

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 □□□□ □□□□.

Microsoft		
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:

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

Microsoft

Be prompted for MFA

Be blocked

Be prompted for MFA

Sign in by using a username and password only

Be blocked

Be blocked

Be prompted for MFA

Sign in by using a username and password only

Answer:

Answer Area

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

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

Explanation:

Answer Area

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

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

NEW QUESTION: 2

LAW1000 Azure Log Analytics 10000 Sub1000 Azure 1000 10000.

Windows Server 2016 10000 LAW10 1000 Azure 10 1000 5000 10000.

LAW10 1000 10000 10 10000 1000 100000.

1000 10000 10 10 1000 100000 LAW10 1000000 10 1000.

10 10 1000 10000 10000 1000? 10000 10 10000 10 1000 10 10000 10 1000 10000 100000.

Actions	Answer Area
Create a new workspace.	
Apply the scope configuration to the solution.	
Create a scope configuration.	
Create a computer group.	
Create a data source.	

Answer:

Actions

Create a new workspace.

Apply the scope configuration to the solution.

Create a scope configuration.

Create a computer group.

Create a data source.

Answer Area

Create a computer group.

Create a scope configuration.

Apply the scope configuration to the solution.

Explanation:

Create a computer group.

Create a scope configuration.

Apply the scope configuration to the solution.

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, Microsoft Entra ID.

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

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

Answer Area

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

Answer:

Answer Area

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

Explanation:

Answer Area

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

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

□□□□ □□ □□ □□□ □ □□ □□□□ □□□□.

Microsoft	
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

Microsoft		Yes	No
Statements			
WebApp1 can connect to VM2.		☒	☐
NSG1 controls inbound traffic to WebApp1.		☐	☒
WebApp2 can connect to VM1.		☐	☒

Explanation:

Answer Area



Microsoft

Statements

WebApp1 can connect to VM2.	☒ Yes	☐ No
NSG1 controls inbound traffic to WebApp1.	☐ Yes	☒ No
WebApp2 can connect to VM1.	☐ Yes	☒ No

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 Administrator

□□□ □□□ □□□□□ □□□□□□□□.

□□□ Subscription1□ □□□□ □□□□ □□□.

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

□□: □□ 1□□ 1□□□□.

User:

▼

User1

User2

User3

User4

Tool:

▼

Azure Account Center

Azure Cloud Shell

Azure PowerShell

Azure Security Center

Answer:

User: Microsoft ▼

- User1
- User2
- User3
- User4

Tool: ▼

- Azure Account Center
- Azure Cloud Shell
- Azure PowerShell
- Azure Security Center

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 Area



AU1:

- AU2 only
- Group2 only
- Identity1 only
- AU2 and Group2 only
- Group2 and Identity1 only

AU2:

- Identity1 only
- AU1 and Identity1 only
- Group1 and Group2 only
- AU1, Group2 and Identity1 only
- Group1, Group2 and User1 only

Answer:

Answer Area



AU1:

- AU2 only
- Group2 only
- Identity1 only
- AU2 and Group2 only
- Group2 and Identity1 only

AU2:

- Identity1 only
- AU1 and Identity1 only
- Group1 and Group2 only
- AU1, Group2 and Identity1 only
- Group1, Group2 and User1 only

Explanation:

Answer Area



AU1: Group2 and Identity1 only

AU2: Group1, Group2 and User1 only

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	DeployIfExists	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


```
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□□□□.

Traffic destined for an Azure Storage account is [answer choice].



- able to connect to East US
- able to connect to East US 2
- able to connect to West Europe
- prevented from connecting to all regions

FTP connections from 1.2.3.4 to 10.0.0.10/32 are [answer choice].

- allowed
- dropped
- forwarded

Answer:

Traffic destined for an Azure Storage account is [answer choice].

- able to connect to East US
- able to connect to East US 2
- able to connect to West Europe
- prevented from connecting to all regions

FTP connections from 1.2.3.4 to 10.0.0.10/32 are [answer choice].

- allowed
- dropped
- forwarded

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 ☐ ☐ ☐ ☐ ☐ ☐?

Container registries:

▼

0

1

2

3

 Workspaces:

▼

0

1

2

3

Answer:

Container registries:

0

1

2

3

Workspaces:

0

1

2

3

 Microsoft

Explanation:
Table Description automatically generated with medium confidence

Container registries:

0

1

2

3

Workspaces:

0

1

2

3

 Microsoft

Reference:

NEW QUESTION: 14

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

□□ □□□□□ □□ □□□ □□□ □□ □□□□. □□ □□□ Microsoft Azure Management □□□□ □□ □□ □□□□ □□□□ □ □□□□□.

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

Portal Policy	Conditions	Locations
Info Delete Name Portal Policy Assignments Users and groups All users Cloud apps 1 app included Conditions 1 condition selected Access controls Grant 2 controls selected Session 0 controls selected	Info Device platforms Not configured Locations 1 included Client apps (preview) Not configured Device state (preview) Not configured	Control user access based on their physical location. Learn more Configure Yes No Include Exclude ☐ Any location ☐ All trusted locations ☒ Selected locations Select Contoso Contoso ...

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

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 Area

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

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

Microsoft

Answer:
answer area

Storage accounts that can be used as the audit log destination:	- Storage1 only - Storage2 only - Storage1 and Storage2 only - Storage1, Storage2, and Storage3
Log Analytics workspaces that can be used as the audit log destination:	- Analytics1 only - Analytics1 and Analytics2 only - Analytics1 and Analytics3 only - Analytics1, Analytics2, and Analytics3

Explanation:

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

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

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

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

NEW QUESTION: 16

[illegible]* :

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

Company1 has two storage accounts named storage1 and storage2. Blob containers are created in storage1. Azure Active Directory has a policy named Policy1.

Name	Storage account	Access policy
container1	storage1	Policy1
container2	storage1	None

Policy1 is configured to require MFA for all users.

Edit policy

Identifier * Permissions

Start time Expiry time

storage1 has a SAS1 policy. The policy is configured as follows:

* Resource: Blob

* Resource type: Container

* Permissions: Read, Write, Delete, Append, Manage

* Blob container: container1

* Start time: 12/15/2025

* Expiry time: 12/31/2025

* Start time: 2025 12 15

* Expiry time: 2025 12 31

* Format: MM/DD/YYYY

* Time zone: UTC, UTC+01:00, UTC+02:00, UTC+03:00, UTC+04:00, UTC+05:00, UTC+06:00, UTC+07:00, UTC+08:00, UTC+09:00, UTC+10:00, UTC+11:00, UTC+12:00, UTC+13:00, UTC+14:00, UTC+15:00, UTC+16:00, UTC+17:00, UTC+18:00, UTC+19:00, UTC+20:00, UTC+21:00, UTC+22:00, UTC+23:00, UTC+24:00

* Time zone: UTC, UTC+01:00, UTC+02:00, UTC+03:00, UTC+04:00, UTC+05:00, UTC+06:00, UTC+07:00, UTC+08:00, UTC+09:00, UTC+10:00, UTC+11:00, UTC+12:00, UTC+13:00, UTC+14:00, UTC+15:00, UTC+16:00, UTC+17:00, UTC+18:00, UTC+19:00, UTC+20:00, UTC+21:00, UTC+22:00, UTC+23:00, UTC+24:00

Which two statements are true about Azure SQL managed instances?

Name	Assigned server admin	Database
sqlsrv1	User1	DB1
sqlsrv2	Group1	DB2

Microsoft Entra ID is used for authentication.

Users are assigned permissions at the database level.

Users are assigned permissions at the server level.

Answer Area

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

Answer:

Answer Area

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

Explanation:

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.	☐	☒

NEW QUESTION: 20

AKS1 is an Azure Kubernetes Service (AKS) cluster. Which two statements are true about AKS1?

Azure DevOps Microsoft Agent for Kubernetes is installed on the AKS1 cluster.

The AKS1 cluster is configured to use the Azure DevOps Microsoft Agent for Kubernetes.

AKS1 is configured to use the Azure DevOps Microsoft Agent for Kubernetes.

A. IP address

B. Azure DevOps Microsoft Agent for Kubernetes (AGIC)

C. Azure DevOps Microsoft Agent for Kubernetes

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□□□□.

Account type:
Azure Active Directory User
Managed identity
Service Principal
Roles:
db_datawriter only
db_datareader and db_datawriter
db owner only

Answer:

Cmdlets

New-AzStorageAccountKey
New-AzStorageTable
Register-AzProviderFeature
New-AzStorageAccount
Register-AzResourceProvider

Answer Area

Answer:

Cmdlets	Answer Area
New-AzStorageAccountKey	New-AzStorageAccount
New-AzStorageTable	New-AzStorageAccountKey
Register-AzProviderFeature	New-AzStorageTable
New-AzStorageAccount	
Register-AzResourceProvider	

Explanation:

Text, table Description automatically generated with medium confidence

New-AzStorageAccount
New-AzStorageAccountKey
New-AzStorageTable

Reference:

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

NEW QUESTION: 24

Azure Vault1 is an Azure Key Vault. Vault1 key1 is a 2048-bit RSA key. key1 is 90 days before expiration. What is the best way to ensure key1 is renewed?

- A. key1 is EC key.
- B. key1 is RSA key.
- C. Vault1 is Key Vault Premium.
- D. Vault1 is Key Vault Standard.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 25

contoso.com Azure Active Directory(Azure AD) and Azure Resource Manager. The following table shows the roles assigned to the users.

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

RG1 is a resource group in the subscription.

RG1 has a virtual network. The virtual network is named VNet1. The virtual network is in the same region as the subscription. The virtual network is in the same address space as the subscription.

What is the minimum number of users that can be assigned the role of Contributor for RG1?

Users who can modify the permissions for RG1:

User1 only

User1 and User2 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

Users who can create virtual networks in RG1:

User1 only

User1 and User2 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

Answer:

Users who can modify the permissions for RG1:

▼

User1 only

User1 and User2 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

Users who can create virtual networks in RG1:

▼

User1 only

User1 and User2 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

Explanation:

Users who can modify the permissions for RG1:

▼

User1 only

User1 and User2 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

Users who can create virtual networks in RG1:

▼

User1 only

User1 and User2 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

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

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

NEW QUESTION: 26

SQL1 is an Azure SQL Database. VM1 is an Azure VM. VM1 is connected to SQL1. VM1 IP is 10.0.0.1.

SQL1 is connected to VM1. SQL1 IP is 10.0.0.1.

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:

NEW QUESTION: 31

KeyVault1 is an Azure Key Vault. It is located in the East US region. It is connected to the VNET1 virtual network.

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

KeyVault1 is configured with Azure Disk Encryption. It is using the Key Vault to store the encryption keys. KeyVault1 is also configured with Azure Key Vault to store the encryption keys.

Save

Discard

Allow access from:

All networks

Selected networks

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

Virtual networks:

+ Add existing virtual networks

+ Add new virtual network

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

Firewall:

IPv4 ADDRESS OR CIDR

IPv4 address or CIDR

...

Exception:

Allow trusted Microsoft services to bypass this firewall?

Yes

No

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

KeyVault1 is configured with Azure Disk Encryption. It is using the Key Vault to store the encryption keys. KeyVault1 is also configured with Azure Key Vault to store the encryption keys.

❑-❑❑❑❑ 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❑❑❑❑.

Microsoft

Users who can create a security group named Contoso Sales:

Admin1 only

Admin1 and Admin2 only

Admin1 and Admin3 only

Admin1, Admin2, and Admin3

Microsoft

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

Admin1 only

Admin1 and Admin2 only

Admin1 and Admin3 only

Admin1, Admin2, and Admin3

Answer:

Users who can create a security group named Contoso Sales:

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

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

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

Explanation:

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 is a Microsoft Enterprise SaaS application. Azure AD is configured with the following settings. contoso.com is an App1 SaaS application. App1 is an Android SaaS application. App1 is an SaaS application. Azure AD is configured with the following settings?

- A. No
- B. Yes
- C. No
- D. Yes

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

NEW QUESTION: 35

Azure AD is configured with the following settings.

Name	Tier
GW1	Basic
GW2	Standard V2
GW3	WAF V2

URL rewrite rules SQL injection attacks. Which gateways should be configured to implement these rules?

Two gateways should be configured to implement these rules. Which gateways should be configured to implement these rules? (Select two.)

Answer Area

Implement URL rewrite: GW2 and GW3 only

Prevent SQL injection attacks: GW3 only

Microsoft

Answer:

Answer Area

Microsoft

Implement URL rewrite: GW2 and GW3 only

Prevent SQL injection attacks: GW3 only

Explanation:

Answer Area

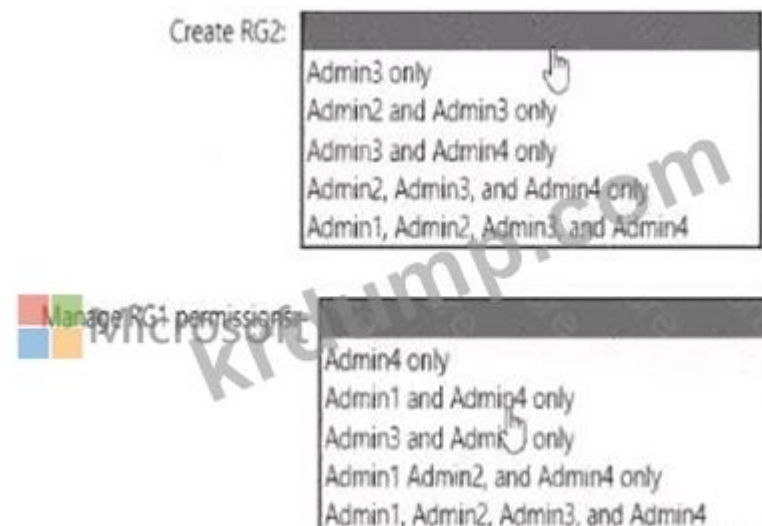
Microsoft

Implement URL rewrite: GW2 and GW3 only

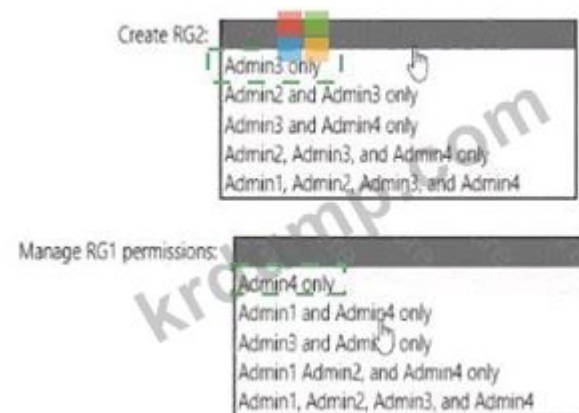
Prevent SQL injection attacks: GW3 only

NEW QUESTION: 36

RG2 is a resource group in a subscription. RG1 is a resource group in a subscription. Which gateways should be configured to implement these rules? (Select two.)

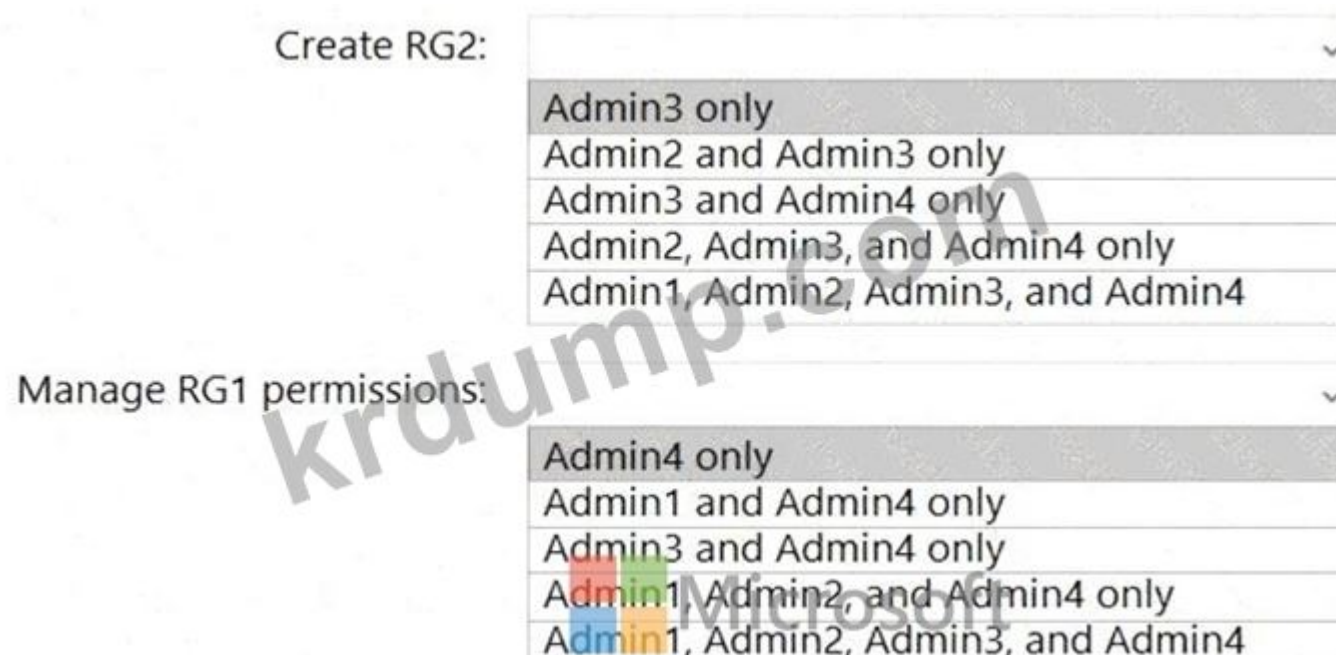


Answer:



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 101 101 101 101 JIT(Just-in-Time) VM 101 101 101 101.
JIT VM 101 101 101 101 101 101 PowerShell 101 101 101 101.
101 101 101? 101 101 101 101 101 101 101.
101: 101 101 101 101.

Answer Area

Microsoft

Permission that must be granted to users on VM:

Read
Update
View
Write

TCP port that must be allowed:

22
25
3389
5986

Answer:

Answer Area

Microsoft

Permission that must be granted to users on VM:

Read
Update
View
Write

TCP port that must be allowed:

22
25
3389
5986

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

101 101 Azure 101 101 101 101 101 101.

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 101 101 Key1 101 101 101 101 101 101 101.
Secret1 Key1 101 101.
101 101 101 101 101 101 101? 101 101 101 101 101 101 101.
101: 101 101 101 101.

You can restore the Secret1 backup to:

	▼
KV1 only	
KV1 and KV2 only	
KV1, KV2 and KV3 only	
KV1, KV2 and KV4 only	
KV1, KV2, KV3, KV4, and KV5	

You can restore the Key1 backup to:

	▼
KV1 only	
KV1 and KV2 only	
KV1, KV2 and KV3 only	
KV1, KV2 and KV4 only	
KV1, KV2, KV3, KV4, and KV5	

Answer:

You can restore the Secret1 backup to:

	▼
KV1 only	
KV1 and KV2 only	
KV1, KV2 and KV3 only	
KV1, KV2 and KV4 only	
KV1, KV2, KV3, KV4, and KV5	

You can restore the Key1 backup to:

	▼
KV1 only	
KV1 and KV2 only	
KV1, KV2 and KV3 only	
KV1, KV2 and KV4 only	
KV1, KV2, KV3, KV4, and KV5	

Explanation:

You can restore the Secret1 backup to:

▼

KV1 only

KV1 and KV2 only

KV1, KV2 and KV3 only

KV1, KV2 and KV4 only

KV1, KV2, KV3, KV4, and KV5

You can restore the Key1 backup to:

▼

KV1 only

KV1 and KV2 only

KV1, KV2 and KV3 only

KV1, KV2 and KV4 only

KV1, KV2, KV3, KV4, and KV5

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 .

Save

Microsoft

Stored access policies

Identifier	Start time	Expiry time	Permissions
Policy1			r ***

+

Add policy

Blob Azure .

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

1
2
4
7
15

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

1
2
4
7
15



Answer:

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

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

Explanation:

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

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

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

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

[illegible][illegible]

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

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

☐ ☐☐☐ ☐☐☐☐ ☐☐☐ ☐☐ ☐ ☐☐☐☐.

[illegible]

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□ □□□□ □□□□□.

□□□□□ □□ □□□ □□□□ □□□?

A. □□□□ □□

B. □□ □□ □□

C. □□□ □□□

D. □□ □□ □□ □□

Answer: ([SHOW ANSWER](#))

AZ-500-KR ☐☐ ☐☐☐ ☐☐☐☐☐ ☐☐ DumpTop ☐☐ ☐☐☐☐ ☐☐☐ AZ-500-KR ☐☐! DumpTop ☐ ☐☐ **AZ-500-KR** ☐☐ ☐☐☐ ☐☐☐☐☐☐, DumpTop AZ-500-KR ☐☐ ☐☐☐ ☐☐☐☐☐☐☐
☐☐☐☐ ☐☐☐☐☐☐☐. ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐ DumpTop AZ-500-KR ☐☐☐ ☐☐☐☐☐. <https://www.dumptop.com/Microsoft/AZ-500-KR-dump.html> (**520 Q&As Dumps**, **30%OFF Special Discount: KrDump**)

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 □□□ □□ □□□□□.

[illegible]

storage1 ☐ ☐☐☐ ☐ ☐☐☐ ☐☐☐☐ ☐☐☐

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 49

□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

Name	Type
VM1	Virtual machine
VNet1	Virtual network
AFW1	Azure firewall

VM100 00 00 Azure 000 0000 00000 0000 00000 AFW10 0000 000. 0000 00 000 00000 000.
000 0000 000?

- 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 00 00 0000 000000 000 000 0 000 00000.

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

You are configuring a virtual machine (VM) named VM1 in a virtual machine monitor (VMM) named VMM1. You are configuring VM1 to access a file named File1 by using a private IP address.

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

You are configuring a virtual machine (VM) named VM1 in a virtual machine monitor (VMM) named VMM1. You are configuring VM1 to access a file named File1 by using a private IP address.

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](#))

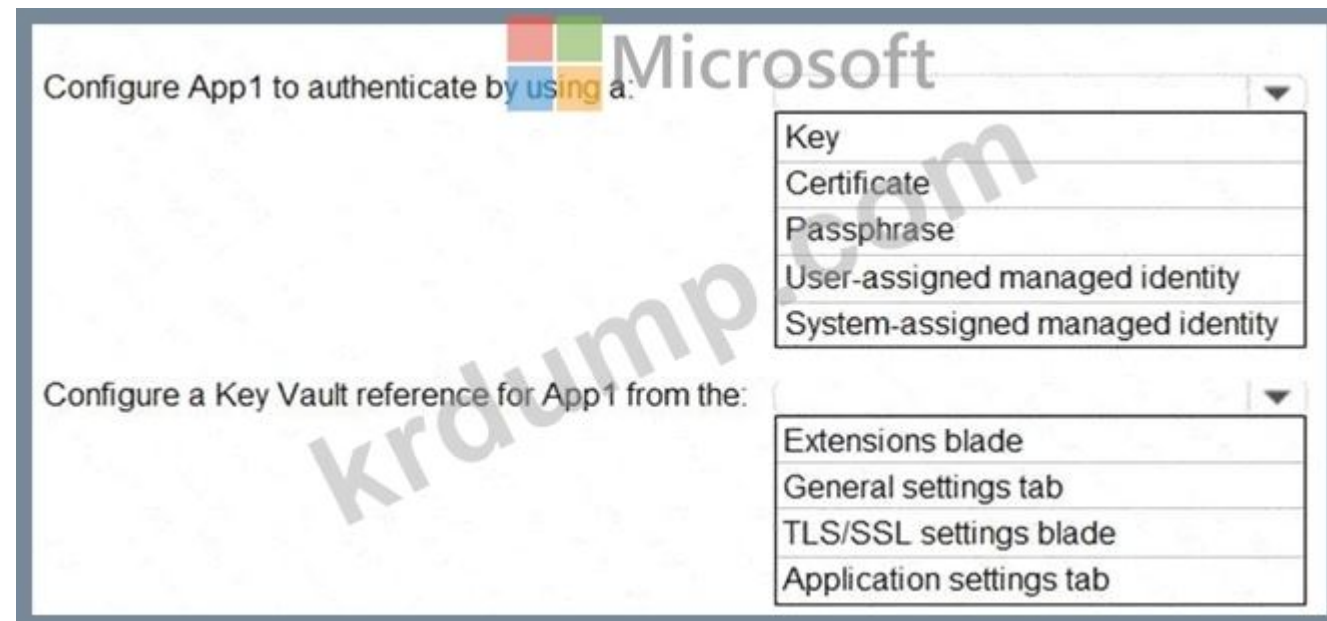
NEW QUESTION: 56

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:

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

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□□□□.

Configure role-based access control (RBAC) role assignments by using:

	▼
Azure Blueprints	
Azure Policy	
Azure Security Center	

Prevent the modification of permissions to RG1 by using:

A resource lock	
A role-based access control (RBAC) role assignment at the resource group level	
Azure Blueprint assignments in locking mode	

Answer:

Configure role-based access control (RBAC) role assignments by using:

- Azure Blueprints
- Azure Policy
- Azure Security Center

Prevent the modification of permissions to RG1 by using:

- A resource lock
- A role-based access control (RBAC) role assignment at the resource group level
- Azure Blueprint assignments in locking mode

Explanation:

Configure role-based access control (RBAC) role assignments by using:

- Azure Blueprints
- Azure Policy
- Azure Security Center

Prevent the modification of permissions to RG1 by using:

- A resource lock
- A role-based access control (RBAC) role assignment at the resource group level
- Azure Blueprint assignments in locking mode

NEW QUESTION: 58

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

[illegible]

□□□ □□□□ □□□?

- A. Key Vault** ☐☐
- B. Azure** ☐☐
- C. Azure Purview**

D. Azure

Answer: B (LEAVE A REPLY)

NEW QUESTION: 59

Microsoft Antimalware is installed on all Windows 10 devices in the Contoso network. The security team wants to ensure that the Antimalware service is always running on all devices. The security team wants to create a custom policy definition that has effect set to: Append, Deny, and DeployIfNotExists. The security team wants to create a policy assignment and modify: The Create a Managed Identify setting, The exclusion settings, and The scope.

Create a custom policy definition that has effect set to:

▼

Append
Deny
DeployIfNotExists

Create a policy assignment and modify:

▼

The Create a Managed Identify setting
The exclusion settings
The scope

Answer:

Create a custom policy definition that has effect set to:

▼

Append
Deny
DeployIfNotExists

Create a policy assignment and modify:

▼

The Create a Managed Identify setting
The exclusion settings
The scope

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

Contoso is planning to migrate its applications to Azure. The migration plan includes the following requirements:

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 is a virtual network in the Central US region. It is currently in the RG2 resource group.

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 Area

Resource group:

Subnet:

Answer:

The screenshot shows the 'Resource group' and 'Subnet' dropdown menus in the Azure portal. The 'Resource group' dropdown is open, showing options RG1, RG2, and RG3. The 'Subnet' dropdown is also open, showing options like 'AzureFirewallSubnet only', 'AzureFirewallSubnet only', 'AzureFirewall or AzureFirewallSubnet only', 'AzureFirewall, AzureFirewallSubnet, or Subnet2 only', and 'AzureFirewall, AzureFirewallSubnet, Subnet1, or Subnet2'.

Explanation:

Answer Area

Microsoft
Resource group: RG2
Subnet: AzureFirewallSubnet only

NEW QUESTION: 61

□ □ □ □ □

□□ 2

VNET01-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

AZ-500-KR ☐☐ ☐☐☐ ☐☐☐☐☐ ☐☐ DumpTop ☐☐ ☐☐☐☐ ☐☐☐ AZ-500-KR ☐☐! DumpTop ☐ ☐☐ **AZ-500-KR** ☐☐ ☐☐☐ ☐☐☐☐☐☐, DumpTop AZ-500-KR ☐☐ ☐☐☐ ☐☐☐☐☐☐☐ ☐ ☐☐☐ ☐☐☐☐☐☐☐. ☐☐☐☐ ☐☐☐ ☐☐☐☐ ☐☐ DumpTop AZ-500-KR ☐☐☐ ☐☐☐☐☐. <https://www.dumptop.com/Microsoft/AZ-500-KR-dump.html> (520 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

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☐☐☐☐☐.

Delegate permissions for ContosoKey1: Microsoft ▼

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

Configure network access to ContosoKey1: ▼

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

Answer:

Delegate permissions for ContosoKey1: Microsoft ▼

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

Configure network access to ContosoKey1: ▼

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

Explanation:

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:

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

Explanation:

Variable1:	Microsoft ▼
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:	Microsoft ▼
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	

Reference:

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

NEW QUESTION: 67

Azure   MG1  RG1  VM1                Azure    

Name	Scoped to
Role1	MG1
Role2	RG1

Role1□ □□ □□□ □□ □□ □□□ □□□□□.


```

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

```

The permissions are assigned to the following role definition:

```

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

```

Which of the following statements are true?

Name	Role
User1	Role1
User2	Role1, Role2
User3	Role2

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

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

Answer:

Statements	Yes	No
User1 can delete VM1.	☒	☐
User2 can delete VM1.	☐	☒
User3 can delete VM1.	☒	☐

Explanation:

Statements	Yes	No
User1 can delete VM1.	☐	☒
User2 can delete VM1.	☐	☒
User3 can delete VM1.	☒	☐

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 share1 Azure

☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐.

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

[illegible]

Actions

Answer Area

Create a private link to storage1.

Enable Active Directory Domain Services (AD DS) authentication on storage1.

Implement Azure AD Connect.

Create a service endpoint to storage1.

Assign share-level permissions for share1.

Answer:

Actions

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

Implement Azure AD Connect.

Enable Active Directory Domain Services (AD DS) authentication on storage1.

Assign share-level permissions for share1.

Explanation:

Implement Azure AD Connect.

Enable Active Directory Domain Services (AD DS) authentication on storage1.

Assign share-level permissions for share1.

Reference:

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

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

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

 You can add VNet1 to Group2.

 You can add VNet2 to Group1.

 You can add Subnet3 to Group3.

Answer Area

Statements

Microsoft

Yes

No

You can add VNet1 to Group2.

☐
☐

You can add VNet2 to Group1.

☐
☐

You can add Subnet3 to Group3.

☐
☐

Answer:

Answer Area

Statements

Microsoft

Yes

No

You can add VNet1 to Group2.

☒
☐

You can add VNet2 to Group1.

☐
☒

You can add Subnet3 to Group3.

☒
☐

Explanation:

Answer Area

Statements

Microsoft

Yes

No

You can add VNet1 to Group2.

☒
☐

You can add VNet2 to Group1.

☐
☒

You can add Subnet3 to Group3.

☒
☐

NEW QUESTION: 71

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

 KeyVault1 and KeyVault2 are in the same region and in the same Azure Active Directory (Azure AD) tenant, but they are in different subscriptions.

 KeyVault2 and KeyVault3 are in the same region and in the same Azure Active Directory (Azure AD) tenant, but they are in different subscriptions.

 KeyVault1 and KeyVault3 are in the same region and in the same Azure Active Directory (Azure AD) tenant, but they are in different subscriptions.

 KeyVault1, KeyVault2, and KeyVault3 are in the same region and in the same Azure Active Directory (Azure AD) tenant, but they are in different subscriptions.

- A. KeyVault1
- B. KeyVault2 and KeyVault3
- C. KeyVault1 and KeyVault3
- D. KeyVault1, KeyVault2, and 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 databases are in the same Azure region. The databases are named SQL1, SQL2, SQL3, and SQL4. SQL1 is the only database in the same region as the other three databases. What is the most likely reason for this?

- A. Azure Advanced Threat Protection(ATP) is enabled for SQL1.
- B. SQL1 is the only database in the same region as the other three databases.
- C. Azure Monitor SQL Health Check is enabled for SQL1.
- D. Azure Sentinel is enabled for SQL1.

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

NEW QUESTION: 73

SQLDB1 is a Microsoft SQL Server database. The database is in the same region as the other three databases. What is the most likely reason for this?

Actions

From the Azure portal, create an Azure AD administrator for LitwareSQLServer1.

In SQLDB1, create contained database users.

Connect to SQLDB1 by using Microsoft SQL Server Management Studio (SSMS).

In Azure AD, create a system-assigned managed identity.

In Azure AD, create a user-assigned managed identity.

Answer Area

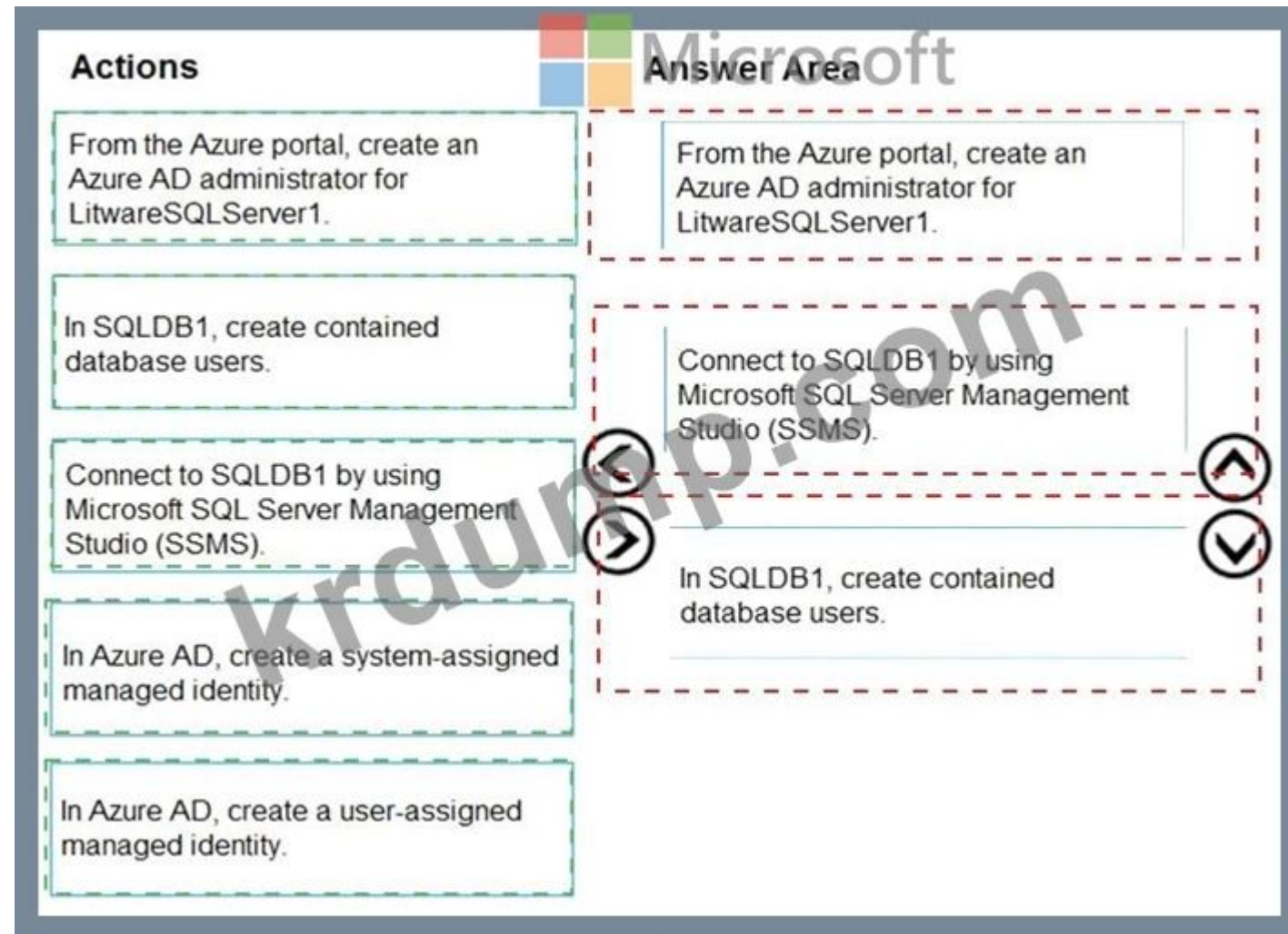
←

→

↑

↓

Answer:



Explanation:

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

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

NEW QUESTION: 74

MG1 is a resource group, and Sub1 is a subscription. Sub1 is a subscription. Sub1 is a subscription. Sub1 is a subscription.

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

Sub1 is a subscription. Microsoft Defender for Servers Plan1 is Microsoft Defender for Key Vault. Sub1 is a subscription.

Azure Defender for Servers Plan 1 is Microsoft Defender for Key Vault. Sub1 is a subscription. Sub1 is a subscription.

Sub1 is a subscription. Sub1 is a subscription.

Answer Area

Defender for Servers Plan 1:

- Sub1 only
- Sub1 and RG1 only
- Sub1 and VM1 only
- Sub1 and MG1 only
- Sub1 and Workspace1 only
- Sub1, MG1, and VM1 only

Defender for Key Vault:

- Sub1 only
- Sub1 and RG1 only
- Sub1 and Vault1 only
- Sub1 and MG1 only
- Sub1 and Workspace1 only
- Sub1, MG1, RG1, and Vault1 only



Answer:
Answer Area

Defender for Servers Plan 1:

- Sub1 only
- Sub1 and RG1 only
- Sub1 and VM1 only
- Sub1 and MG1 only
- Sub1 and Workspace1 only
- Sub1, MG1, and VM1 only

Defender for Key Vault:

- Sub1 only
- Sub1 and RG1 only
- Sub1 and Vault1 only
- Sub1 and MG1 only
- Sub1 and Workspace1 only
- Sub1, MG1, RG1, and Vault1 only



Explanation:

Defender for Servers Plan 1: Sub1, MG1, RG1, and VM1 only

Defender for Key Vault: Sub1 only

NEW QUESTION: 75

WebApp1 is an Azure App Services application. Vault1 is an Azure Key Vault. Cert1, Cert2, Cert3, and Cert4 are certificates in the Azure Key Vault. Cert1 and Cert2 are RSA certificates. Cert3 and Cert4 are RSA certificates. Cert1 and Cert2 are 2048-bit certificates. Cert3 and Cert4 are 4096-bit certificates. Cert1 and Cert2 are used for TLS. Cert3 and Cert4 are used for TLS. Cert1 and Cert2 are used for TLS. Cert3 and Cert4 are used for TLS.

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 is configured to use TLS. Cert1 and Cert2 are used for TLS. Cert3 and Cert4 are used for TLS.

WebApp1 is configured to use TLS. Cert1 and Cert2 are used for TLS. Cert3 and Cert4 are used for TLS.

Vault1 is configured to use TLS. Cert1 and Cert2 are used for TLS. Cert3 and Cert4 are used for TLS.

A. Cert1, Cert2, Cert3 and Cert4

B. Cert1 and Cert2

C. Cert1 and Cert3

D. Cert3 and Cert4

Answer: B (LEAVE A REPLY)

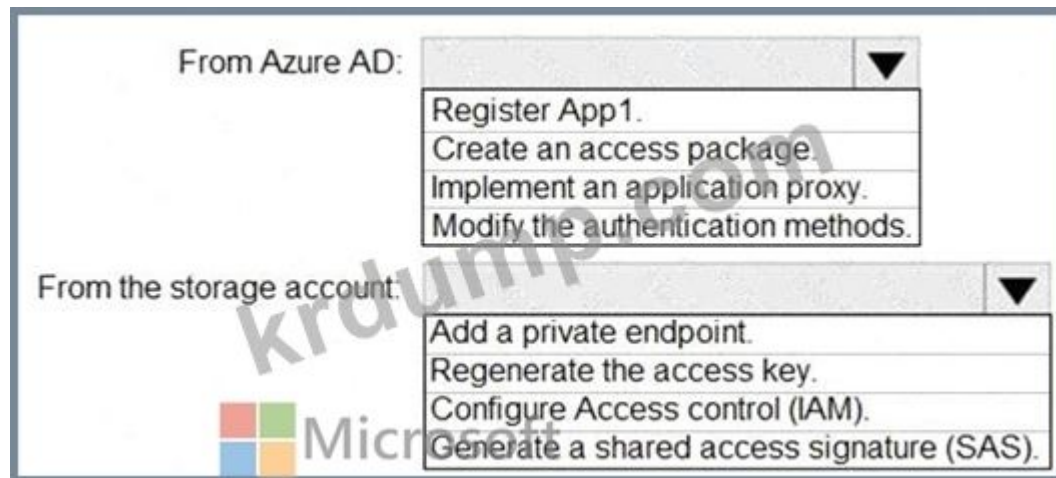
NEW QUESTION: 76

container1 is an Azure Container App. Blob is an Azure Storage blob. App1 is an Azure App Service. Azure Storage is an Azure Storage account. Azure Active Directory (Azure AD) is an Azure Active Directory.

Azure Active Directory (Azure AD) is configured to use TLS. Cert1 and Cert2 are used for TLS. Cert3 and Cert4 are used for TLS.

What is the correct configuration for container1?

Options: 1. 1. 1. 1.



Answer:

Which of the following risk events are associated with the High risk level? (Select all that apply.)

Impossible travel to atypical locations.

Users with leaked credentials.

Sign ins from IP addresses with suspicious activity.

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

Answer:

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

Explanation:

Medium

High

Medium

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

NEW QUESTION: 78

Which of the following operating systems are supported by Azure Security Center?

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

Azure Security Center supports which of the following operating systems?

Which of the following operating systems are supported by Azure Security Center?

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

Log Analytics supports which of the following operating systems?

- 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 is an Azure VM. You need to configure the VM's network security group (NSG) to allow inbound traffic from the Internet to the VM.

VM1 is an Azure VM. You need to configure the VM's network security group (NSG) to allow inbound traffic from the Internet to the VM. Which of the following is the correct configuration for the NSG?

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

VM1 is an Azure VM. You need to configure the VM's network security group (NSG) to allow inbound traffic from the Internet to the VM. Which of the following is the correct configuration for the NSG?

* Port: 3389, 22

* Port: 3389

* IP: 0.0.0.0

JIT is a feature that allows you to enable Just-in-Time (JIT) VM access. JIT is a feature that allows you to enable Just-in-Time (JIT) VM access. JIT is a feature that allows you to enable Just-in-Time (JIT) VM access.

JIT is a feature that allows you to enable Just-in-Time (JIT) VM access. JIT is a feature that allows you to enable Just-in-Time (JIT) VM access. JIT is a feature that allows you to enable Just-in-Time (JIT) VM access.

JIT is a feature that allows you to enable Just-in-Time (JIT) VM access. JIT is a feature that allows you to enable Just-in-Time (JIT) VM access. JIT is a feature that allows you to enable Just-in-Time (JIT) VM access.

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

Answer Area

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

Answer Area

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

 Microsoft

□□□□□ 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 is a storage administrator. storage1 is an Azure Storage account. storage1 contains the following resources.

Name	Type
container1	Container
folder1	File share
table1	Table

User1 is a storage administrator. storage1 is an Azure Storage account. storage1 contains the following resources.

* container1 Blob storage

* folder1 File share

* table1 Table storage

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:

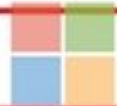
No, Yes, No

NEW QUESTION: 84

AKS1 is an Azure Kubernetes Service (AKS) cluster.

AKS1 contains the following resources. AKS1 is configured to use the following authentication method.

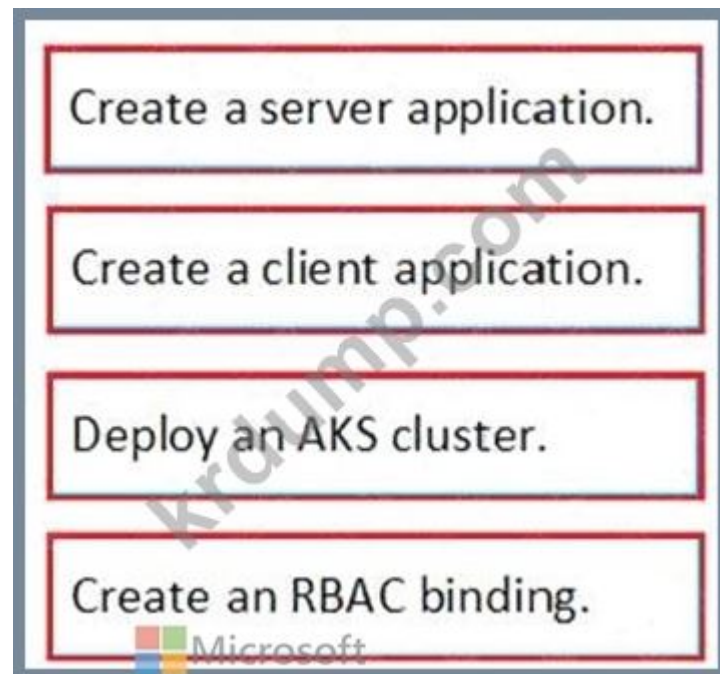
AKS1: AKS1 is configured to use the following authentication method.

Actions	Answer Area
Deploy an AKS cluster.	
Create a client application.	
Create a server application.	 Microsoft
Create an RBAC binding.	
Create a custom RBAC role.	

Answer:

Actions	Answer Area
Deploy an AKS cluster.	Create a server application.
Create a client application.	Create a client application.
Create a server application.	Deploy an AKS cluster.
Create an RBAC binding.	Create an RBAC binding.
Create a custom RBAC role.	

Explanation:



Scenario: Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.

Litewire plans to deploy AKS1, which is a managed AKS (Azure Kubernetes Services) cluster.

Step 1: Create a server application

To provide Azure AD authentication for an AKS cluster, two Azure AD applications are created. The first application is a server component that provides user authentication.

Step 2: Create a client application

The second application is a client component that is used when you are 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 Subnet0.
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 NSG) Azure

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

Azure



NSG1 ☐ NSG2 ☐ ☐☐ ☐☐☐ ☐☐ ☐☐?

B. NSG1□ □□□□ □□ □□□ □□□□□□.

D. NSG2 ☐ ☐☐☐☐ ☐☐ ☐☐☐☐☐

Answer: D (LEAVE A REPLY)

NEW QUESTION: 86

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

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

[illegible]

□□□□ □□□ □□□□□?

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 is not an Active Directory. It is an Azure Active Directory(Azure AD) cloud service.

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. $\square\square\square 2$

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 000 00 000 0000 000.

□□ 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

Resource Providers	Answer Area
Microsoft.Compute	
Microsoft.Network	
Microsoft.Security	
Microsoft.Solutions	

Role1:

Role2:

Microsoft

Answer:

Resource Providers	Answer Area
Microsoft.Compute	
Microsoft.Network	
Microsoft.Security	
Microsoft.Solutions	

Role1: Microsoft.Network

Role2: Microsoft.Network

Microsoft

Explanation:

Resource Providers

Microsoft.Compute

Microsoft.Network

Microsoft.Security

Microsoft.Solutions



Answer Area

Role1: Microsoft.Network

Role2: Microsoft.Network

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>

AZ-500-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ AZ-500-KR □□! DumpTop □ □□ **AZ-500-KR** □□ □□□ □□□□□□, DumpTop AZ-500-KR □□ □□□ □□□□□□□ □ □□□ □□□□□□□□. □□□□ □□□ □□□□ □□ DumpTop AZ-500-KR □□□ □□□□□. <https://www.dumptop.com/Microsoft/AZ-500-KR-dump.html> (520 Q&As Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 92

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

□□ □□□ □□ □□ □□ □□□□ □□□ □□□□□.

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

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

□□: □□ 1□□ 1□□□□.

Settings | Continuous export

Visual Studio Enterprise Subscription

Microsoft

Save

Continuous export

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

Event hub

Log Analytics workspace

Export enabled

OnOff

Exported data types

☐ Security recommendations

No selected recommendation

☒ Secure score ⓘ

Overall score.Control score

Controls

All controls selected

☐ Security alerts

No selected severities

☐ Regulatory compliance

No selected standards

Export frequency

☒ Streaming updates ⓘ

☐ Snapshots (Preview) ⓘ

Answer:



Settings | Continuous export ...

Visual Studio Enterprise Subscription



Save



Continuous export

Configure streaming export setting of Defender for Cloud data to multiple export targets.

Exporting Defender for Cloud's data also enables you to use experiences such as integration with 3rd-party SIEM and Azure Data Explorer.

[Learn More >](#)

Event hub

Log Analytics workspace

Export enabled

On

Off

Exported data types

☐ Security recommendations	No selected recommendation
☒ Secure score ⓘ	Overall score,Control score
Controls	All controls selected
☐ Security alerts	No selected severities
☐ Regulatory compliance	No selected standards

Export frequency

☒ Streaming updates ⓘ
☐ Snapshots (Preview) ⓘ

Explanation:



NEW QUESTION: 93

Microsoft Enterprise PIM(Privileged Identity Management)은 Azure AD에 있는 User1은 Azure AD에 있는 2개의 그룹에 속해 있습니다. 이 그룹은 Azure AD에 있는 어떤 리소스에 접근할 수 있는 권한이 있습니까?

- 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□□□□.

81cb93e71e7e401095f37bb5841417dd

Key version

Save Discard changes Download public key

Key type	RSA
RSA key size	2048
Created	4/24/2023, 7:39:34 PM
Updated	4/24/2023, 7:39:34 PM
Key Identifier	https://vsk230424.vault.azure.net/keys/Key2/81cb93e71e7e401095f37bb5841417dd

Set expiration date

Expiration date: 01/01/2030 6:49:00 PM
 (UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague

Enabled: Yes

Tags: 0 tags

Permitted operations

- ☐ Encrypt
- ☐ Decrypt
- ☐ Sign
- ☐ Verify
- ☒ Wrap Key
- ☒ Unwrap Key

Answer:

Answer Area

81cb93e71e7e401095f37bb5841417dd

Key version

Save Discard changes Download public key

Key type RSA

RSA key size 2048

Created 4/24/2023, 7:39:34 PM

Updated 4/24/2023, 7:39:34 PM

Key Identifier <https://vk230424.vault.azure.net/keys/Key/81cb93e71e7e401095f37bb5841417dd>

Set expiration date ☒

Expiration date 01/01/2030 6:49:00 PM

(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague

Enabled ☒ No

Tags

Permitted operations

☐ Encrypt

☐ Decrypt

☐ Sign

☐ Verify

☒ Wrap Key

☒ Unwrap Key

Explanation:

81cb93e71e7e401095f37bb5841417dd

Key version

Save Discard changes Download public key

Key type RSA

RSA key size 2048

Created 4/24/2023, 7:39:34 PM

Updated 4/24/2023, 7:39:34 PM

Key Identifier <https://vk230424.vault.azure.net/keys/Key/81cb93e71e7e401095f37bb5841417dd>

Set expiration date ☒

Expiration date 01/01/2030 6:49:00 PM

(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague

Enabled ☒ No

Tags

Permitted operations

☐ Encrypt

☐ Decrypt

☐ Sign

☐ Verify

☒ Wrap Key

☒ Unwrap Key

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□□□□.

Group5:

Microsoft

User1 only

User1 and Group1 only

User1, Group1, and Managed1 only

User1, Group1, Managed1, and App1

Group6:

Microsoft

User1 only

User1 and Group1 only

User1, Group1, and Managed1 only

User1, Group1, Managed1, and App1

Answer:

Group5:  ▼

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

Group6: ▼

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

Explanation:

Graphi cal user interface, text, application Description automatically generated

Group5:  Microsoft ▼

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

Group6: ▼

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

NEW QUESTION: 98

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

Enable and Target Configure

Authentication binding

Select the default protection level for all certificate bindings. To override the default, create special rules.

Protection Level  Single-factor authentication Multi-factor authentication

[Add rule](#)

Rule type	Identifier	Protection Level	
Certificate issuer	CN=ContosoCA, DC=contoso, DC=com	Single-factor authentication	...

Username binding

Select user attribute to create binding. The first certificate field has the highest priority in the username bind

Certificate field	User attribute	
1 PrincipalName	userPrincipalName	...
2 RFC822Name	userPrincipalName	...
3 SubjectKeyIdentifier	certificateUserIds	...
4 SHA1PublicKey	Select user attribute	...

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

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.	☒	☐

Explanation:

Answer Area

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

NEW QUESTION: 99

SQL1 is an Azure SQL database. SQL1 is configured with Always Encrypted. SQL1 is configured with Always Encrypted. SQL1 is configured with Always Encrypted. SQL1 is configured with Always Encrypted.

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

SQL1 is configured with Always Encrypted. SQL1 is configured with Always Encrypted. SQL1 is configured with Always Encrypted. SQL1 is configured with Always Encrypted.

SQL1 is configured with Always Encrypted. SQL1 is configured with Always Encrypted. SQL1 is configured with Always Encrypted. SQL1 is configured with Always Encrypted.

SQL1 is configured with Always Encrypted. SQL1 is configured with Always Encrypted. SQL1 is configured with Always Encrypted. SQL1 is configured with 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 00 00 0000 000 000000 0000 000. 0000 00 00 000 0000 000.

* VNet1 □ □ □ □ □ □ □ □ □ □ Microsoft □ □ □ □ □ □ □ □ □ □ storage1, storage2 □ Azure AD □ □ □ □ □ □ □ □ □ □.

* VNet2 □□□□ □□□□ □□ □□□ Microsoft □□ □□□□□ □□□□ storage1□ KeyVault1□ □□□□□ □□□.

```
* 00 000 VNet1 0 VNet2 0 000 00 Microsoft 00 000000 0000 0000.
```

[illegible]

□□: □□ 1□□ 1□□□□.

Answer Area

VNet1: 

- 1
- 2
- 3
- 5
- 10

VNet2: 

- 1
- 2
- 3
- 6
- 15

 Microsoft

Answer:

Answer Area

Microsoft

VNet1: 1

VNet2: 2

Explanation:

Answer Area

Microsoft

VNet1: 1

VNet2: 2

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 Area

App1:

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

App2:

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



Answer:



The screenshot shows the Windows Security Center interface. The 'App1' dropdown menu is open, displaying a list of users: 'User1 only', 'User1 and User2 only', 'User1 and User3 only', 'User1, User2, and User3 only', and 'User1, User2, User3, and User4'. The 'App2' dropdown menu is also open, displaying a list of users: 'User1 only', 'User1 and User2 only', 'User1 and User4 only', 'User1, User2, and User4 only', and 'User1, User2, User3, and User4'. The 'User1 and User2 only' option is selected for both App1 and App2.

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

Rules

Rule5
Rule4
Rule3
Rule2
Rule1

Answer Area



Answer:

Rules

Rule5
Rule4
Rule3
Rule2
Rule1

Answer Area

Rule1
Rule2
Rule3
Rule4
Rule5

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

10000 00 0000 0000 Azure 0000 00000. 00 00 00000 Azure 0000 000000 00000.

00000 Azure 0000 000000 00000 00000.

00 00 0000 00000 0000.

* 30 00 00 0000 0000 00000 000000.

* Windows Server 20160 00000 00 0000 00 00000 000000.

Azure Monitor00 0000 00000 0000? 00 00000 0000 00 0000 0000 00 0000 0000 00000. 0 00 0000 0 0, 00 0 00 00 00000 00 0 00000. 00000 0000

0 0000 00 0000 0000 0000 0000000 0 00 00000.

□□: □□ 1□□ 1□□□□.

Settings

Answer Area

Activity log

Logs

Metrics

Service Health

Identify the user who deleted a virtual machine three weeks ago:

Query the security events of a virtual machine that runs
Windows Server 2016:



Answer:

Settings

Answer Area

Activity log

Logs

Metrics

Service Health

Identify the user who deleted a virtual machine three weeks ago:

Query the security events of a virtual machine that runs
Windows Server 2016:

Activity log

Logs

Explanation:



Identify the user who deleted a virtual machine three weeks ago:

Activity log

Query the security events of a virtual machine that runs
Windows Server 2016:

Logs

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 is a dedicated network path between Azure and on-premises networks. It provides a high-speed, low-latency connection that is not shared with other users. ExpressRoute is available in most regions and is supported by a variety of network providers. To configure ExpressRoute, you must first create an ExpressRoute circuit. This circuit is then connected to your on-premises network and to the Azure network. The circuit is then used to route traffic between your on-premises network and Azure resources.



Answer:



Explanation:

Answer Area

Microsoft

Layer 2 encryption: ER3 and ER4 only

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

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

Operating systems:

Microsoft

SLES only

Windows Server only

SLES and Windows Server

Platforms:

Azure virtual machines only

Azure virtual machines and Hyper-V virtual machines only

Azure Arc-enabled servers and Azure virtual machines only

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

These are the selections for Platforms.

Answer:

Platforms:

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

These are the selections for Platforms.

- 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 Area

Answer:

Answer Area

Users who can onboard Azure AD Identity Protection: ☐ User1 only ☐ User1 and User2 only ☐ User1, User 2, and User3 only ☐ User1, User 2, User3, and User 4 only

Users who can remediate users and configure policies: ☐ User1 and User2 only ☐ User1 and User3 only ☐ User1, User 2, and User3 only ☐ User1, User 2, User3, and User 4

Explanation:

Users who can onboard Azure AD Identity Protection:

▼
User1 only
User1 and User2 only
User1, User2, and User3 only
User1, User2, User3, and User4 only

Users who can remediate users and configure policies:

▼
User1 and User2 only
User1 and User3 only
User1, User2, and User3 only
User1, User2, User3, and User4

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 is an Azure API Management service. ContosoAPI1 is configured to use an Azure API service.

ContosoAPI1 is configured to use an Azure API service.

Azure Portal is used to configure the API service.

- A. The API service is configured to use an Azure API service.
- B. The API service is configured to use an Azure API service.
- C. The API service is configured to use an Azure API service.
- D. API service is configured to use an Azure API service.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 112

ContosoAPI1 is an Azure API Management service. ContosoAPI1 is configured to use an Azure API service.

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	20.224.219.212

ContosoAPI1 is an Azure API Management service. ContosoAPI1 is configured to use an Azure API service.

Allow access from

☐ All networks ☒ Selected networks

Configure network security for your Cosmos DB account. Learn more

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

VM1 can access cosmos1 over the internet.

Yes

No

VM2 can access cosmos1 over the internet.

VM3 can access cosmos1 over the internet.

☒☐☐☐☐☒

Explanation:

Yes, Yes, No

NEW QUESTION: 113

Group1 is a group in Azure Active Directory(Azure AD). Group1 is assigned the role of Group1. What is the role of Group1?

A. Group1 is assigned the role of Group1.

B. Microsoft Authenticator is assigned the role of Group1.

C. Group1 is assigned the role of Group1.

D. Group1 is assigned the role of Group1.

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

NEW QUESTION: 114

Azure Sentinel is a cloud-based security management and analytics solution.

Microsoft Sentinel is a cloud-based security management and analytics solution.

It is a cloud-based security management and analytics solution.

* Rule 1: CEF(Common Event Format) is a syslog format, IP address, URL, and other data.

* Rule 2: Microsoft Sentinel is a cloud-based security management and analytics solution.

It is a cloud-based security management and analytics solution.

Rule: Rule 1 is a rule.



Answer:

Answer Area



Microsoft

Rule1: Threat intelligence
Fusion
Machine learning (ML) behavioral analytics
Microsoft Security
Threat intelligence

Rule2: Machine learning (ML) behavioral analytics
Fusion
Machine learning (ML) behavioral analytics
Microsoft Security
Threat intelligence

Explanation:

Answer Area

Microsoft

Rule1: Threat intelligence

Rule2: Machine learning (ML) behavioral analytics

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

[illegible]

□□: □□ 1□□ 1□□□□.

Components	Answer Area
A data connector for Security Center	Enable alert notifications from Security Center: Component
A data connector for the firewall software	Create an incident: Component
A playbook	Initiate a script to configure the firewall rule: Component
A rule	
A Security Events connector	
A workbook	

Answer:

Components

- A data connector for Security Center
- A data connector for the firewall software
- A playbook
- A rule
- A Security Events connector
- A workbook

Answer Area

Enable alert notifications from Security Center: A data connector for Security Center

Create an incident: A rule

Initiate a script to configure the firewall rule: A playbook



Explanation:

Enable alert notifications from Security Center: A data connector for Security Center

Create an incident: A rule

Initiate a script to configure the firewall rule: A playbook



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

Microsoft Authenticator (.)

Enable and Target Configure

Enable ☒

Include Exclude

Target ☒ All users ☐ Select groups

Add groups

Name	Type	Registration	Authentication mode
Group1	Group	Optional	Passwordless

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

Enable and Target

Configure

Microsoft

Note: Users must be included as part of the Microsoft Authenticator targeted groups under the 'Enable and Target' tab.

GENERAL

Allow use of Microsoft Authenticator OTP Yes No

Require number matching for push notifications

Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time after the preview. [Learn more](#)

Status Enabled

Target Include Exclude

☐ All users

☒ Select group

[Add selected group](#)

Include target

Group2

□□: □□ 1□□ 1□□□□.

Answer Area

Statements	Yes	No
User1 is required to use number matching during sign-in.	☐	☐
User2 is required to use number matching during sign-in.	☐	☐
User3 is required to use number matching during sign-in.	☐	☐

Answer:

Answer Area

Statements	Yes	No
User1 is required to use number matching during sign-in.	☐	☒
User2 is required to use number matching during sign-in.	☐	☒
User3 is required to use number matching during sign-in.	☒	☐

Explanation:

Answer Area

Statements	Yes	No
User1 is required to use number matching during sign-in.	☐	☒
User2 is required to use number matching during sign-in.	☐	☒
User3 is required to use number matching during sign-in.	☒	☐

NEW QUESTION: 120

Which of the following are supported by Microsoft Defender for Cloud?

* AWS

* Azure (AWS)

* Azure (GCP)

Microsoft Defender for Cloud is a cloud-native security solution.

It provides a unified view of your cloud environment and helps you identify and respond to threats. It is available for Azure, AWS, and GCP.

It is available for free.

Answer Area

Containers: Azure, AWS, and GCP
Azure only
Azure and AWS only
Azure and GCP only
Azure, AWS, and GCP

Storage: Azure only
Azure only
Azure and AWS only
Azure and GCP only
Azure, AWS, and GCP

Answer:

Answer Area

Containers: Azure, AWS, and GCP
Azure only
Azure and AWS only
Azure and GCP only
Azure, AWS, and GCP

Storage: Azure only
Azure only
Azure and AWS only
Azure and GCP only
Azure, AWS, and GCP

Explanation:

Answer Area

Containers: Azure, AWS, and GCP

Storage: Azure only

NEW QUESTION: 121

Two Azure virtual networks are configured as follows:

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

What is the result of this configuration?

Answer Area

Statements	Yes	No
You can associate RT1 with Subnet3.	☐	☐
You can delete RT1.	☐	☐
When you attempted ping VM2 from VM1 traffic is routed to 172.16.10.10.	☐	☐

Answer:

Answer Area

Statements	Yes	No
You can associate RT1 with Subnet3.	☒	☐
You can delete RT1.	☐	☒
When you attempt to ping VM2 from VM1, traffic is routed to 172.16.10.10.	☐	☒

Explanation:

Answer Area

Statements

You can associate RT1 with Subnet3. ☒ Yes ☐ No

You can delete RT1. ☐ Yes ☒ No

When you attempt to ping VM2 from VM1, traffic is routed to 172.16.10.10. ☐ Yes ☒ No

AZ-500-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ AZ-500-KR □□! DumpTop □ □□ **AZ-500-KR** □□ □□□ □□□□□□, DumpTop AZ-500-KR □□ □□□ □□□□□□□
□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop AZ-500-KR □□□ □□□□□. <https://www.dumptop.com/Microsoft/AZ-500-KR-dump.html> (**520 Q&As Dumps**, **30%OFF Special Discount: KrDump**)

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'
            negationCondition: true
            matchValues: [
              '10.10.10.0/24'
            ]
          }
        ]
      }
    ]
    policySettings: {
      requestBodyCheck: true
      maxRequestBodySizeInKb: 128
      state: 'Enabled'
      mode: 'Detection'
    }
    managedRules: {
      managedRuleSets: [
        {
          ruleSetType: 'OWASP'
          ruleSetVersion: '3.2'
        }
      ]
    }
  }
}

```


Which two statements are true?
Select two.

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

A company has an Active Directory forest (AD DS) with a domain controller named DC1. User1 is a member of the domain. The company has a Microsoft Entra ID tenant. User1 is a member of the tenant. Which two statements are true?

1. 1. 1. Azure Files 1. 1. Azure 1. 1. 1.
 storage1 storage2 1. 1. 1. SMB 1. 1. 1. 1. 1. 1. 1. 1.
 Share! 1. 1. 1. 1. 1. 1. 1. 1. 1.

Security

Protocol settings

Azure Files exposes settings that let you toggle the SMB protocol to be more compatible or more secure, depending on your organization's requirements. Restricting these settings may prevent some clients from being able to connect. [Learn more](#)

Profile

Custom

SMB protocol versions

- ☐ SMB 2.1
- ☐ SMB 3.0
- ☒ SMB 3.1.1

Authentication mechanisms

- ☒ NTLM v2
- ☒ Kerberos

SMB channel encryption

- ☐ None
- ☒ AES-128-CCM
- ☒ AES-128-GCM
- ☒ AES-256-GCM

Kerberos ticket encryption

- ☒ RC4-HMAC
- ☒ AES-256

For more information on support for protocol settings in SMB clients, see [SMB on Windows](#) and [SMB on Linux](#).



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

Security

Protocol settings

Azure Files exposes settings that let you toggle the SMB protocol to be more compatible or more secure, depending on your organization's requirements. Restricting these settings may prevent some clients from being able to connect. [Learn more](#)

Profile

Custom

SMB protocol versions

- ☐ SMB 2.1
- ☐ SMB 3.0
- ☒ SMB 3.1.1

Authentication mechanisms

- ☐ NTLM v2
- ☒ Kerberos

SMB channel encryption

- ☐ None
- ☒ AES-128-CCM
- ☒ AES-128-GCM
- ☒ AES-256-GCM

Kerberos ticket encryption

- ☒ RC4-HMAC
- ☒ AES-256

For more information on support for protocol settings in SMB clients, see [SMB on Windows](#) and [SMB on Linux](#).

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

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

Answer:

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

Explanation:

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

NEW QUESTION: 124

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

□ □ 6

```
VM10000 00 0000 00 CPU 0000 15 00 70% 0 00 00 adminl@contoso.com000 000000 0000000 0000 0000.
```

Answer:

Check below steps in explanation for Task.

Explanation:

To email an alert to a user named `admin1@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, admin1@contoso.com.
 - * Select OK.

NEW QUESTION: 125

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

[illegible]

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

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

00 00: 0000 000 00 ID0 00000 AKS10 00000 00 ID0 Azure Kubernetes Service 0000 0000 0000 000000.

□□□ □□ □□□ □□□□□?

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☐ ☐☐☐ ☐ ☐☐ ☐☐ ☐☐ ☐☐☐.

+

Add user

Edit

Remove

Update Credentials

Columns

Got feedback?

The application will appear on the access panel for assigned users. Set 'visible to users?' to no in properties to prevent this.

→

First 100 shown, to search all users & groups, enter a display name

DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
☐ GR Group1	Group	Default Access

☐ ☐ ☐ ☐ App1☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐.

Allow users to request access to this application?

Yes

No

To which group should assigned users be added?

Select group

Group2

>

Require approval before granting access to this application?

Yes

No

Who is allowed to approve access to this application?

Select approvers

1 users selected

>

To which role should users be assigned in this application?

*Select a role

Default Access

>

Microsoft

User3☐ App1☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐.

Group2☐ ☐☐☐ App1☐ ☐☐☐ ☐☐ ☐.

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

□□: □□ 1□□ 1□□□□.

Group2 owners:

	▼
User2 only	
User3 only	
User1 and User2 only	
User2 and User3 only	
User1, User2, and User3	

App1 users:

	▼
Group1 members only	
Group2 members only	
Group1 and Group2 members only	
Group1 and Group2 members and User1 only	
Group1 and Group2 members, User1, and User3 only	

Answer:

Group2 owners:

	▼
User2 only	
User3 only	
User1 and User2 only	
User2 and User3 only	
User1, User2, and User3	

App1 users:

	▼
Group1 members only	
Group2 members only	
Group1 and Group2 members only	
Group1 and Group2 members and User1 only	
Group1 and Group2 members, User1, and User3 only	

Explanation:

Group2 owners:

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

App1 users:

- Group1 members only
- Group2 members only
- Group1 and Group2 members only
- Group1 and Group2 members and User1 only
- Group1 and Group2 members, User1, and User3 only

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

Create a secret

Upload options

Manual

* Name   Microsoft

Password1

* Value

.....

Content type (optional)

Set activation date?  ☒

Activation date

2019-03-01  12:00:00 AM

(UTC+02:00) --- Current Time Zone ---

Set expiration date?  ☒

Expiration date

2020-03-01  12:00:00 AM

(UTC+02:00) --- Current Time Zone ---

Enabled? ☒ Yes ☐ No

User2 Vault1

* , .. .

* : .. .

* : .. . , .. .

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:

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.	☐	☐

Explanation:

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.	☐	☒

NEW QUESTION: 128

ASG1, ASG2, NSG1, NSG2, NSG3, NSG4, VM1, VM2, VM3, VM4.

NSG1, ASG1, NSG2, NSG3, NSG4, VM1, VM2, VM3, VM4, ASG2, NSG2, NSG3, NSG4, VM1, VM2, VM3, VM4.

Answer Area

NSGs:

- NSG2 only
- NSG2 and NSG4 only
- NSG2, NSG3, and NSG4

Virtual machines:

- VM3 only
- VM2 and VM4 only
- VM1, VM2, and VM4 only
- VM1, VM2, and VM3 only
- VM1, VM2, VM3, and VM4

Answer:

Answer Area

NSGs:

- NSG2 only
- NSG2 and NSG4 only
- NSG2, NSG3, and NSG4

Virtual machines:

- VM3 only
- VM2 and VM4 only
- VM1, VM2, and VM4 only
- VM1, VM2, and VM3 only
- VM1, VM2, VM3, and VM4

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

Microsoft

NSGs:

NSG2 only

NSG2 and NSG4 only

NSG2, NSG3, and NSG4

Virtual machines:

VM3 only

VM2 and VM4 only

VM1, VM2, and VM4 only

VM2, VM3, and VM4 only

VM1, VM2, VM3, and VM4

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 SQLdb1.
- * Implement ExpressRoute circuits to the on-premises network as shown in the following table.

NEW QUESTION: 131

contoso.com Azure AD Premium P1 .

Group1 .

1. , , ? .

: 1 .

Portal:

- The Azure Active Directory admin center only
- The Microsoft 365 admin center only
- The Azure Active Directory admin center or the Microsoft 365 admin center

Group type:

- Security only
- Microsoft 365 only
- Security or mail-enabled security only
- Security or Microsoft 365 only
- Security, Microsoft 365, or mail-enabled security

Answer:

Portal:

- The Azure Active Directory admin center only
- The Microsoft 365 admin center only
- The Azure Active Directory admin center or the Microsoft 365 admin center

Group type:

- Security only
- Microsoft 365 only
- Security or mail-enabled security only
- Security or Microsoft 365 only
- Security, Microsoft 365, or mail-enabled security

Explanation:

Portal: The Azure Active Directory admin center only
The Microsoft 365 admin center only
The Azure Active Directory admin center or the Microsoft 365 admin center

Group type: Security only
Microsoft 365 only
Security or mail-enabled security only
Security or Microsoft 365 only
Security, Microsoft 365, or mail-enabled security

<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:

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 is a registered application.

User1 is an Azure AD user. App1 is a registered application. User1 is a registered application.

User1 is a registered application.

A. User1 is a registered application.

B. User1 is a registered application.

C. Azure AD is a registered application.

D. Azure AD is a registered application.

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

Reference:

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

NEW QUESTION: 135

RG1 is a resource group in Azure. RG1 has 15 resources.

RG1 is a resource group in Azure. RG1 has 15 resources.

RG1 is a resource group in Azure. RG1 has 15 resources.

RG1 is a resource group in Azure. RG1 has 15 resources.

A. Azure Active Directory(Azure AD) ID is a resource.

B. Microsoft Defender for Cloud is a resource.

C. RG1 is a resource.

D. RG1 is a resource.

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

RG1 is a resource group in Azure. RG1 has 15 resources.

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

RG1 is a resource group in Azure. RG1 has 15 resources.

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/>

AZ-500-KR ☐☐ ☐☐☐ ☐☐☐☐☐ ☐☐ DumpTop ☐☐ ☐☐☐☐ ☐☐☐ AZ-500-KR ☐☐! DumpTop ☐ ☐☐ **AZ-500-KR** ☐☐ ☐☐☐ ☐☐☐☐☐☐, DumpTop AZ-500-KR ☐☐ ☐☐☐ ☐☐☐☐☐☐☐☐
☐☐☐☐ ☐☐☐☐☐☐☐☐. ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐ DumpTop AZ-500-KR ☐☐☐ ☐☐☐☐☐☐. <https://www.dumptop.com/Microsoft/AZ-500-KR-dump.html> (**520** Q&As Dumps, **30%OFF Special Discount: KrDump**)

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

Which of the following is a valid Azure role definition?

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

Which of the following is a valid Azure role definition?

* A role definition that is assigned to a user.

* A role definition that is assigned to a group.

Which of the following is a valid Azure role definition?

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 VMs are running Windows Server. Which of the following Azure VMs are running Windows Server?

2016

[illegible]

```

{
  "if" : {
    "allof": [
      {
        "field" : "type",
        "equals": "Microsoft.Compute/virtualMachines"
      }
      {
        "field" : "Microsoft.Compute/imagesSKU",
        "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:


```

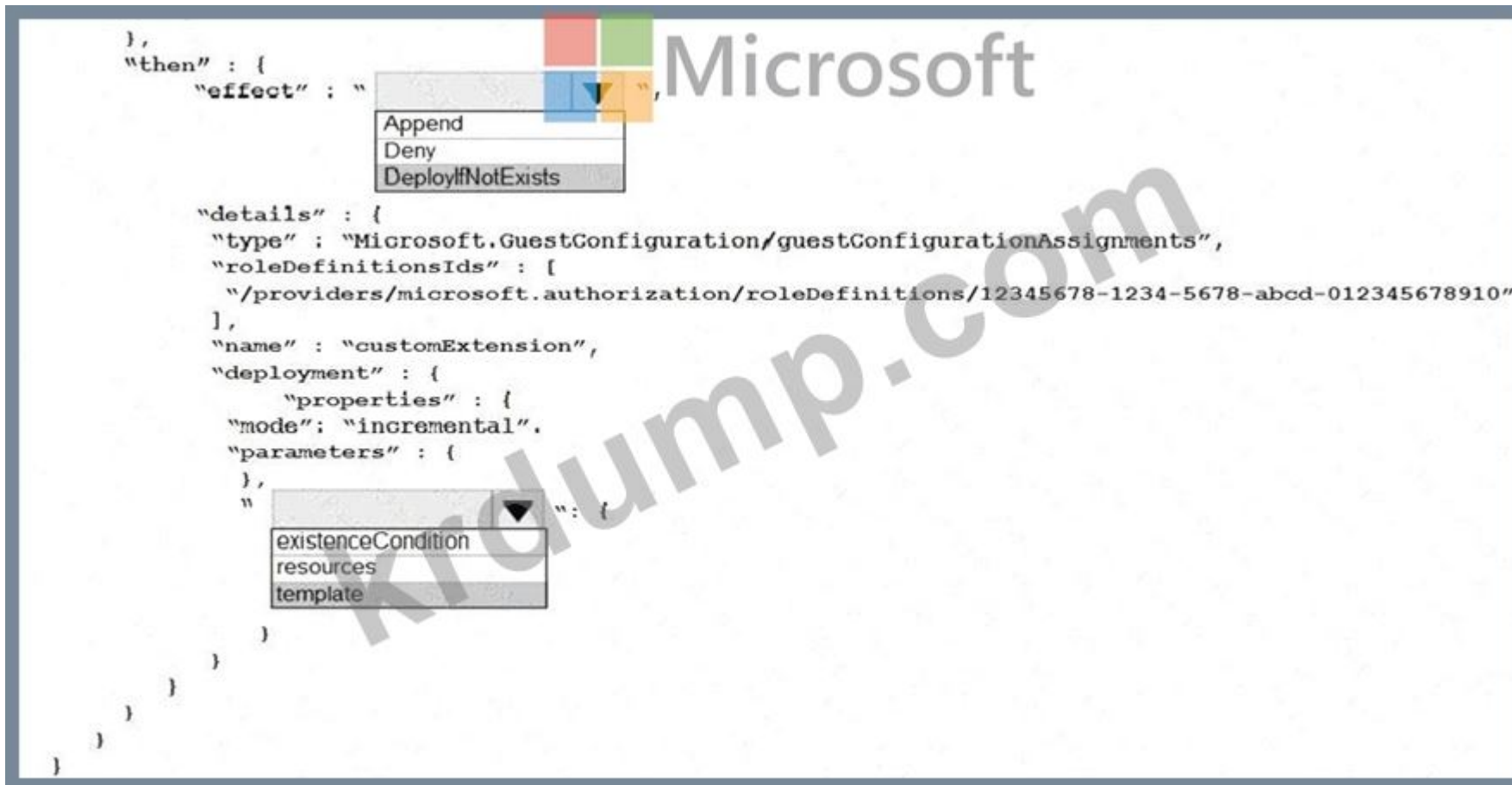
{
  "if" : {
    "allOf": [
      {
        "field" : "type",
        "equals": "Microsoft.Compute/virtualMachines"
      }
    ],
    "then" : {
      "effect" : "
      Append
      Deny
      DeployIfNotExists
      ",

      "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 is an Azure App Service.

WebApp1 has a custom domain name. WebApp1 has a custom domain name.

WebApp1 has a custom domain name.

WebApp1 has a custom domain name?

A. WebApp1 has a custom domain name ID.

B. WebApp1 has a custom domain name.

C. WebApp1 has a custom domain name ID.

D. WebApp1 has a custom domain name.

Answer: (SHOW ANSWER)

Reference:

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

NEW QUESTION: 141

WebApp1 is a web application.
WebApp1 uses a Web Application Firewall (WAF) to protect it.
WebApp1 is in a virtual network (VNet).
WebApp1 is in a resource group (RG).

- A. Azure Front Door
- B. WebApp1
- C. Azure Front Door

Answer: (SHOW ANSWER)

NEW QUESTION: 142

VM1 is a virtual machine (VM) in an Azure virtual network (VNet).
VM1 is in a resource group (RG).
* VM1 is in a virtual network (VNet).
* VM1 is in a resource group (RG).
* VM1 is in a virtual network (VNet).

- A. Azure Disk Encryption
- B. Azure Key Vault
- C. Azure Backup
- D. Azure Disk Encryption

Answer: (SHOW ANSWER)

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

NEW QUESTION: 143

VM1 is a virtual machine (VM) in an Azure virtual network (VNet).

Name	Type
Policy1	Standard
Policy2	Premium

VM1 is in a virtual network (VNet).

Name	Tier	Policy
FW1	Premium	Policy2
FW2	Premium	Policy1

VM1 is in a virtual network (VNet).

Name	Firewall
VNet1	FW1
VNet2	FW2
VNet3	None

VM1 is in a virtual network (VNet).

Answer Area

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

Answer:

Answer Area

Statements

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

Explanation:

Answer Area

Statements

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

NEW QUESTION: 144

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

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

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

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

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

Actions

Publish an Azure Blueprints version

Assign an Azure blueprint.

Create a policy assignment.

Create a custom role-based access control (RBAC) role.

Create a dedicated management subscription.

Create an Azure Blueprints definition.

Create an initiative assignment.

Answer Area

⬅

➡

⬅

➡



Answer:

Actions

Publish an Azure Blueprints version

Assign an Azure blueprint.

Create a policy assignment.

Create a custom role-based access control (RBAC) role.

Create a dedicated management subscription.

Create an Azure Blueprints definition.

Create an initiative assignment.

Answer Area

Create an Azure Blueprints definition.

Publish an Azure Blueprints version

Assign an Azure blueprint.



Explanation:

Create an Azure Blueprints definition.

Publish an Azure Blueprints version

Assign an Azure blueprint



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:

User1: ▼

A key vault access policy
Azure Information Protection
Azure Policy
Managed identities for Azure resources
RBAC

User2:  ▼

A key vault access policy
Azure Information Protection
Azure Policy
Managed identities for Azure resources
RBAC

Answer:

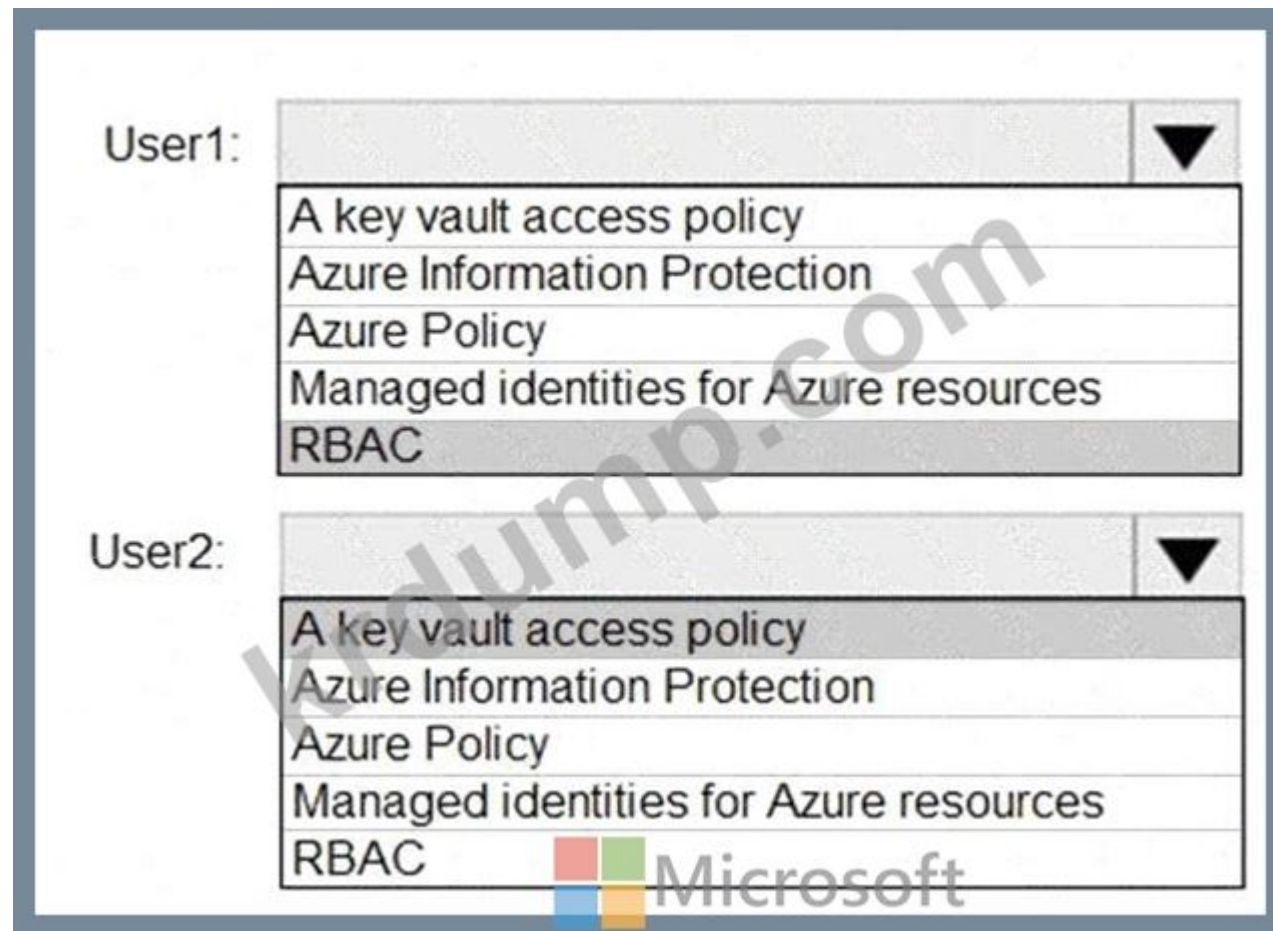
User1: ▼

A key vault access policy
Azure Information Protection
Azure Policy
Managed identities for Azure resources
RBAC

User2:  ▼

A key vault access policy
Azure Information Protection
Azure Policy
Managed identities for Azure resources
RBAC

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

Which of the following is a cloud security framework?

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

Which of the following is a cloud security framework? Microsoft Defender for Cloud is a cloud security framework. Which of the following is a cloud security framework?

- A. CIS (CIS)
- B. NIST 800-53
- C. ISO 27001
- D. SOC 2 (SOC) 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>

AZ-500-KR ☐☐ ☐☐☐ ☐☐☐☐☐ ☐☐ DumpTop ☐☐ ☐☐☐☐ ☐☐☐ AZ-500-KR ☐☐! DumpTop ☐ ☐☐ **AZ-500-KR** ☐☐ ☐☐☐ ☐☐☐☐☐☐, DumpTop AZ-500-KR ☐☐ ☐☐☐ ☐☐☐☐☐☐☐☐
☐ ☐☐☐ ☐☐☐☐☐☐☐. ☐☐☐☐ ☐☐☐ ☐☐☐☐ ☐☐ DumpTop AZ-500-KR ☐☐☐ ☐☐☐☐☐. <https://www.dumptop.com/Microsoft/AZ-500-KR-dump.html> (**520** Q&As Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 152

Azure Sentinel ☐☐ ☐☐☐ ☐☐☐ Azure ☐☐☐ ☐☐☐.

Azure Sentinel is a cloud-native security solution that provides a centralized view of your organization's security data. It uses machine learning and threat intelligence to detect and respond to threats in real-time. Azure Sentinel is built on the Azure cloud platform and integrates with various Microsoft and third-party security products. It provides a comprehensive set of tools for threat detection, investigation, and response, including a central dashboard, incident response workflows, and a rich set of analytics and playbooks. Azure Sentinel is designed to be scalable and flexible, allowing you to tailor your security solution to your organization's specific needs. It is a key component of the Microsoft Security Center, which provides a unified view of your organization's security posture across all Microsoft and third-party services.

* Azure Sentinel is a cloud-native security solution that provides a centralized view of your organization's security data. It uses machine learning and threat intelligence to detect and respond to threats in real-time. Azure Sentinel is built on the Azure cloud platform and integrates with various Microsoft and third-party security products. It provides a comprehensive set of tools for threat detection, investigation, and response, including a central dashboard, incident response workflows, and a rich set of analytics and playbooks. Azure Sentinel is designed to be scalable and flexible, allowing you to tailor your security solution to your organization's specific needs. It is a key component of the Microsoft Security Center, which provides a unified view of your organization's security posture across all Microsoft and third-party services.

* Azure Sentinel is a cloud-native security solution that provides a centralized view of your organization's security data. It uses machine learning and threat intelligence to detect and respond to threats in real-time. Azure Sentinel is built on the Azure cloud platform and integrates with various Microsoft and third-party security products. It provides a comprehensive set of tools for threat detection, investigation, and response, including a central dashboard, incident response workflows, and a rich set of analytics and playbooks. Azure Sentinel is designed to be scalable and flexible, allowing you to tailor your security solution to your organization's specific needs. It is a key component of the Microsoft Security Center, which provides a unified view of your organization's security posture across all Microsoft and third-party services.

It is a key component of the Microsoft Security Center, which provides a unified view of your organization's security posture across all Microsoft and third-party services. It is a key component of the Microsoft Security Center, which provides a unified view of your organization's security posture across all Microsoft and third-party services. It is a key component of the Microsoft Security Center, which provides a unified view of your organization's security posture across all Microsoft and third-party services.



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 is an Azure subscription.

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

Subscription1 is an Azure subscription.

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

Subscription1 is an Azure subscription.

Subscription1 is an Azure subscription.

Subscription1 is an Azure subscription.

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

Answer:

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

Explanation:

NO

NO

NO

Reference:

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

NEW QUESTION: 154

Azure 1001 VM1000 Azure 1000 1000.

VM10 Microsoft SQL Server1000 VNet1000 1000 1000. App1, VM1, Vent1000 Azure 1000 1000.

App10 VM10 1000 1000 1000 1000. 1000 1000 1000 1000.

A. Azure Application Gateway 100

B. Azure 100

C. 1000 1000 1000 1000

D. NAT 100000 100

E. 100000 1000 1000 1000 1000

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

NEW QUESTION: 155

100 1000 100 sk2311000 Azure Key Vault10000 10000.


sk2311 | Properties
☆
...
✕

Key vault

»
Save
✕ Discard changes
🔄 Refresh

Name

sk2311

Sku (Pricing tier)

Standard

Location

eastus

Vault URI

https://sk2311.vault.azure.net/

Resource ID

/subscriptions/7efd66e-8694-4b54-beae-...

Subscription ID

7efd66e-8694-4b54-beae-17fd819d4873

Subscription Name

Visual Studio Enterprise Subscription

Directory ID

5864e735-7190-4615-b2a0-0b20615b75de

Directory Name

Default Directory

Soft-delete

Soft delete has been enabled on this key vault

Days to retain deleted vaults

90

Purge protection

☒ Disable purge protection (allow key vault and objects to be purged during retention period)

☐ Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)

Sk2311□□ □□ □□ □□□ □□□ □□□□ □□□□.

Microsoft	
Name	Type
Item1	Key
Item2	Secret
Policy1	Access policy

sk2311□□□ □□ □□□□ □□□□ □□□□□□.

* Item1□ □□□□□□□□.

* □□2□ □□1□ □□□□□□□□.

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

□□: □□ 1□□ 1□□□□□.

Answer Area

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

Answer:

Answer Area

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

Explanation:

Answer Area

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

NEW QUESTION: 156

User1 is a user in an Azure AD tenant. User1 is a member of the Azure AD group named Group1.

* Group1 is a security group.

* Group1 is a mail-enabled security group.

* Group1 is an Azure AD group.

Group1 is a security group. User1 is a member of Group1. What is the result of the following command?

A. Group1 is a security group.

B. Group1 is a mail-enabled security group.

C. ID of Group1 is returned.

D. Group1 is a security group.

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

NEW QUESTION: 157

VM1 is a virtual machine in an Azure subscription. VM1 is a member of the Azure AD group named Group1.

□□□□ □□□ □□ □□□ □□□□ □□□.

□□ □□ □□□ □□ □□□?

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 □□ □□ □□□ □□□□□.

Custom smart lockout

Lockout threshold ⓘ 10

Lockout duration in seconds ⓘ 60

Custom banned passwords

Enforce custom list ⓘ Yes No

Custom banned password list ⓘ

Adatum

Microsoft

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ Yes No

Mode ⓘ Enforced Audit

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

□□: □□ 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 □□□□□□ □□□ □□□□□ Web3! 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

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

☐ ☐☐ ☐☐☐☐ ☐☐☐ ☐☐ ☐ ☐☐☐☐.

[illegible]

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

[illegible][illegible]

□□□: □□ □□□ □□□ □□□□□□ □□□ □□□□.

□□□ □□□ □□□□□?

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 ☐ ☐ ☐ ☐ ☐ ☐.

[illegible]

Actions

Run the `Set-AzVMDiskEncryptionExtension` cmdlet.

Set the Key Vault access policy to **Enable access to Azure Virtual Machines for deployment**.

Set the Key Vault access policy to **Enable access to Azure Disk Encryption for volume encryption**.

Generate a key vault certificate.

Create an Azure key vault.

Configure storage1 to use a customer-managed key.

Answer Area


Microsoft

Answer:

Actions

Run the `Set-AzVMDiskEncryptionExtension` cmdlet.

Set the Key Vault access policy to **Enable access to Azure Virtual Machines for deployment**.

Set the Key Vault access policy to **Enable access to Azure Disk Encryption for volume encryption**.

Generate a key vault certificate.

Create an Azure key vault.

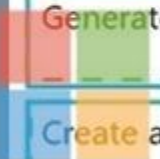
Configure storage1 to use a customer-managed key.

Answer Area

Create an Azure key vault.

Set the Key Vault access policy to **Enable access to Azure Disk Encryption for volume encryption**.

Run the `Set-AzVMDiskEncryptionExtension` cmdlet.


Microsoft

Explanation:

Graphical user interface, text, application Description automatically generated

Create an Azure key vault.

Set the Key Vault access policy to **Enable access to Azure Disk Encryption for volume encryption**.

Run the `Set-AzVMDiskEncryptionExtension` cmdlet.


Microsoft

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 is an Azure Key Vault, which is a cloud-based service for storing and managing secrets. Vault1 is a secure storage for secrets and keys. Vault1 is a secure storage for secrets and keys.

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

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.

Yes **No**

☒ ☐

☐ ☒

☐ ☒

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□ □□□□□ □□□ □□□ □□□□□ □□□.

[illegible]

- A. ☐☐
- B. ☐☐
- C. ☐☐☐☐☐☐

Answer: C (LEAVE A REPLY)

AZ-500-KR ☐☐ ☐☐☐ ☐☐☐☐☐ ☐☐ DumpTop ☐☐ ☐☐☐☐ ☐☐☐ AZ-500-KR ☐☐! DumpTop ☐☐☐ **AZ-500-KR** ☐☐ ☐☐☐ ☐☐☐☐☐☐, DumpTop AZ-500-KR ☐☐ ☐☐☐ ☐☐☐☐☐☐☐☐
☐☐☐☐ ☐☐☐☐☐☐☐☐. ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐ DumpTop AZ-500-KR ☐☐☐☐ ☐☐☐☐☐☐. <https://www.dumptop.com/Microsoft/AZ-500-KR-dump.html> (**520 Q&As Dumps**, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 167

contoso.com Active Directory

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

Azure AD Connect ☐ ☐☐☐ Active Directory ☐ Azure AD ☐☐☐☐ ☐☐☐☐.

☐☐ ☐☐ ☐☐☐ ☐☐☐☐ ☐☐ ☐☐☐☐ ☐☐☐☐

[illegible]

Which of the following is a benefit of using Azure Active Directory?

- A. Active Directory Federation Services(AD FS) can be used to connect to on-premises ID
- B. Single Sign-On(SSO) can be used to connect to on-premises ID
- C. Single Sign-On(SSO) can be used to connect to on-premises ID

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

Which of the following is a benefit of using Azure Key Vault?

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

Azure Key Vault can be used to store secrets and keys.

VM1 and VM2 are both Azure Disk Encryption enabled.

Which of the following is a benefit of using Azure Key Vault?

Answer: C (LEAVE A REPLY)

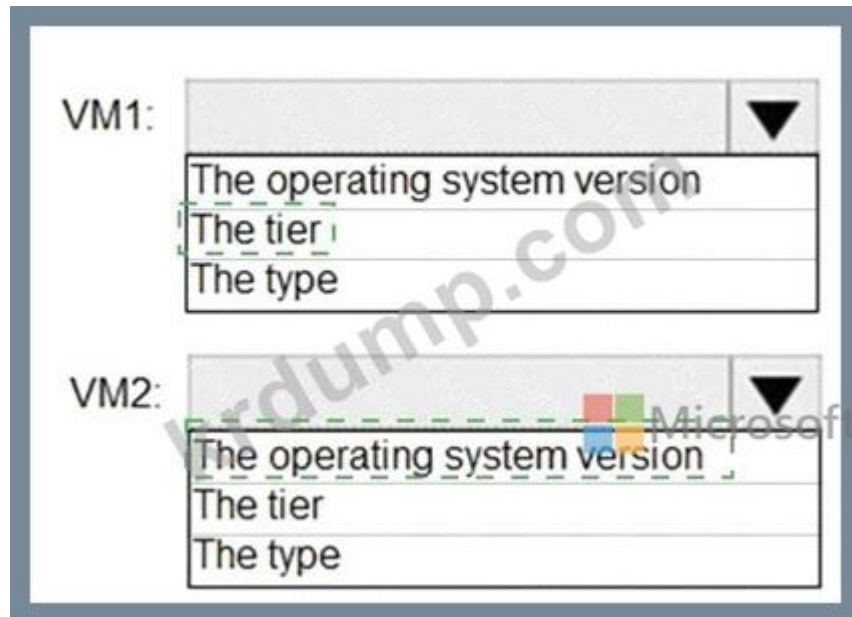
VM1: ▼

The operating system version
The tier
The type

VM2: ▼

The operating system version
The tier
The type Microsoft

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 is integrated with Azure Monitor. It can detect and respond to threats in Azure resources. It can also detect and respond to threats in on-premises resources. Which of the following is a benefit of using Microsoft Defender for Cloud?

- A. Azure Monitor can detect and respond to threats in Azure resources.
- B. PostgreSQL Audit (pgAudit) can detect and respond to threats in Azure resources.
- C. Microsoft Defender for Cloud can detect and respond to threats in Azure resources.
- D. Azure Monitor can detect and respond to threats in on-premises resources.

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

NEW QUESTION: 170

Sub1 is an Azure subscription. It contains a resource group named RG1. RG1 contains a virtual machine named VM1. VM1 is running Windows Server 2016. The virtual machine is configured with the following settings:

- Operating system: Windows Server 2016
- Virtual machine size: Standard_D2s_v2
- Storage: Standard HDD
- Network: Virtual Network
- Security: Windows Defender

- A. Azure DevOps
- B. Azure Logic Apps
- C. Azure Monitor
- D. Azure Security Center

Answer: ([SHOW ANSWER](#))

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

<https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time?tabs=jit-config-asc%2Cjit-request-asc>

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

□□ □□: □ □□ □□□□ 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

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

[illegible]

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 Area

Microsoft

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

Answer:

Answer Area

Microsoft

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

Explanation:

Answer Area

Microsoft

Statements

	Yes	No
WebApp1 can connect to VM2.	☒	☐
NSG1 controls inbound traffic to WebApp1.	☒	☐
WebApp2 can connect to VM1.	☐	☒

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 ☐.

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

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

-EnabledForDeployment
-EnablePurgeProtection

-Tag

-Confirm
-DefaultProfile
-EnableSoftDelete
-SKU

Answer:

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

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

-EnabledForDeployment
-EnablePurgeProtection

-Tag

-Confirm
-DefaultProfile
-EnableSoftDelete
-SKU

Explanation:

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

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

-EnabledForDeployment
-EnablePurgeProtection
-Tag

-Confirm
-DefaultProfile
-EnableSoftDelete
-SKU

Box 1: -EnablePurgeProtection

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

Box 2: -EnableSoftDelete

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

References:

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

NEW QUESTION: 180

Windows Server 2019 VM1 VM2 Azure VMs.

Azure Automation VMs.

Update1 VMs.

Update! VMs.

* VM1 VM2 VMs.

* VMs Windows Server 2019 VMs Update1 VMs.

1 VMs?

A. VMs VMs VMs VMs VMs VMs

B. VMs VMs VMs VMs VMs VMs

C. VMs VMs VMs

D. Kusto VMs VMs VMs

Answer: C (LEAVE A REPLY)

NEW QUESTION: 181

VMs VMs

VMs 4

VMs Azure Resource Manager VMs VMs VMs VMs VMs KV31330471 VMs Azure Key Vault VMs VMs VMs VMs VMs.

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.

AZ-500-KR VMs VMs VMs VMs VMs DumpTop VMs VMs VMs AZ-500-KR VMs! DumpTop VMs VMs **AZ-500-KR** VMs VMs VMs VMs VMs, DumpTop AZ-500-KR VMs VMs VMs VMs VMs VMs VMs VMs. VMs VMs VMs VMs VMs DumpTop AZ-500-KR VMs VMs VMs VMs. <https://www.dumptop.com/Microsoft/AZ-500-KR-dump.html> (520 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

NEW QUESTION: 182

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

VMs App1 VMs VMs VMs VMs VMs VMs. App1 VMs Windows Server 2016 VMs VMs VMs VMs VMs. App1 VMs contoso.com VMs VMs Microsoft Graph VMs VMs VMs VMs VMs.

App1 VMs VMs VMs VMs VMs VMs.

Azure Portal VMs VMs VMs VMs VMs VMs VMs VMs? VMs VMs VMs VMs VMs VMs VMs VMs VMs VMs VMs VMs VMs.

Actions

Grant permissions

Add a delegated permission.

Configure Azure AD Application Proxy.

Add an application permission.

Create an app registration.

Answer Area

Answer:

ACTIONS

Grant permissions

Add a delegated permission.

Configure Azure AD Application Proxy.

Add an application permission.

Create an app registration.

Create an app registration.

Add an application permission.

Grant permissions

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:

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□□ □□□□□ □□□ □□ □□□□□ □□□□ □□□□□ □□□.

* □□□□ □□□ □□ □□□ □□□□□ □□□.

VNet1□ NSG1□ □□ □□□ □□□□ □□□? □□□ □□ □□ □□□ □□□ □□□□ □□□□ □□□□. □ □□ □□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□. □□□□ □□□ □ □ □□ □□ □□□□□ □□□□□ □ □□ □□□□. □□: □□□ □□ □□□ 1□□□□.

Components

- A private endpoint
- A route table
- A service endpoint
- A service tag

Answer Area

VNet1:

NSG1:

Answer:

Components

- A private endpoint
- A route table
- A service endpoint
- A service tag

Answer Area

VNet1:

NSG1:

Explanation:

Components

- A private endpoint
- A route table
- A service endpoint
- A service tag

Answer Area

VNet1:

NSG1:

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

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

[illegible]

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

Azure Disk Encryption ☐ ☐ ☐ ☐ VM1 ☐ ☐ ☐ ☐ ☐ ☐.

[illegible]

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



Answer:

Custom smart lockout

Lockout threshold ⓘ 10 ✓

Lockout duration in seconds ⓘ 60 ✓

Custom banned passwords

Enforce custom list ⓘ Yes No

Custom banned password list ⓘ

Adatum ✓

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ Yes No

Mode ⓘ Enforced Audit

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

□□: □□ 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:

Microsoft **Statements**

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

User1 will be prompted to change the password on the next sign-in.

Yes

☐

No

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 00000.
- B.** 00000 0000 000 000 000 000000.
- C.** RT1 AzureFirewallSubnet 00000.
- D.** 00000 DNAT 000 00000.

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

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

Answer:

Answer Area



Explanation:

A screenshot of a computer Description automatically generated

Answer Area

...

```

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

```

...

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□□□□.

Microsoft

Update1: ▼

VM2 only
VM4 only
VM1 and VM2 only
VM1, VM2, VM4, VM5, and VM6

Update2: ▼

VM5 only
VM1 and VM5 only
VM4 and VM5 only
VM1, VM2, and VM5 only
VM1, VM2, VM3, VM4, and VM5

Answer:

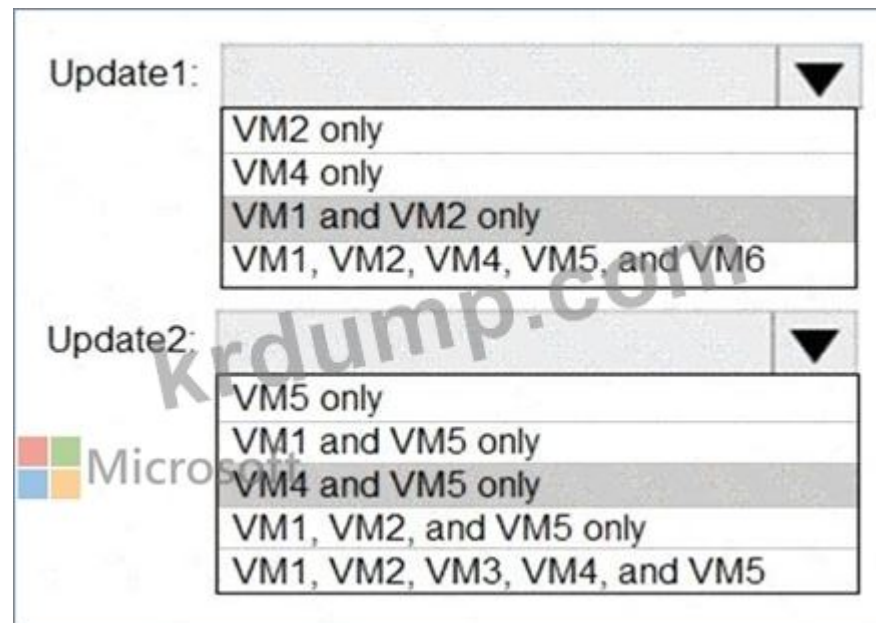
Update1: ▼

VM2 only
VM4 only
VM1 and VM2 only
VM1, VM2, VM4, VM5, and VM6

Update2: ▼

VM5 only
VM1 and VM5 only
VM4 and VM5 only
VM1, VM2, and VM5 only
VM1, VM2, VM3, VM4, and VM5

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

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

Actions

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

Answer Area

Answer:

Actions

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

Answer Area

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

Explanation:

QUESTION 193

⋮

Add a managed certificate.

⋮

Configure the Inbound traffic configuration settings and the Outbound traffic configuration settings.

⋮

Add a custom domain to WebApp1.

⋮

Add a public key certificate (.cer).



QUESTION 194

1

⋮

Change the App Service plan to Basic.

2

⋮

Change the App Service plan to Shared.

3

⋮

Add a deployment slot to WebApp1.

NEW QUESTION: 193

Sub1 is an Azure subscription. You need to create a storage account and an Azure key vault in Sub1.

Name	Type
storage1	Storage account
KeyVault1	Azure key vault

You need to run a command to create the storage account and the key vault. Which command should you run?

- A. Add-A:StorageAccountmanagementPolicyAction
- B. -A=StorageAccount -KeyVault
- C. Set-A; -KeyVault
- D. Add-AsKeyVaultmanageStorageAccount

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

NEW QUESTION: 194

Sub1 is an Azure subscription. You need to create a storage account and an Azure key vault in Sub1.

Azure Security Center Play1 is a playbook that you want to change. Play1 is a User1 playbook that you want to change. You need to change the playbook 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:

Play1 is a playbook that you want to change. You need to change the playbook 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:

Play1 is a playbook that you want to change. You need to change the playbook 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:

Play1 is a playbook that you want to change. You need to change the playbook 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.

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 ☐ ☐ ☐: User1 -28681041@ExamUsers.com

Azure ☐ ☐ ☐: GpOAe4@IDg

Azure Portal☐ ☐ ☐ ☐ ☐ ☐ CTRL-K☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐.

☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐.

☐ ☐ ☐ ☐: 28681041

☐ ☐ 1

☐ ☐ ☐ ☐ VM1☐ ☐ ☐ ☐ RDP ☐ ☐ ☐ ☐ Azure☐ ☐ ☐ ☐.

☐ ☐ ☐ VM1☐ ☐ ☐ ☐ ☐ ☐.

Answer:

Check below steps in explanation for Task.

Explanation:

* 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.

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□□ □□□□□.

Values

- ☐ Get-AzPolicyAssignment
- ☐ Get-AzPolicyDefinition
- ☐ Get-AzPolicySetDefinition
- ☐ New-AzPolicyAssignment
- ☐ New-AzPolicyDefinition
- ☐ New-AzPolicySetDefinition
- ☐ Set-AzPolicySetDefinition
- ☐ Set-AzPolicyAssignment
- ☐ Set-AzPolicyDefinition

Answer Area

```
$rg = Get-AzResourceGroup -Name 'RG1'
$Policy = Get-AzPolicyDefinition -Name 'Policy1'
New-AzPolicyAssignment -Name 'AuditStorageAccounts' -PolicyDefinition
$Policy -Scope $rg.ResourceId
```

Answer:

Values

- ☒ Get-AzPolicyAssignment
- ☒ Get-AzPolicyDefinition
- ☒ Get-AzPolicySetDefinition
- ☒ New-AzPolicyAssignment
- ☒ New-AzPolicyDefinition
- ☒ New-AzPolicySetDefinition
- ☒ Set-AzPolicySetDefinition
- ☒ Set-AzPolicyAssignment
- ☒ Set-AzPolicyDefinition

Answer Area

```
$rg = Get-AzResourceGroup -Name 'RG1'
$Policy = Get-AzPolicyDefinition -Name 'Policy1'
New-AzPolicyAssignment -Name 'AuditStorageAccounts' -PolicyDefinition
$Policy -Scope $rg.ResourceId
```

Explanation:

Values

Get-AzPolicyAssignment

Get-AzPolicyDefinition

Get-AzPolicySetDefinition

New-AzPolicyAssignment

New-AzPolicyDefinition

New-AzPolicySetDefinition

Set-AzPolicySetDefinition

Set-AzPolicyAssignment

Set-AzPolicyDefinition

Answer Area

```
$rg = Get-AzResourceGroup -Name 'RG1'
$Policy = Get-AzPolicyDefinition -Name 'Policy1'
New-AzPolicyAssignment -Name 'AuditStorageAccounts' -PolicyDefinition
$Policy -Scope $rg.ResourceId
```



Microsoft

NEW QUESTION: 202

Azure □□□ □□□□.

VM1□□□ □□ □□□ □□□ □□□□□.

VM1□□ □□ □□□ □□□□ □□□□ □□□.

VM1□ □□ □□ □□ □□□□ □□□□ □□, □□ □□□ □□□□ □□□□ □□□□ □ □□ □□□ □□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □□ 1□□ 1□□□□.

Answer Area

Virtual machine series:

ECasv5
Ddsv5
ECasv5
Lsv2
NVadsA10v5

Disks:

The OS disk and data disks
Data disks only
The OS disk only
The OS disk and data disks

Answer:

Answer Area

Virtual machine series: ECasv5
Ddsv5
ECasv5
Lsv2
NVadsA10v5

Disks: The OS disk and data disks
Data disks only
The OS disk only
The OS disk and data disks

Explanation:

Answer Area

Microsoft

Virtual machine series: ECasv5

Disks: The OS disk and data disks

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

.

Temporary Access Pass settings



Temporary Access Pass, or TAP, is a time-limited or limited-use passcode that can be used by users for bootstrapping new accounts, account recovery, or when other auth methods are unavailable.

[Learn more.](#)

TAP is issuable only by administrators, and is seen by the system as strong authentication. It is not usable for Self Service Password Reset.

Enable and Target

Configure

Enable ☒

Include ☒ Exclude ☐

Target ☐ All users ☒ Select groups

[Add groups](#)

Name

Type

Registration

Group1

Group

Optional

Admin2 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 Area

Statements

Admin1 can view the Temporary Access Pass of Admin2.

Yes

No

☐☐

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 is a cloud-based service that helps you protect your data. It uses Azure Information Protection labels to classify and protect your data. You can create and manage these labels in the Azure Information Protection portal. You can also use the Azure Information Protection PowerShell cmdlets to manage labels. You can also use the Azure Information Protection REST API to manage labels. You can also use the Azure Information Protection SDK to manage labels. You can also use the Azure Information Protection CLI to manage labels. You can also use the Azure Information Protection GUI to manage labels. You can also use the Azure Information Protection PowerShell cmdlets to manage labels. You can also use the Azure Information Protection REST API to manage labels. You can also use the Azure Information Protection SDK to manage labels. You can also use the Azure Information Protection CLI to manage labels. You can also use the Azure Information Protection GUI to manage labels.

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

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

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:

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	

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 □□□ □□□□.

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)

Answer:

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)

Explanation:

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

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)

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

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)

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

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

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

□□: □□ 1□□ 1□□□□.

Microsoft

NSGs: ▼

1
2
3
4

Network security rules: ▼

1
2
3
4

Answer:

Microsoft

NSGs: ▼

1
2
3
4

Network security rules: ▼

1
2
3
4

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□□□□.

Authentication methods	Answer Area
FIDO2 security key only	User1:
Microsoft Authenticator app only	User2:
Windows Hello for Business only	
Microsoft Authenticator app and Windows Hello for Business only	
Windows Hello for Business and FIDO2 security key only	
Microsoft Authenticator app, Windows Hello for Business, and FIDO2 security key	

Microsoft

Answer:

Authentication methods	Answer Area
FIDO2 security key only	User1: Microsoft Authenticator app only
Microsoft Authenticator app only	User2: Windows Hello for Business only
Windows Hello for Business only	
Microsoft Authenticator app and Windows Hello for Business only	
Windows Hello for Business and FIDO2 security key only	
Microsoft Authenticator app, Windows Hello for Business, and FIDO2 security key	

Microsoft

Explanation:

Authentication methods

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

Answer Area

User1: Microsoft Authenticator app only

User2: Windows Hello for Business only

NEW QUESTION: 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:

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.	☐	☒

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 is an Azure Active Directory(Azure AD) tenant. RG1 is a resource group in Subscription1 in the contoso.com tenant. Role1 is a custom role in the contoso.com tenant. Role1 is assigned to the contoso.com\RG1\Subscription1 role. What is the correct role assignment?

- A. contoso.com\RG1\Subscription1
- B. contoso.com\RG1
- C. contoso.com\Subscription1
- D. contoso.com, RG1\Subscription1

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

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

NEW QUESTION: 219

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

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

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

□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

Microsoft	
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 □□□ □□□□.

Microsoft	
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 is a role that is defined in the JSON file below.

Name	Role
User1	Role1
User2	Role2
User3	Role1, Role2

There are three users, User1, User2, and User3, who are assigned to Role1 and Role2. Role1 is a role that is defined in the JSON file below. Role2 is a role that is defined in the JSON file below.

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

Answer:

Answer Area

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

Explanation:

Answer Area

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

NEW QUESTION: 224

Scenario: Your company has a Microsoft Entra ID tenant named Contoso. The tenant contains the following objects:

Group1: A security group that contains User1 and User2.

Group2: A Microsoft 365 group that contains User1 and User2.

App1: An application registration that is assigned the Owner role for Group1 and Group2.

MI1: A user-assigned managed identity that is assigned the Owner role for App1 and App2.

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

Two Azure SQL databases, SQL1 and SQL2, are deployed to a Microsoft Entra ID tenant named Contoso.

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 is a single-tier Azure SQL database. SQL2 is a Microsoft Entra ID database.

User1 and User2 are both members of Group1 and Group2. They are both assigned the Owner role for App1 and MI1.

Group1 is a security group. SQL1 is a Microsoft Entra ID database.

What is the result of the following query?

A. Success

B. Failure

Answer: B (LEAVE A REPLY)

NEW QUESTION: 225

AzFW1 is an Azure Firewall policy. AzFW1 is assigned to FWP1. FWP1 is assigned to FWP1. FWP1 is assigned to FWP1.

* FQDN is a fully qualified domain name.

* TCP is a transport layer protocol.

What is the result of the following query?

□□: □□ 1□□ 1□□□□.

Answer Area

Microsoft

Allow traffic based on the destination FQDN:

- Application only
- Network only
- Application only
- Network or DNAT only
- Application or DNAT only
- Network or application only
- Network, application, or DNAT

Allow TCP traffic:

- Network only
- Network only
- Application only
- Network or DNAT only
- Application or DNAT only
- Network or application only
- Network, application, or DNAT

Answer:

Answer Area

Microsoft

Allow traffic based on the destination FQDN:

- Application only
- Network only
- Application only
- Network or DNAT only
- Application or DNAT only
- Network or application only
- Network, application, or DNAT

Allow TCP traffic:

- Network only
- Network only
- Application only
- Network or DNAT only
- Application or DNAT only
- Network or application only
- Network, application, or DNAT

Explanation:

Answer Area



Allow traffic based on the destination FQDN: Application only

Allow TCP traffic: Network only

NEW QUESTION: 226

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

App1□□□ □□ □□□□□.

User1□ Azure AD □□□□□□ □□□□ □□□□ App1□ □□□□ □□□.

User1□□ □□ □□□ □□□□ □□□?

A. □□□□ □ □□ □□□

B. □□□□ □□□□□□ □□□

C. □□□□□ ID □□□

D. □□□□□□ □□□

Answer: ([SHOW ANSWER](#))

AZ-500-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ AZ-500-KR □□! DumpTop □ □□ **AZ-500-KR** □□ □□□ □□□□□□, DumpTop AZ-500-KR □□ □□□ □□□□□□□ □ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop AZ-500-KR □□□ □□□□□. <https://www.dumptop.com/Microsoft/AZ-500-KR-dump.html> (520 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

NEW QUESTION: 227

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

* Azure Active Directory ID □□

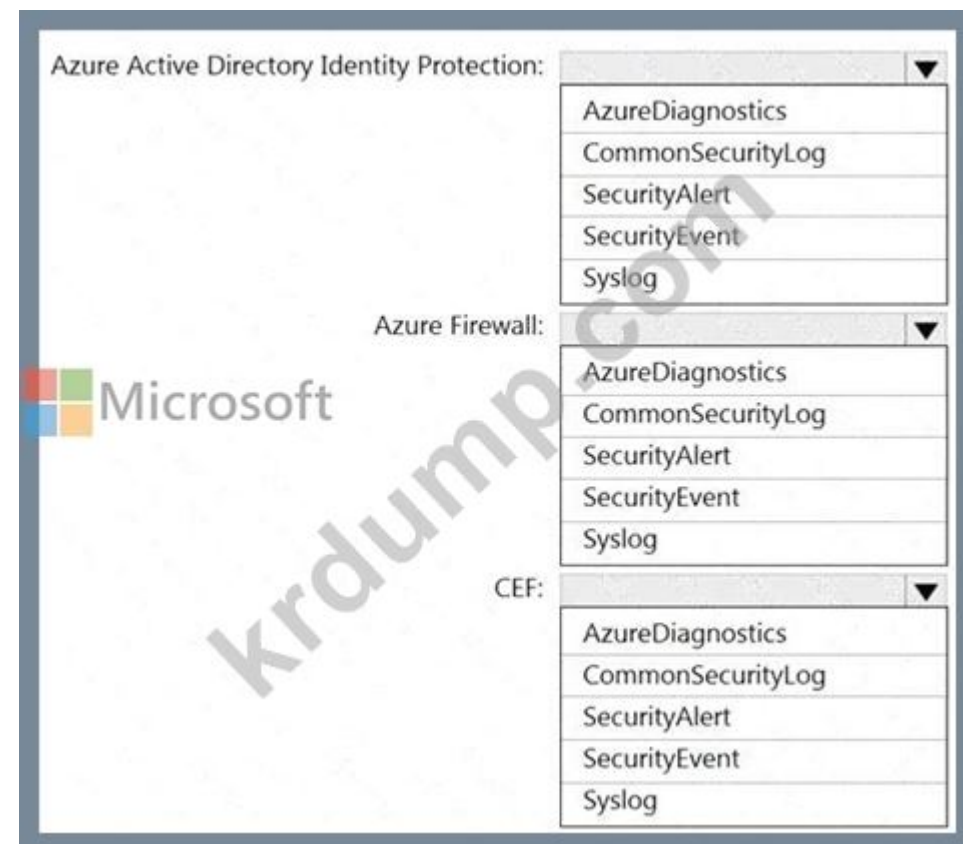
* □□ □□□ □□(CEF)

* Azure □□□

□ □□□□□ □□□□ □□□□□ □□□ □□□.

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

□□: □□ 1□□ 1□□□□.



Answer:

Azure Active Directory Identity Protection

AzureDiagnostics

CommonSecurityLog

SecurityAlert

SecurityEvent

Syslog

Azure Firewall:

AzureDiagnostics

CommonSecurityLog

SecurityAlert

SecurityEvent

Syslog

CEF:

AzureDiagnostics

CommonSecurityLog

SecurityAlert

SecurityEvent

Syslog

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

Azure Active Directory Identity Protection:

AzureDiagnostics

CommonSecurityLog

SecurityAlert

SecurityEvent

Syslog

Azure Firewall:

AzureDiagnostics

CommonSecurityLog

SecurityAlert

SecurityEvent

Syslog

CEF:

AzureDiagnostics

CommonSecurityLog

SecurityAlert

SecurityEvent

Syslog

NEW QUESTION: 228
Azure Security Center Registry1 Azure Container Registry .

□□□ □□ □□□ □□ □□ □□ □□□ □□(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		Yes	No
Statements			
	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		Yes	No
Statements			
	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

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

Yes

☐

No

☒

The custom role grants a user permission to manage the Microsoft Entra admin settings for an Azure SQL Database server.

☐☒

The custom role grants a user permission to reset the administrator password for instances of Azure Database for MariaDB.

☐☒

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@IDg

Azure Portal ☐☐☐☐ ☐☐☐ ☐☐ CTRL-K ☐☐ ☐☐ ☐☐ ☐☐ ☐☐.

☐☐ ☐☐ ☐☐ ☐☐.

☐☐ ☐☐☐☐: 28681041

☐☐ 8

rg1lod28681041n1 Azure Storage ☐☐ ☐☐ HTTP ☐☐ ☐☐ ☐☐.

Answer:

Check below steps in explanation for Task.

Explanation:

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

- * In the Azure portal, search for and select the storage account named rg1lod28681041n1.
- * In the left pane, select Firewalls and virtual networks.
- * In the Firewalls and virtual networks pane, select Selected networks.
- * In the Selected networks pane, select Add existing virtual network.
- * In the Add existing virtual network pane, select the virtual network that does not allow HTTP connections.

* Select Add.

NEW QUESTION: 233

Vault1 is an Azure Key Vault. VM1 is a virtual machine in the same Azure subscription as Vault1. VM1 needs to access the secrets in Vault1.

Vault1 is in the same resource group as VM1.

VM1 needs to access the secrets in Vault1.

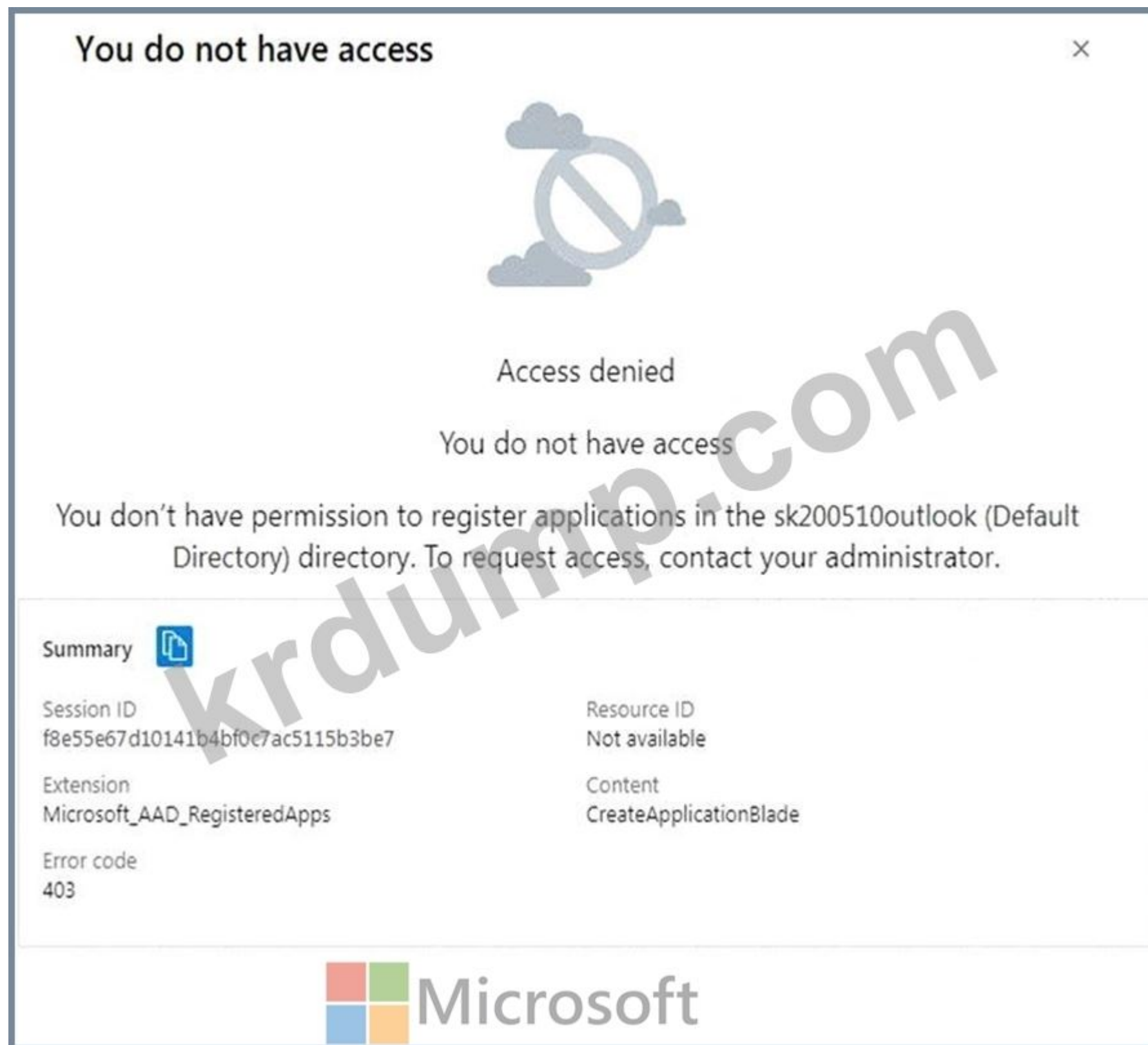
- A. Create a service principal and assign it the Key Vault Secrets User role.
- B. Create a service principal and assign it the Key Vault Secrets User role.
- C. Create a service principal and assign it the Key Vault Secrets User role.
- D. Create a service principal and assign it the Key Vault Secrets User role.
- E. Create a service principal and assign it the Key Vault Secrets User role.
- F. Create a service principal and assign it the Key Vault Secrets User role.

Answer: E (LEAVE A REPLY)

NEW QUESTION: 234

Azure Active Directory(Azure AD) is a cloud-based directory service.

App1 is an application that needs to access the secrets in Azure AD.



- □□□□ 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□□ □□□ □□□□.



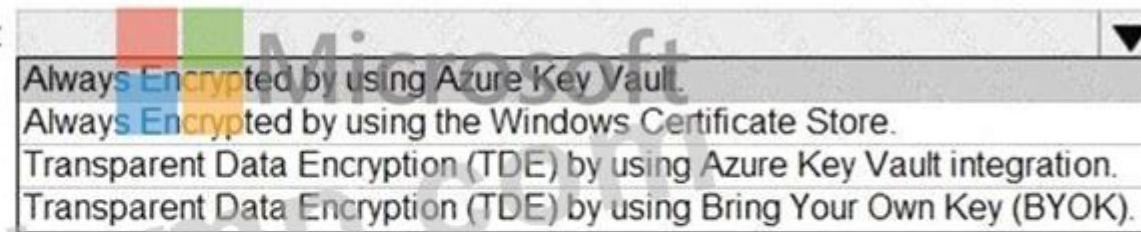
Answer:



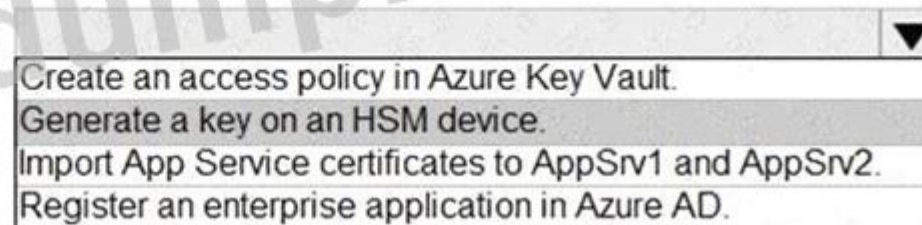
Explanation:

Text Description automatically generated with medium confidence

To configure the encryption of Database1:



To obtain the cryptographic keys:



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□□□□.

Detect suspicious threats:

- A Kusto query language query
- A Transact-SQL query
- An Azure PowerShell query
- An Azure Sentinel playbook

Automate responses:

- An Azure Functions app
- An Azure PowerShell script
- An Azure Sentinel playbook
- An Azure Sentinel workbook

Answer:



Explanation:

Detect suspicious threats:

- A Kusto query language query
- A Transact-SQL query
- An Azure PowerShell query
- An Azure Sentinel playbook

Automate responses:

- An Azure Functions app
- An Azure PowerShell script
- An Azure Sentinel playbook
- An Azure Sentinel workbook

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](#))

AZ-500-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ AZ-500-KR □□! DumpTop □ □□ **AZ-500-KR** □□ □□□ □□□□□□, DumpTop AZ-500-KR □□ □□□ □□□□□□□ □ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop AZ-500-KR □□□ □□□□□. <https://www.dumptop.com/Microsoft/AZ-500-KR-dump.html> (**520** Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

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 Area

Server1:

Subscription:

Microsoft

Answer:

Answer Area

Server1:

Subscription:

Microsoft

Explanation:

Answer Area

Server1:

Subscription:

Microsoft

NEW QUESTION: 244

□□□ □□

□□□ □□ □□ □□□ □□ □□□ □□□□□.

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

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

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

Azure □□□□: GpOAe4@IDg

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 is an Azure Storage account. storage1 has a share named shares1. User1 wants to map shares1 to a local drive on Server1 using SMB. storage1 has the following settings:



Based on the settings, which of the following statements are true? (Select all that apply.)

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.	☐	☐

Answer:

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.	☐	☒

Explanation:

Statements

User1 can map share1 to Server1 by using the access key of storage1.

☒ Yes

No

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.

O



AZ-500-KR                                