://appl.contoso.com URL□ □□□□ App1□ □□□□□□. Pool!□ Pool2□□ □ □□ □□ □□ □□□□□. Pool1□ □□ □□□□ □□□□□, Pool2□ □□ □□□□ □□□□□□. Appl□ □□□ □□□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
* Pool1□ Pool2□□ TLS □□□ □□ □□□ □□□□□□.
* □□□ URL □□□ □□□□ □□□ □□□ □□ □□ □□□□□□.
□□□□ □□□ □□□□ □□□?
A. Azure □□□□□□ □□□□□
B. Azure □□□ □□□
C. Azure □□
D. Azure □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 199
Microsoft Defender for Cloud□ □□□□ Azure □□□ □□□□. □□ □□□□ □□ □□ □□ □□ Azure □□ □□□ □□□□ □□□□.

Name	Type	Category
Policy1	Policy	Regulatory Compliance
Policy2	Policy	Security Center
Initiative1	Initiative	Regulatory Compliance
Initiative2	Initiative	Security Center

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

A. Policy1 □ Policy2□

B. Policy1 □ Initiative1□

C. Initiative1 □ Initiative2□

D. Policy2 □ Initiative2□ □□

E. □□1, □□2, □□□□□1, □□□□□2

Answer: (SHOW ANSWER)

NEW QUESTION: 200

storage1□□□ □□□ Azure Data Lake Storage Gen2 □□□ □□□ Azure □□□ □□□□.

synapsews1□□□ Azure Synapse Analytics □□ □□□ □□□ □□ □□□□□ □□□□□. synapsews1□□ storage1□□ □□□□ □□□□□ □□□. □□□ □□□□ □□□?

A. □□ □□□□□

B. □□□□ □□ □□(NSG)

C. □□ □□□□ □□□□□

D. □□□

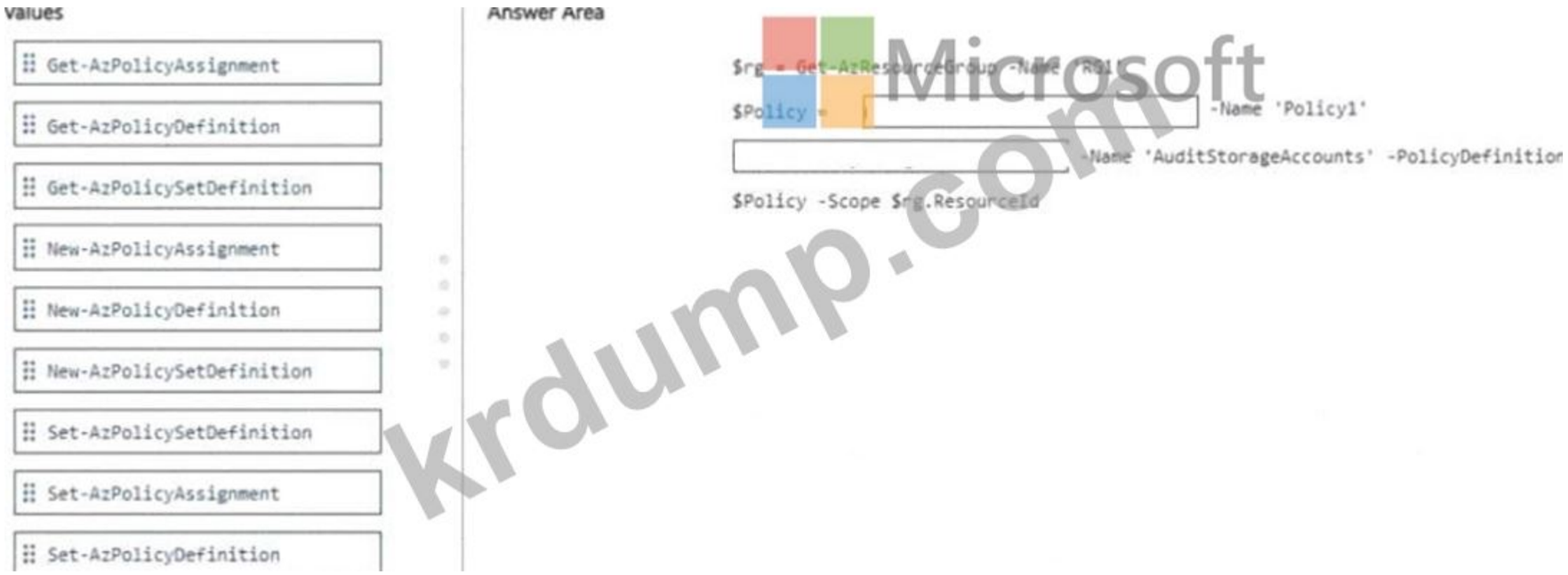
Answer: (SHOW ANSWER)

NEW QUESTION: 201

RG1□□□ □□□ □□□ Policy1□□□ Azure □□□ □□□ Azure □□□ □□□□.

RG1□ Policy1□ □□□□ □□□.

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



Answer:

Explanation:

NEW QUESTION: 202
Azure □□□ □□□□.
VM1□□□ □□ □□□ □□□ □□□□□.
VM1□□ □□ □□□ □□□□ □□□□ □□□.
VM1□ □□ □□ □□ □□□□ □□□□ □□, □□ □□□ □□□□ □□□□ □□□□ □ □□ □□□ □□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 203

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

Name	Has a network security group (NSG) associated to the virtual subnet
Subnet1	Yes
Subnet2	No

□□□□ □□ □□ □□□ □□ □□□ □□□□ □□□□.

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

□□ □□ □□□ □□ JIT(Just-In-Time) VM □□□□ □□□□□□.

JIT□ □□□□ □□ □□□ □□□□ □□□.

□□ □□ □□□ □□□□ □□□?

A. VM4□ □□

B. VM1 □ VM3□ □□

C. VM1, VM3 □ VM4□ □□

D. VM1, VM2, VM3 □ VM4

Answer: (SHOW ANSWER)

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

Reference:

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

NEW QUESTION: 204

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

□□□ □□ - □□ □□ □□□□ □□□ Microsoft Sentinel □□□□ □□□□ □□□.

□□ □□ □□□ □□□□ □□□?

A. Log Analytics □□ □□

B. Azure Machine Learning □□ □□
C. □□ □□
D. □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 205
□□ □□ □□□ □□ □□□□□ □□□□ Sub1□ Sub2□□ □ □□ Azure □□□ □□□□.

Name	Subscription	Tag
VNet1	Sub1	None
VNet2	Sub1	Red

□□ □□□ □□ AVNM1□□□ Azure Virtual Network Manager □□□□□ □□□□.
* □□□□ : Sub1
* □□□□ □□:
* NetGrp1: VNet1□ □□□□ □□ □□□
* NetGrp2: □□ □□□ □□ □□ □□□: Red□ □□□□ □□
* □□ □□ □□ □□□: SARule1
* □□ Azure □□□ □□□

Name	Subscription	Tag
VNet3	Sub1	Red
VNet4	Sub2	Red

□□ □□ □□□ □□ □ □□ □□□ □□ □□□□□ □□□□.
□□ □□ □□□□□ SARule1□ □□□□□?
A. VNet1, VNet2, VNet3 □ VNet4
B. VNet1 □ VNet2□ □□
C. VNet2, VNet3 □ VNet4□ □□
D. VNet2 □ VNet3□ □□
E. VNet1, VNet2 □ VNet3□ □□
Answer: E (LEAVE A REPLY)

NEW QUESTION: 206
□□ □□ □□□ □□□□ □□□ Microsoft Entra □□□□ □□□□.

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

□□ □□□ □□ □□□ □□ □□□ □□ □□□□□.

Admin2□ □□ □□□ □□ □□ □□□ □□□□□.
□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.
□□: □□ 1□□ 1□□□□.

Answer Area

Statements	Yes	No
Admin1 can view the Temporary Access Pass of Admin2.	○	○
Admin2 can add the Temporary Access Pass authentication method to User1.	○	○
Admin2 can add the Temporary Access Pass authentication method to Admin1.	○	○

Answer:

Answer Area

Statements	Yes	No
Admin1 can view the Temporary Access Pass of Admin2.	○	○
Admin2 can add the Temporary Access Pass authentication method to User1.	○	○
Admin2 can add the Temporary Access Pass authentication method to Admin1.	○	○

Explanation:

Answer Area

Statements	Yes	No
Admin1 can view the Temporary Access Pass of Admin2.	○	◉
Admin2 can add the Temporary Access Pass authentication method to User1.	◉	○
Admin2 can add the Temporary Access Pass authentication method to Admin1.	○	◉

NEW QUESTION: 207

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

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

□□□□ Azure Active Directory □□ □□□□ □□□ □□ □□□?

A. □□ □□□□□□ Azure □□□□ □□ □□□ □□□ □□□□ □□□□□.

B. □□□ □□ □□□□□□ □□□□ □□□□□□□ □□□ □ □□□ □□□□□.

C. □□ Wade□□ □□ □□□ □□□ □□ □□□□□.

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

Answer: B (LEAVE A REPLY)

NEW QUESTION: 208

□□ □□□ Azure Information Protection □□□ □□ □□□□.

Name	Pattern	Case sensitivity
Condition1	White	On
Condition2	Black	Off

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

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

Azure Information Protection□ □□□ □□□□ □□□□ □□□ □□□□ □□□.
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.

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

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

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

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

Answer:

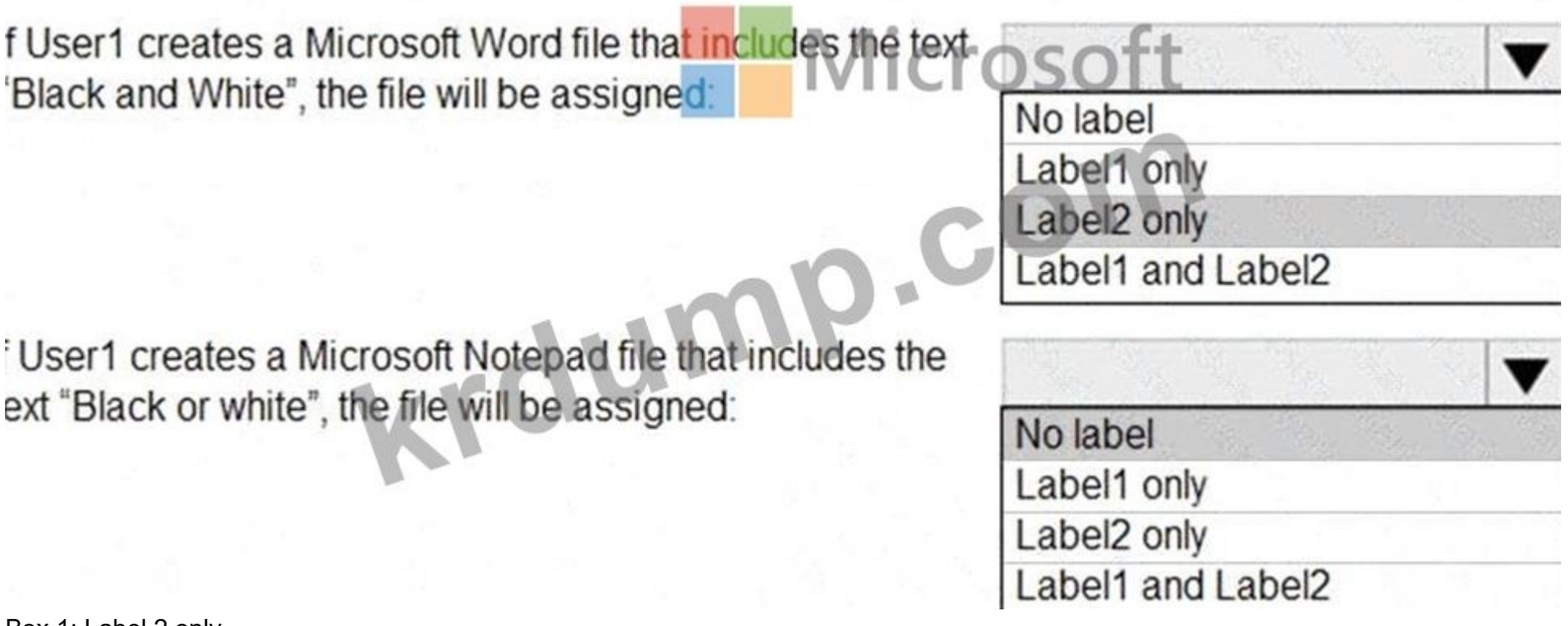
If User1 creates a Microsoft Word file that includes the text "Black and White", the file will be assigned:

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

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

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

Explanation:



Box 1: Label 2 only

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

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

Box 2: No Label

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

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

NEW QUESTION: 209
□□□ □□
□□ 5
Debbie□□ □□□□ □□□ □□□ Azure □□ □□□□ □□□□.
□□□ □□□ □□□□ debbie@contoso.com□ □□□ □□□□□ □□ □□□.
Answer:
see the task answer with step by step below:
* Create an Azure Resource Manager service principal. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to specify a name and a role for the service principal, such as Contributor.
* Grant permission to the service principal to access the secrets in the key vault. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to assign the Key Vault Secrets User role to the service principal at the scope of the key vault or individual secrets.
* Enable template deployment for the key vault. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to set the enabledForTemplateDeployment property of the key vault to true.
* Reference the secrets in the template by using their resource ID. You can use the listSecrets function to get the resource ID of a secret in the key vault. You need to specify the name of the key vault and the name of the secret as parameters.
* Deploy the template by using Azure PowerShell, Azure CLI, or REST API. You can use the New- AzResourceGroupDeployment cmdlet, the az deployment group create command, or the Deployments - Create Or Update REST API to do this. You need to provide the template file or URI and any required parameters. You also need to provide the credentials of the service principal.

NEW QUESTION: 210
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □ □ □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□□ □□□□.
Azure Security Center□ □□□□ □ □□ Azure □□□ □□ □□ □□□ □□ □□□ □□□□□.
□□□ □□□ □□□□□ □□ □□ □□ □□□ □□□□□.
□ □□ □□ □□□ □□ □□□ □□□□ □□□□ □□□.
□□□: □□□ □□□ □□□ □□□ □□ □□□□□□ □□□ □□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)
Instead use a management group.
Management groups in Microsoft Azure solve the problem of needing to impose governance policy on more than one Azure subscription simultaneously.
Reference:
https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with- managementgroups/

NEW QUESTION: 211
□□ □□ □□□ □□□□ □□□ Azure 480z □□□ □□□□.

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

□□ □□ □□□□ □□ □□□□.

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

SQL!□□□ □□□ Azure SQL □□ □□□□□ □□□ Microsoft Entra □□ □□□ □□□□□□.
User!□ User2□ □□ SQL1□ □□ Microsoft Entra □□□□ □□□□ □□□ □□□□ □□□.
□□ □□: Group2□ SQL1□ Microsoft Entra □□□□ □□□□□.
□□□ □□□ □□□□□?

A. □

B. □□□

Answer: (SHOW ANSWER)

NEW QUESTION: 212

□□ □□ □□□ □□□ □□□ □□□ Azure □□□ □□□□.

Name	Type
storage1	Azure Blob storage
storage2	Azure Files SMB
storage3	Azure Table storage

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

torage1:

- Shared Key only
- Shared access signature (SAS) only
- Azure Active Directory (Azure AD) only
- Shared Key and shared access signature (SAS) only
- Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

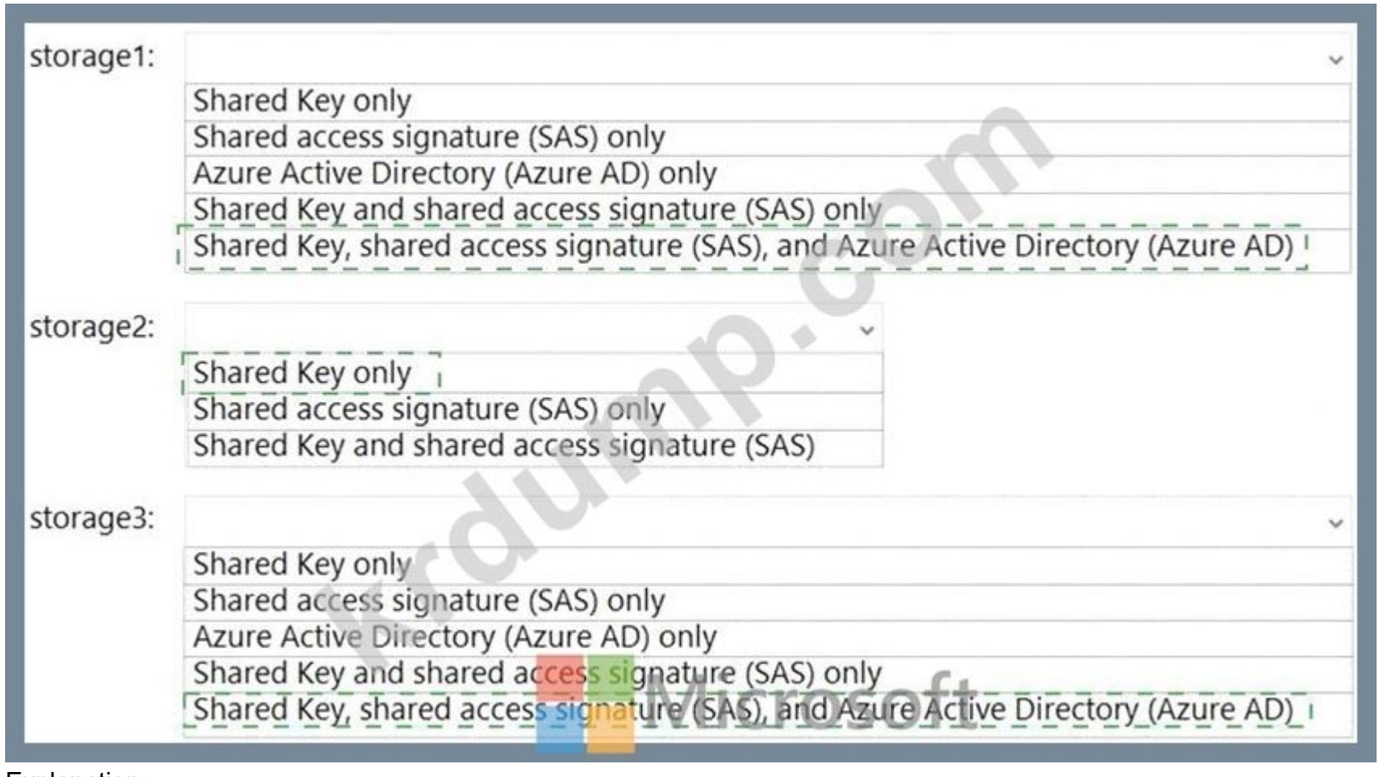
torage2:

- Shared Key only
- Shared access signature (SAS) only
- Shared Key and shared access signature (SAS)

torage3:

- Shared Key only
- Shared access signature (SAS) only
- Azure Active Directory (Azure AD) only
- Shared Key and shared access signature (SAS) only
- Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

Answer:



Explanation:

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

storage1:

- Shared Key only
- Shared access signature (SAS) only
- Azure Active Directory (Azure AD) only
- Shared Key and shared access signature (SAS) only
- **Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)**

storage2:

- **Shared Key only**
- Shared access signature (SAS) only
- Shared Key and shared access signature (SAS)

storage3:

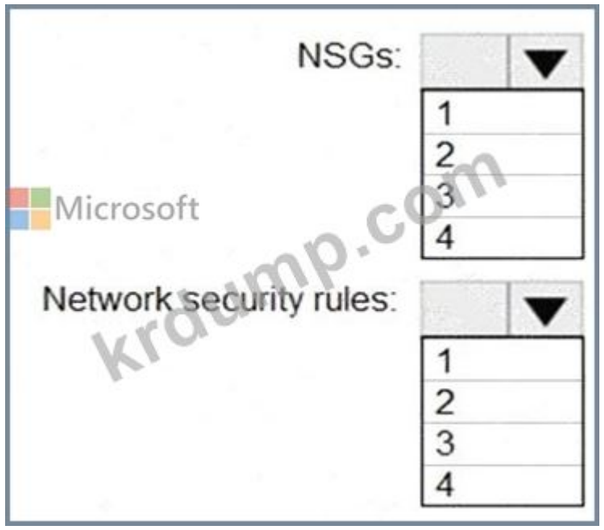
- Shared Key only
- Shared access signature (SAS) only
- Azure Active Directory (Azure AD) only
- Shared Key and shared access signature (SAS) only
- **Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)**

Reference:
https://docs.microsoft.com/en-us/azure/storage/common/authorize-data-access

NEW QUESTION: 213
Sub1□□□ Azure □□□ □□□□.
□□□ □□□□ □□□□ □□ □□□□□ □□□□. □□ □□□□ □□ □□ □□□ □□ □□□ □□□□□□□□.

Name	Network interface	Application security group assignment	IP address
VM1	NIC1	AppGroup12	10.0.0.10
VM2	NIC2	AppGroup12	10.0.0.11
VM3	NIC3	AppGroup3	10.0.0.100
VM4	NIC4	AppGroup4	10.0.0.200

□□ □□□□ □□ □□(NSG)□ □□□□□□□ □□□□□.
□□ □□ □□□ □□□□□ □□□□ □□□ □□□□ □□□.
* VM3□□□ VM4□□ □□□□ □□□□□.
* □□□□□ VM1□ VM2□□ □□□□ □□□□□.
* NSG □□ □□□□ □□ □□□ □□□□□□.
NSG□ □□□□ □□ □□□ □ □□ □□□□ □□□? □□ □□□□ □□□ □□□ □□□□ □□□□□.
□□: □□ 1□□ 1□□□□.



Answer:

Explanation:

NSGs: 1

Network security rules: 3

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

References:

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

NEW QUESTION: 214

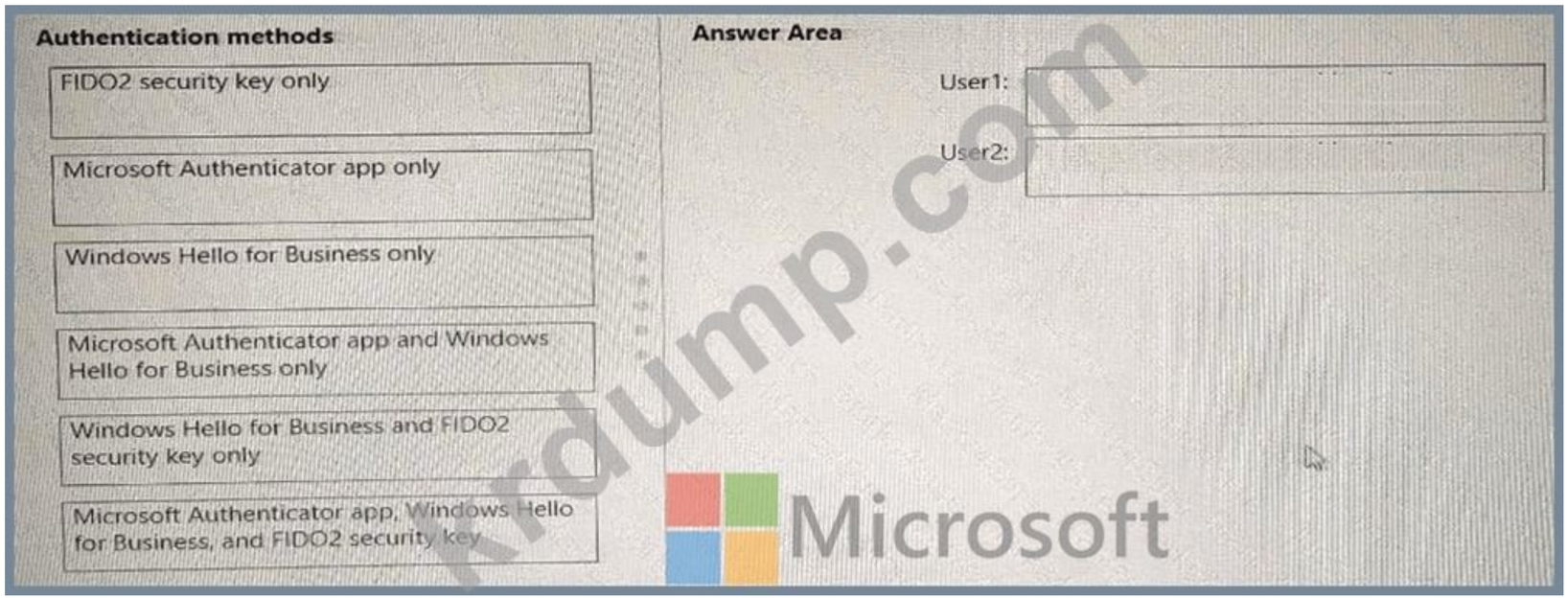
□□ □□ □□□ □□□□ □□□ Azure AD □□□□ □□□□.

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

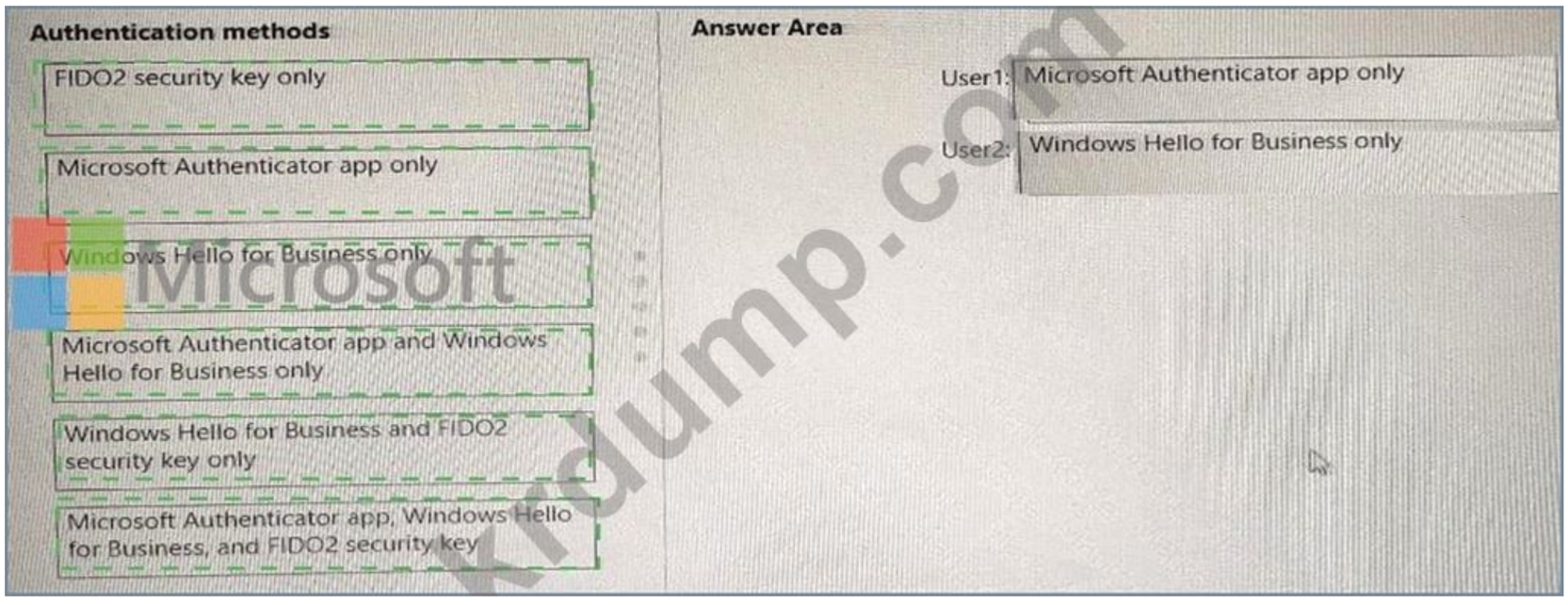
□□□□ □□ □□ □□ □□□ □□□□□□.

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

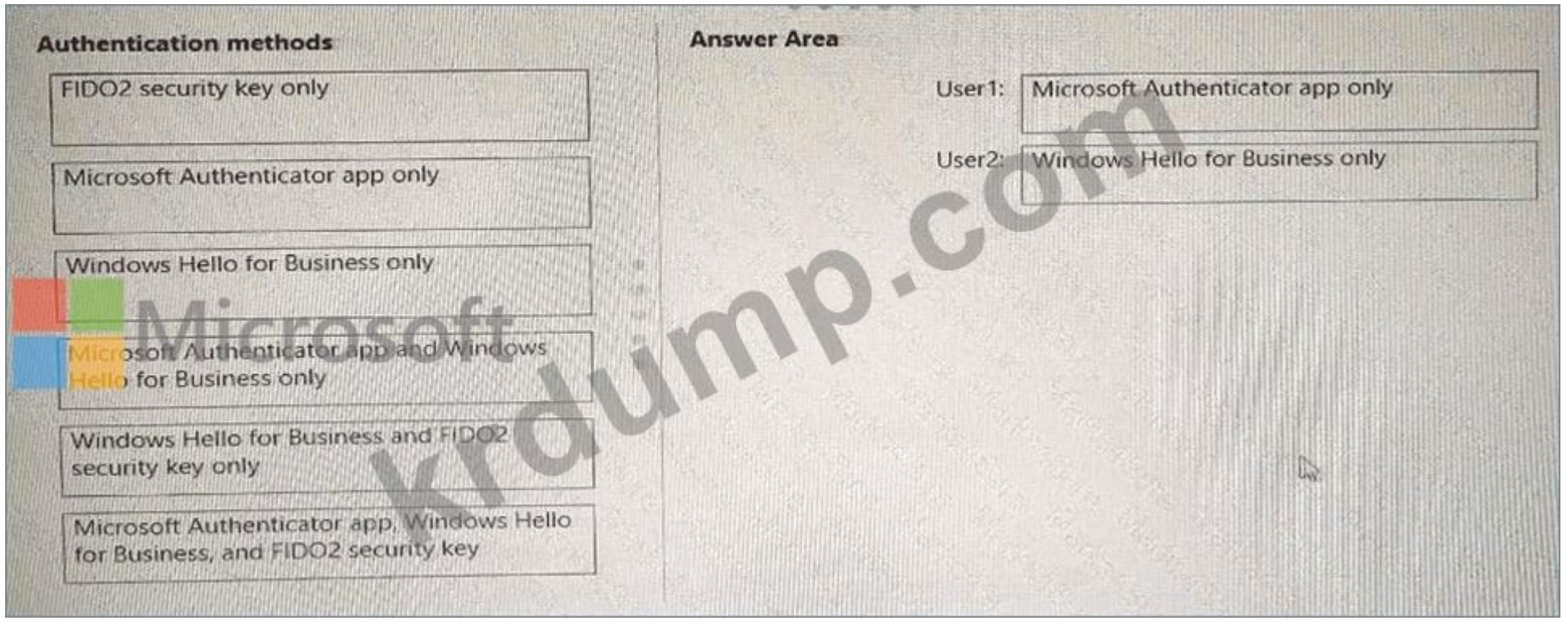
□□: □□ 1□□ 1□□□□.



Answer:



Explanation:



NEW QUESTION: 215

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

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

□□□□ □□ □□ □□□ □□□ □□□ □□□□□.

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

□□ □□ □□□ □□ App1□□□ □□□□ □□ □□ □□□ □□□ □□□ □□□□.

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

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

□□: □□ 1□□ 1□□□□.

Answer Area

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

Answer:

Answer Area

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

Explanation:

NEW QUESTION: 216
□□□ □□
□□ 3
SQL Server Management Studio(SSMS) □ Azure AD □□ □□□ □□□□ Danny-31330471□□□ □□□□ web31330471□□□ Microsoft SQL □□□ □□ SQL □□□□□□□ □□□□ □ □□□ □ □ □□□.
Answer:
see the task answer with step by step below:
* Create and register an Azure AD application. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to specify a name, such as SQLServerCTP1, and select the supported account types, such as Accounts in this organization directory only.
* Grant application permissions. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to assign the Directory.Read.All permission to the application and grant admin consent for your organization.
* Create and assign a certificate. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to create a self-signed certificate and upload it to the application. You also need to store the certificate in Azure Key Vault and grant access policies to the application and your SQL Server.
* Configure Azure AD authentication for SQL Server through Azure portal. You can use the Azure portal to do this. You need to select your SQL Server resource and enable Azure AD authentication. You also need to select your Azure AD application as the Azure AD admin for your SQL Server.
* Create logins and users. You can use SSMS or Transact-SQL to do this. You need to connect to your SQL Server as the Azure AD admin and create a login for Danny-31330471. You also need to create a user for Danny-31330471 in each database that he needs access to.
* Connect with a supported authentication method. You can use SSMS or SqlClient to do this. You need to specify the Authentication connection property in the connection string as Active Directory Password or Active Directory Integrated. You also need to provide the username and password of Danny-31330471.

NEW QUESTION: 217
□□ □□ □□□ □□□□□ AKS1 □ ID1 □□ ID□ □□□□ □□□. □□□□ □□ □□ □□□ □□□ □□□.
□ ID□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.

Answer:

Explanation:

NEW QUESTION: 218

contosos.com□□□ Azure Active Directory(Azure AD) □□□□ RG1□□□ □□□ □□□ □□□□ Subcription1□□□ Azure □□□ □□□□.

contoso.com□ □□ Role1□□□ □□□ □□ □□□ □□□□.

□□ □□□ □□ Role1□ □□□ □ □□ □□□ □□□□ □□□.

□□□ □□□□ □□□?

A. contoso.com□

B. contoso.com □ RGT□

C. contoso.com □ Subscription1□ □□

D. contoso.com, RG1 □ Subcription1

Answer: A (LEAVE A REPLY)
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles

NEW QUESTION: 219
□□: □ □□□□ □□□ □□□□□ □□□ □□□ □□ □□□ □□ □□□ □□□□ □□□□. □ □□□ □□ □□□ □□ □□□ □□□□ □□□□□. □□□□ □□□ □□□ □□□□□ □□□□ □ □□.
□□□ □□ □ □ □□□ □□ □□□ □□□ □ □□□□. □□ □□□ □□ □ □ □□□□ □□□ □□□□ □□ □□ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□□ □□□□.
□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

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

□□ □□ □□□□ □□ □□□□.

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

SQL1□□□ □□□ Azure SQL □□ □□□□□ □□□ Microsoft Entra □□ □□□ □□□□□□.
User1□ User2□ □□ SQL1□ □□ Microsoft Entra □□□□ □□□□ □□□ □□□□ □□□.
□□ □□: MM□ SQL1□ Microsoft Entra □□□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 220
□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

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

□□□ □□ Azure Defender□ □□□□ □□□□□.
Azure Defender□ □□□□ □□ □□□□ □□□ □ □□□?
A. VM1, VNET1, storage1 □ Vault1
B. VM1, VNET1 □ storage1□ □□
C. VM1, storage1 □ Vault1□ □□

D. VM1 □ VNET1□ □□
E. VM1 □ storage1□
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/security-center/azure-defender

NEW QUESTION: 221
□□□ Azure □□□□ □□ □□ □□□ □□ □□□□ □□□□ □□□□.

Name	SKU	Backend pool configuration
LB1	Standard	NIC
LB2	Standard	IP address
LB3	Gateway	NIC
LB4	Gateway	IP address

PLink1□□□ □□□ □□ □□ □□□□ □□□□ □□□.
PLink1□ □□ □□ □□ □□□□ □□□ □ □□□□?
A. LB1 □ I_B2
B. LB1 □ LB3
C. LB1 □□
D. LB2□ □□
E. LB2 □ LB4
Answer: A (LEAVE A REPLY)

NEW QUESTION: 222
User1□□□ □□□□ ConReg1□□□ Azure Container Registry□ □□□ Azure □□□ □□□□.
ContReg1□ □□ □□□ □□□ □□□□□□.
User1□ ContReg1□□ □□□ □ □□ □□□□ □□□ □ □□□ □□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
User1□□ □□ □ □□ □□□ □□□□ □□□? □ □□□ □□□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.
A. AcrQuarantineReader
B. □□□
C. AcrPush
D. AcrImageSigner
E. AcrQuarantineWriter
Answer: C,D (LEAVE A REPLY)
References:
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles

NEW QUESTION: 223
Azure □□□ RG1□□□ □□□ □□□ □□□□. RG1□□ storage1□□□ □□□□ □□□ □□□□.
RG1□ □□□ □□□ Role1 □ Role2□□ □ □□ □□□ □□ Azure □□□ □□□□.
Role1□ □□ □□□ □□ JSON □□□ □□ □□□□.

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

Role2□ □□ □□□ □□ JSON □□□ □□ □□□□.

Name	Role
User1	Role1
User2	Role2
User3	Role1, Role2

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

□□: □□ □□□ 1□□□□.

Answer Area

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

Answer:

Answer Area

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

Explanation:

NEW QUESTION: 224

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

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

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

□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

□□ □□ □□□□ □□ □□□□.

SQL1□□□ □□□ Azure SQL □□ □□□□□ □□□ Microsoft Entra □□ □□□ □□□□□□.

User1□ User2□ □□ SQL1□ □□ Microsoft Entra □□□□ □□□□ □□□ □□□□ □□□.

□□ □□: Group1□ SQL1□ Microsoft Entra □□□□ □□□□□.

□□□ □□□ □□□□□?

A. □□□

B. □

Answer: B (LEAVE A REPLY)

NEW QUESTION: 225

AzFW1□□□ Azure □□□□ □□□ Azure □□□ □□□□. AzFW1□□ FWPolicy1□□□ □□□ □□□ □□□□. □□ □□ □□□ □□□□□ FWPolicy1□ □□ □□□□ □□□□ □□□.

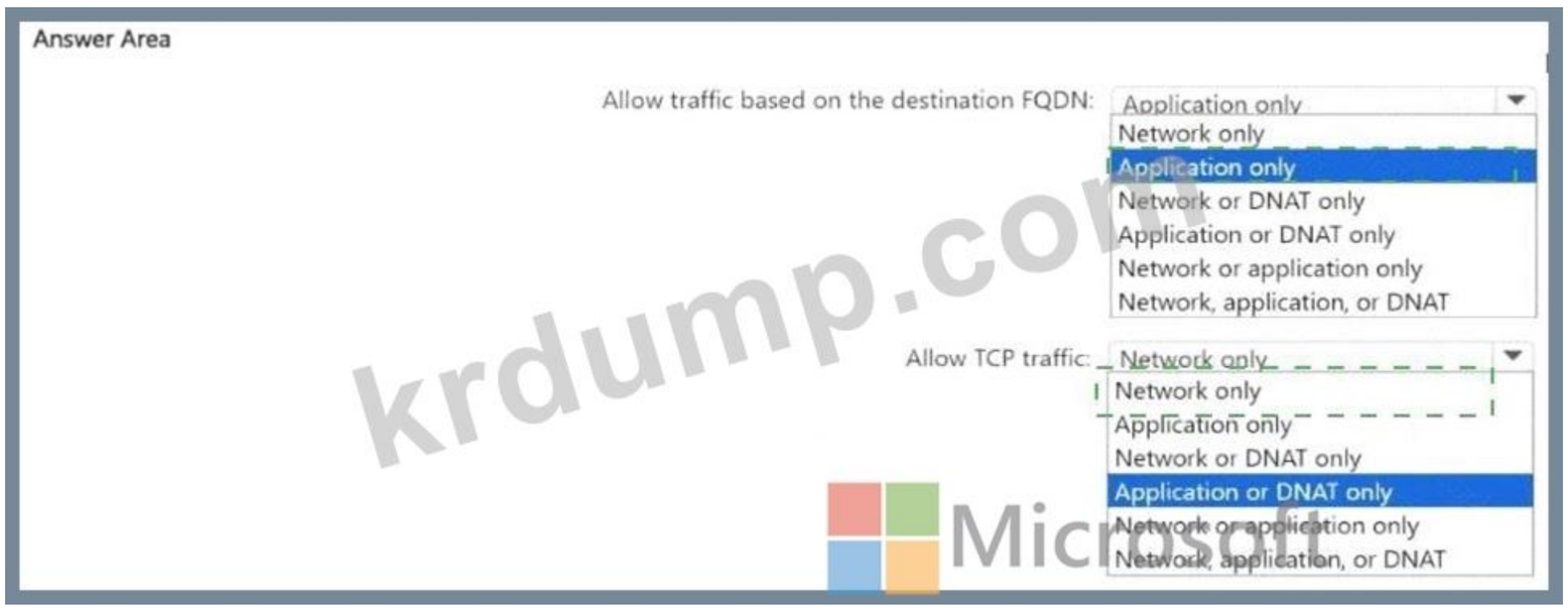
* □□□□ FQDN□ □□□□ □□□□ □□□□□.

* TCP □□□□ □□□□□.

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

□□: □□ 1□□ 1□□□□.

Answer:



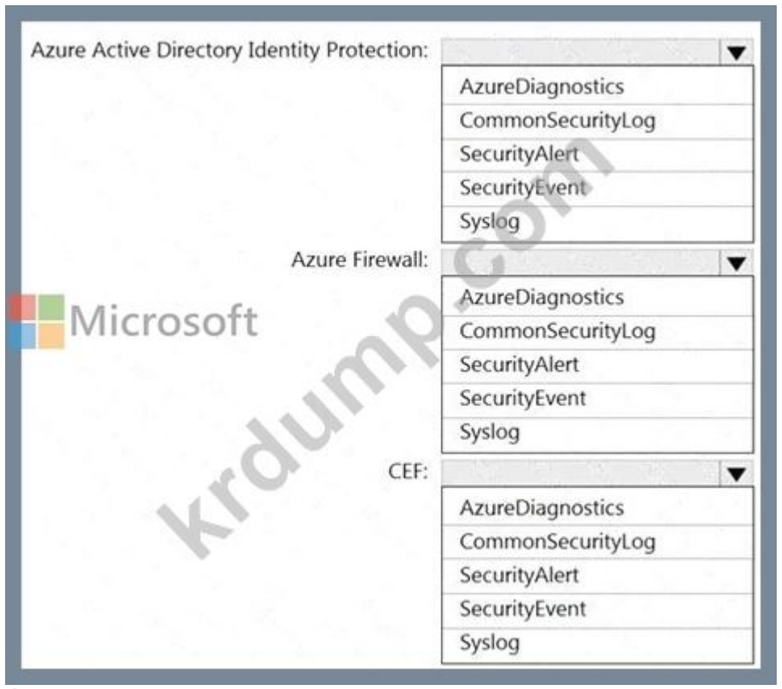
Explanation:

NEW QUESTION: 226

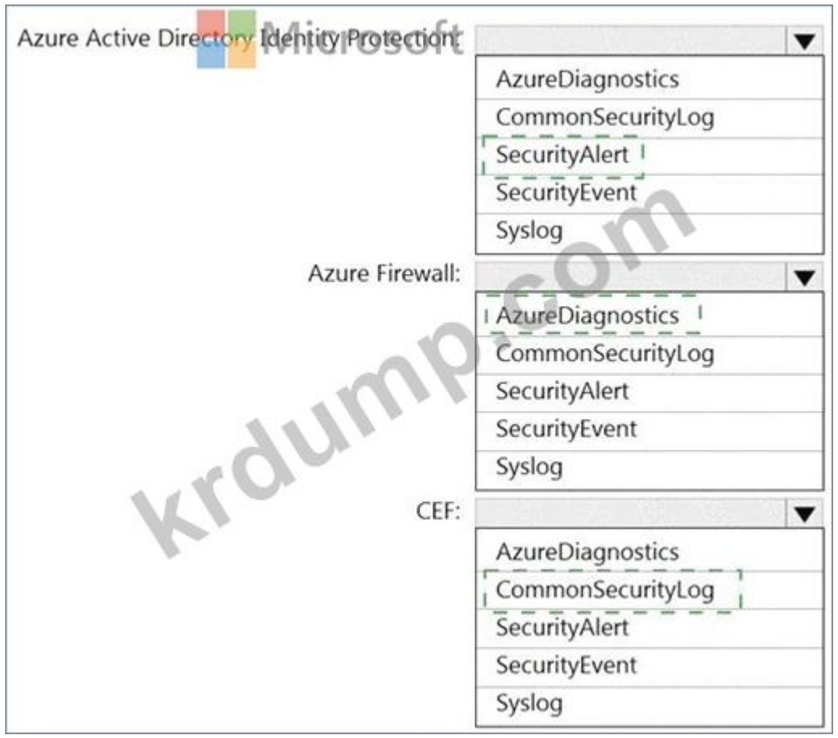
User1□□□ □□□□ □□□ Azure AD□ □□□□□ □□□□.

App1□□□ □□ □□□□□.
User1□ Azure AD □□□□□□ □□□□ □□□□ App1□ □□□□ □□□.
User1□□ □□ □□□ □□□□ □□□?
A. □□□□ □ □□ □□□
B. □□□□ □□□□□□ □□□
C. □□□□□ ID □□□
D. □□□□□□ □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 227
□□ □□□ □□□□ □□ Azure Sentinel □□ □□□ □□□□.
* Azure Active Directory ID □□
* □□ □□□ □□(CEF)
* Azure □□□
□ □□□□□ □□□□ □□□□□ □□□□ □□□.
□□ □□ □□□ □ □□□□ □□ □□ □□□□ □□□□ □□□? □□ □□□□ □□□ □□□ □□□□ □□□□□.
□□: □□ 1□□ 1□□□□.

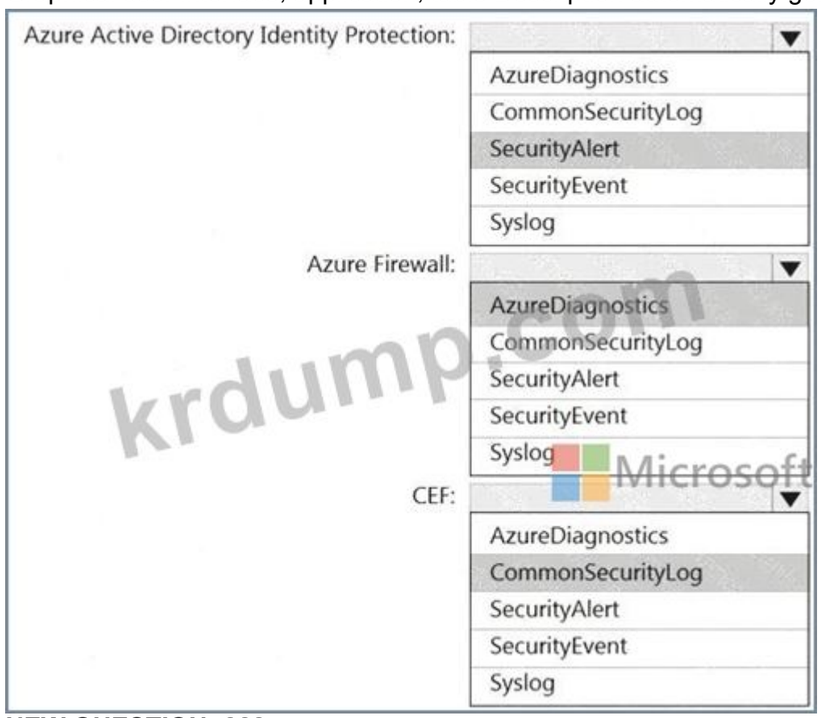


Answer:



Explanation:

Graphical user interface, application, table Description automatically generated



NEW QUESTION: 228

Azure Security Center□□ Registry1□ □□□□ □□ Azure Container Registry □□□ □□□ □□□□□□.

□□ □□□ □□□□□.
* Image1□□□ Windows □□□□ Registry1□ □□□□□.
* Image2□□ Linux □□□□ Registry1□ □□□□□.
* Image3□□□ □□□ Windows □□□□ Registry1□ □□□□□.
* Image1□ □□□□ □ □□□□ Image4□ Registry1□ □□□□□.
* Image2□ □□□□ □ □□□□ Image5□ Registry1□ □□□□□.
□□□□ □□□ □ □□□□ □□□□□? □□□ □□ □□□ □□□□ □□□□□.
□□: □□ 1□□ 1□□□□.
A. □□□4
B. □□□2
C. □□□3
D. □□□1
E. □□□5
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 229
□□ □□ Azure □□□ DB1□□□ Azure SQL □□□□□□□ □□□ Azure □□□ □□□□. □□ □□ □□ □□ □□□ □□□ □□□□.

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

DB1□ □□ □□□ □□□□ □□□□□.
DB1□ □□ □□□□ □□ □□□□ □□□ □□□ □ □□□?
A. Storage2 □ storage3□
B. storage1□
C. storage1 □ storage4□
D. storage1, storage2 □ storage3□
Answer: (SHOW ANSWER)

NEW QUESTION: 230
Azure □□□ □□□□.
□□□ □□ □□□ □□ □□ □□ □□□ □□(RBAC) □□ □□□ □□□□.

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

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

Answer Area

Statements	Yes	No
The custom role grants a user permission to delete Azure SQL Database resources.	○	○
The custom role grants a user permission to manage the Microsoft Entra admin settings for an Azure SQL Database server.	○	○
The custom role grants a user permission to reset the administrator password for instances of Azure Database for MariaDB.	○	○

Answer:

Answer Area

Statements	Yes	No
The custom role grants a user permission to delete Azure SQL Database resources.	○	○
The custom role grants a user permission to manage the Microsoft Entra admin settings for an Azure SQL Database server.	○	○
The custom role grants a user permission to reset the administrator password for instances of Azure Database for MariaDB.	○	○

Explanation:

Answer Area

Statements	Yes	No
The custom role grants a user permission to delete Azure SQL Database resources.	○	●
The custom role grants a user permission to manage the Microsoft Entra admin settings for an Azure SQL Database server.	○	●
The custom role grants a user permission to reset the administrator password for instances of Azure Database for MariaDB.	○	●

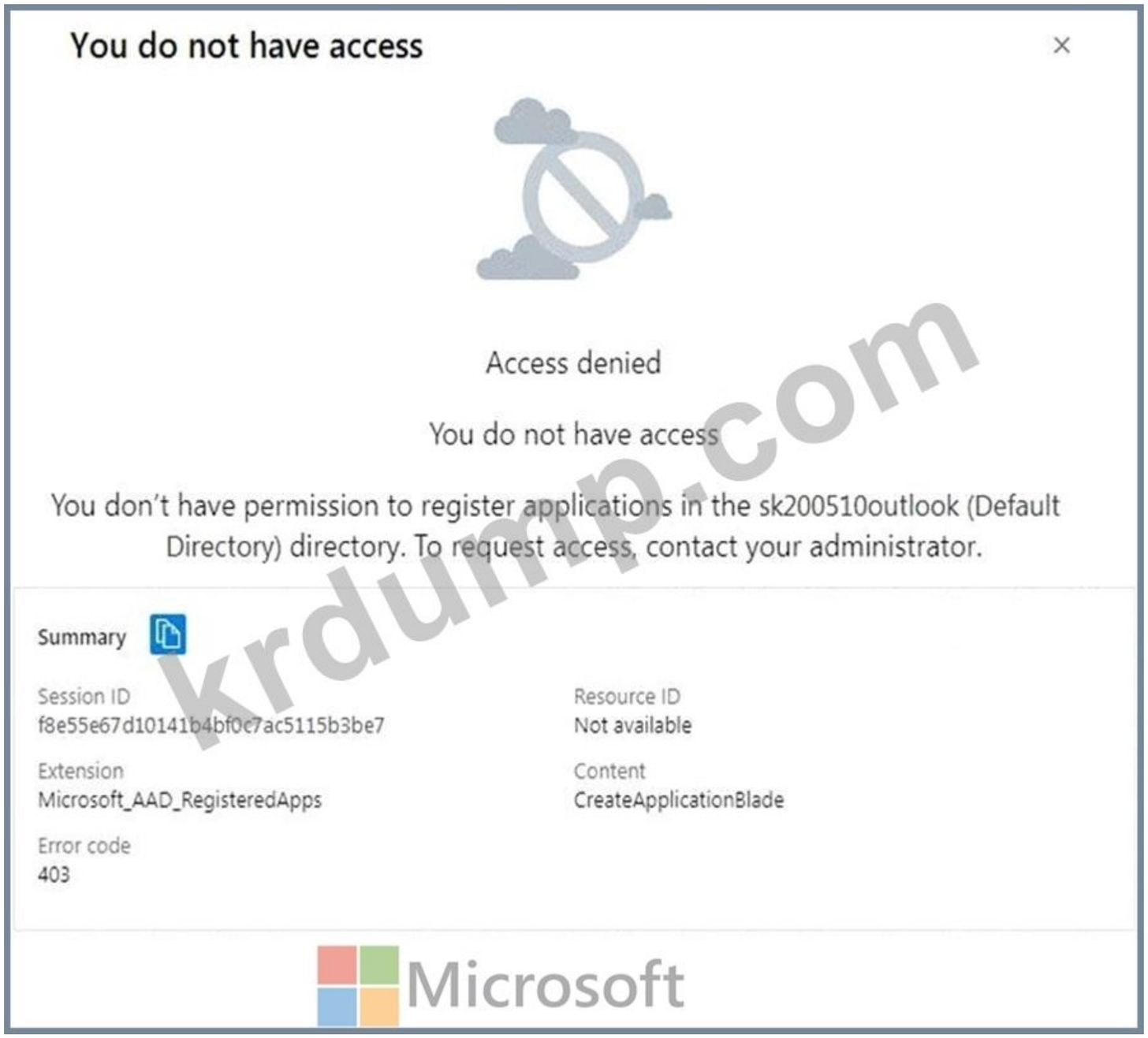
NEW QUESTION: 231
Microsoft Entra □□□□ □□□□.
□□□ □□ Microsoft Entra □□□□ Microsoft Entra ID□□ □□□ □□□ □□□□ □□□□ □□□□ □□□.
A. □□ □□□□□□ □□ □□□ □□□ □□ □□□□□.
B. □□□ □□ □□□□□□ Microsoft Entra ID □□ □□□ □□ □□□ □□□ □□ □□□□□.
C. □□□ □□ □□□□□□ □□□□ □□□□□□□ □□□ □ □□□ □□□□ □□□□□.
D. □□ □□□□□□ Azure □□□□ □□ □□□ □□□ □□□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 232
□□□ □□
□□□ □□ □□ □□□ □□ □□□ □□□□□.
□□□ □□□ □□□□□ □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
□□□□□ □□□□□ □□□□ □□ □□□ □□□ □□ □□□ □□□□□ □□□□□.
Azure □□□ □□: Userl -28681041@ExamUsers.com
Azure □□□□: GpOAe4@lDg
Azure Portal□ □□□□□ □□□□□ □□□□ □□□ CTRL-K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.
□□ □□□ □□ □□ □□□□□ □□□□□.
□□□ □□□□: 28681041
□□ 8
rg1lod28681041n1 Azure Storage □□□ □□ HTTP □□□ □□□□ □□□.
Answer:
Check below steps in explanation for Task.
Explanation:
To prevent HTTP connections to the rg1lod28681041n1 Azure Storage account, you can follow these steps:
* In the Azure portal, search for and select the storage account named rg1lod28681041n1.
* In the left pane, select Firewalls and virtual networks.
* In the Firewalls and virtual networks pane, select Selected networks.
* In the Selected networks pane, select Add existing virtual network.
* In the Add existing virtual network pane, select the virtual network that does not allow HTTP connections.

* Select Add.

NEW QUESTION: 233
Vault1□□□ Azure Key Vault□ VM1□□□ □□ □□□ □□□ Azure □□□ □□□□. VM1□□ Key Vault VM □□□ □□□□ □□□□.
Vault1□ □□ □, □□, □□□□ □□□□□.
VM1□ □□□□ □□□□□□ □□□ □□□□□?
A. □□□
B. □□□ □□□□
C. □, □□ □ □□□
D. □□ □□□
E. □□□□
F. □□
Answer: E (LEAVE A REPLY)

NEW QUESTION: 234
Azure Active Directory(Azure AD) □□□□ □□□ Azure □□□ □□□□.
□□□□ □□□□ App1□□□ □□ □□□□□ □□ □□ □□□ □□□ □□ □□□□ □□□□□.



□□□□ □□□□ App1□ □□□ □ □□□ □□□□ □□□.
□□□□ □□ □□□ □□ □□□?

A. □□□ □□ □□
B. □□ □□□ □□□□□ □□□□□.
C. □□□□ □□□ □□□□□.
D. □□□□□□ □□□□□□□ □□ □□ □ □□ □□□ □□□□□.

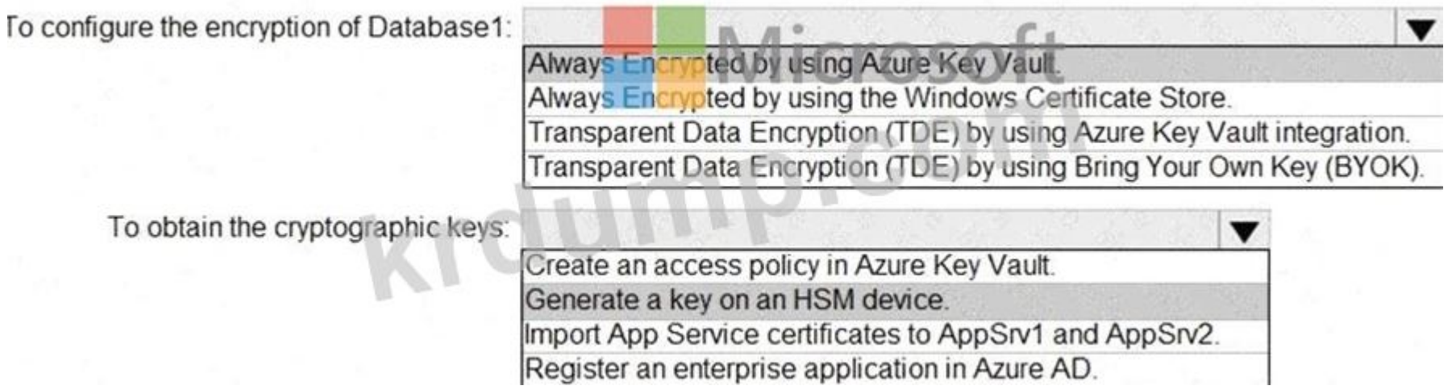
Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 235
□□ □□□□ □□□ Azure □□□ □□□□.
* Azure □ □□□
* Database1□□□ Azure SQL □□□□□□
* □□□□□ □□□ □□ ID□ □□□□ Database1□ □□□□□□ □□□ AppSrv1 □ AppSrv2□□ □ □□ Azure App Service □□ Database1□ □□ □□□ □□□□ □□□□ □□, □□ □□ □□ □ □□ □□□□ □□□.
* Database1□ Discount□□ □□ □□□□ AppSrv1□ □□□□ □□□ □ □□□ □□□□□□ □□□.
* AppSrv1 □ AppSrv2□ □□□ □□ □□ □□ □□□□ ID□ □□□□ □□□□□ □□□.
Database1□ □□□ □□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□□ □□ □□□□ 1□□ □□□ □□□□.

Answer:

Explanation:
Text Description automatically generated with medium confidence

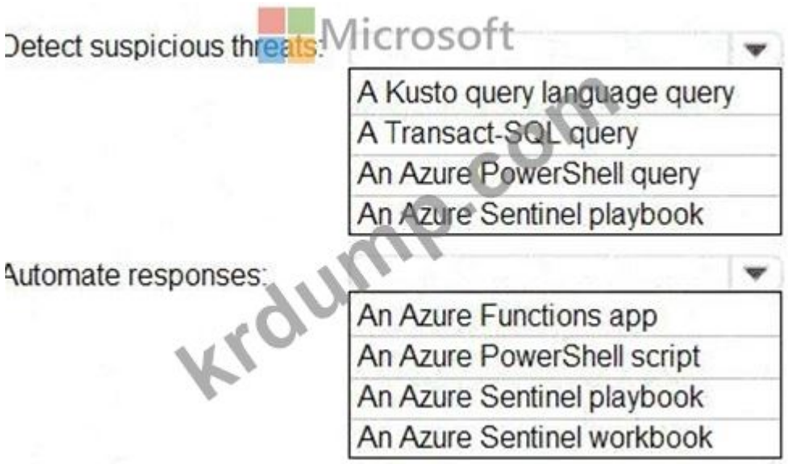


Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/database/always-encrypted-azure-key-vault-configure?tabs=azure-powershell

NEW QUESTION: 236
Azure □□□ □□□□.
ISO 27001 □□□ □□□□ □□ Azure □□ □ □□□□□ □□□□ □□□. □□□ □□□□ □□□?
A. Azure Sentinel
B. Azure Active Directory(Azure AD) ID □□
C. Azure □□ □□
D. Azure □□ □□ □□(ATP)
Answer: C (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-compliance-dashboard

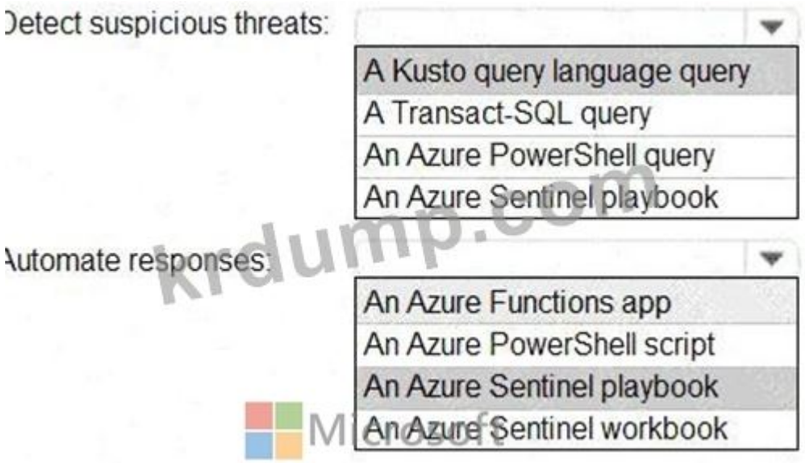
NEW QUESTION: 237
Azure □□□ WebApp1□□□ Azure App Services □ □□ □□□□. WebApp1□ □□ Azure □□□ □□□□ □□□□□□.
WebApp1□ □□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
* □□□□ □ □□□□□□□ □□□□□.
* □□ □□ □□□□ □□□□ □□□□ □□□□ □□□□□□.
□□□ □□□□ □□□?
A. Azure □□□
B. Azure Front Door Premium
C. Azure Application Gateway
D. Azure □□□ □□ □□□□(CDN)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 238
Azure Sentinel□ □□□□ □□□□□ □□□ □□□□ □□□ □□□□□ □□ □□□ □□ □□□□□.
□□□ □□□ □□ □□□ □□□□□? □□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ 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: 239

Azure Storage □□□ □□ □□□ □□□□ □□□□.

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

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

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

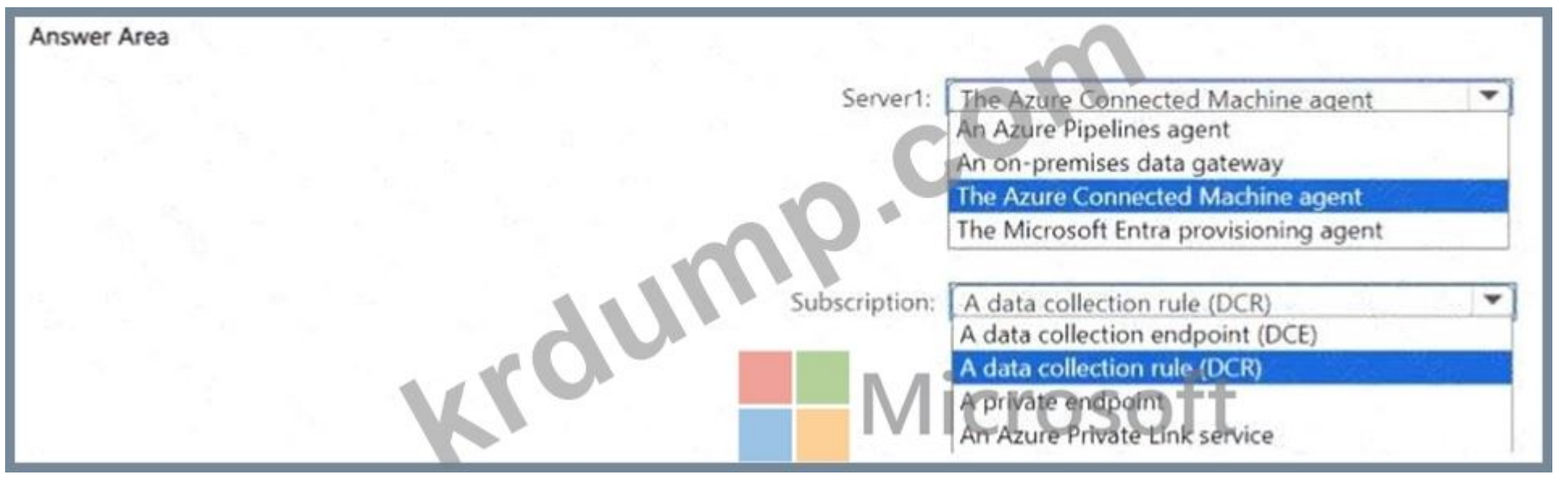
NEW QUESTION: 240
Azure Firewall Standard□ AzFWL □□□□□ □□□ Azure □□□ □□□□. AzFW1□□ □□ □□□ □□□ □ □□□ □□□□ □□□.
* TLS □□
* □□ □□□□□
* □□□□ □□ □□ □ □□ □□□(IDPS)
□□□ □□□ □ □□□?
A. □□ □□□□□□
B. TLS □□□ □□
C. □□ □□□□□ □ IDPS□
D. TLS □□ □ IDPS□
E. TLS □□, □□ □□□□□ □ IDPS
Answer: (SHOW ANSWER)

NEW QUESTION: 241
Azure □□□ □□□□.
□□□□□ Azure DNS □□□ □□ □□□ □□□ □□ □□□.
Cloud Workload Protection(CWP)□ □□ □□ Microsoft Defender □□□ □□□□□ □□□?

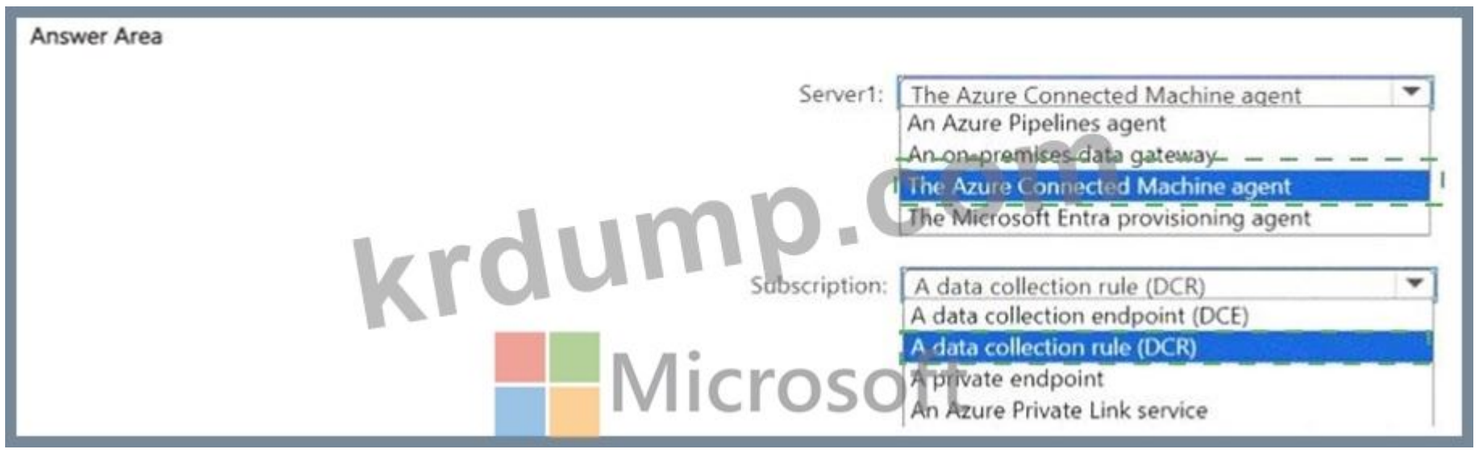
A. API
B. □ □□□
C. □□
D. □□□ □□□
E. □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 242
Azure Key Vault□ Azure Storage □□□ □□□ Azure □□□ □□□□. Key Vault□□ □□ □□ □□ □□□□ □□□□. Storage □□□ Key Vault□ □□□ □□ □□ □□ □□□□□ □□□□ □□□ □.
□□ □□□□ □□□□ Azure□ □□□□ □□□ □□□□□.
* Azure □□
* Azure Blob □□□
* Azure □□ □□
* Azure □□□ □□□
* Azure □ □□□
□ □□□□ □□□ □□ □□□□ □□□□ □□□□□ □ □□□□ □□□□□? □ □□□ □□□ □□□□ □□□□□.
□□: □□ 1□□ 1□□□□.
A. □ □□□
B. □□□ □□□
C. Azure □□
D. □□ □□□
Answer: C,D (LEAVE A REPLY)
https://docs.microsoft.com/en-us/azure/storage/common/account-encryption-key-create?tabs=portal

NEW QUESTION: 243
Server1□□□ □□□□□ □□□ □□□□.
Sentinel 1□□□ Microsoft Sentinel □□ □□□ □□□ Azure □□□ □□□□.
Sentinel1□ Windows □□□ □□□□ □□□□□.
Server1□ Windows Defender □□□□ □□□□□□□ Microsoft Sentinel□ □□□□ □□□.
Server1□ □□□ □□□□ □□, Azure □□□ □□□ □□□□ □□□? □□ □□□□ □□□ □□□ □□□□ □□□□□.
□□: □□ 1□□ 1□□□□.



Answer:



Explanation:

NEW QUESTION: 244

□□□ □□

□□□ □□ □□ □□□ □□ □□□ □□□□□.

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

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

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

Azure □□□□: GpOAe4@lDg

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

□□ □□□ □□ □□ □□□□□ □□□□□.

□□□ □□□□: 28681041
□□ 9
KeyVault28681041 Azure Key Vault□ □□□ □□ □□□□ rg1lod28681041n1 Azure Storage □□□ □□□□□□□ □□□□ □□□.
Answer:
Check below steps in explanation for Task.
Explanation:
To ensure that the rg1lod28681041n1 Azure Storage account is encrypted by using a key stored in the KeyVault28681041 Azure key vault, you can follow these steps:
* In the Azure portal, search for and select the storage account named rg1lod28681041n1.
* In the left pane, select Encryption.
* In the Encryption pane, select Customer-managed key.
* In the Customer-managed key pane, select Select from Key Vault.
* In the Select from Key Vault pane, enter the following information:
* Key vault: Select the KeyVault28681041 Azure key vault.
* Key: Select the key you want to use.
* Select Save.

NEW QUESTION: 245
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: (SHOW ANSWER)
Azure Container Registry implements Docker ' s content trust model, enabling pushing and pulling of signed images.
To push a trusted image tag to your container registry, enable content trust and push the image with docker push.
To work with trusted images, both image publishers and consumers need to enable content trust for their Docker clients. As a publisher, you can sign the images you push to a content trust-enabled registry.
Reference:
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust

NEW QUESTION: 246
contoso.com□□□ □□□□□ Microsoft Entra □□□□ □□, □□□□ Uset1□□□ □□□□ □□ □□ □□□ □□□ □□□□ □□□□.

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

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

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

Answer:

Explanation:

Answer Area

Statements	Yes	No
User1 can map share1 to Server1 by using the access key of storage1.	○	●
User1 can map share1 to Server1 by using the user's credentials.	●	○
User1 can map share1 to Server2 by using the access key of storage1.	○	●