

Microsoft.AZ-500.v2026-01-22.q208

Exam Code:	AZ-500
Exam Name:	Microsoft Azure Security Technologies
Certification Provider:	Microsoft
Free Question Number:	208
Version:	v2026-01-22
# of views:	127
# of Questions views:	2080
https://www.freepdfdumps.com/Microsoft.AZ-500.v2026-01-22.q208.html	

NEW QUESTION: 1

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

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

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

Name	Usage location
User1	United States
User2	Germany

You create the groups shown in the following table.

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

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

Dynamic membership rules



Save Discard | Got feedback?

Configure Rules Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. [Learn more](#)

And/Or	Property	Operator	Value	
	accountEnabled	Equals	true	
Or	usageLocation	Equals	US	

[+ Add expression](#) [+ Get custom extension properties](#)

Rule syntax

Edit

```
(user.accountEnabled -eq true) or (user.usageLocation - eq "US")
```

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

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

Answer:

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

Explanation:

Text Description automatically generated

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

Reference:

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

NEW QUESTION: 2

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

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

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

Storage accounts:

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

Virtual machines:

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

Answer:

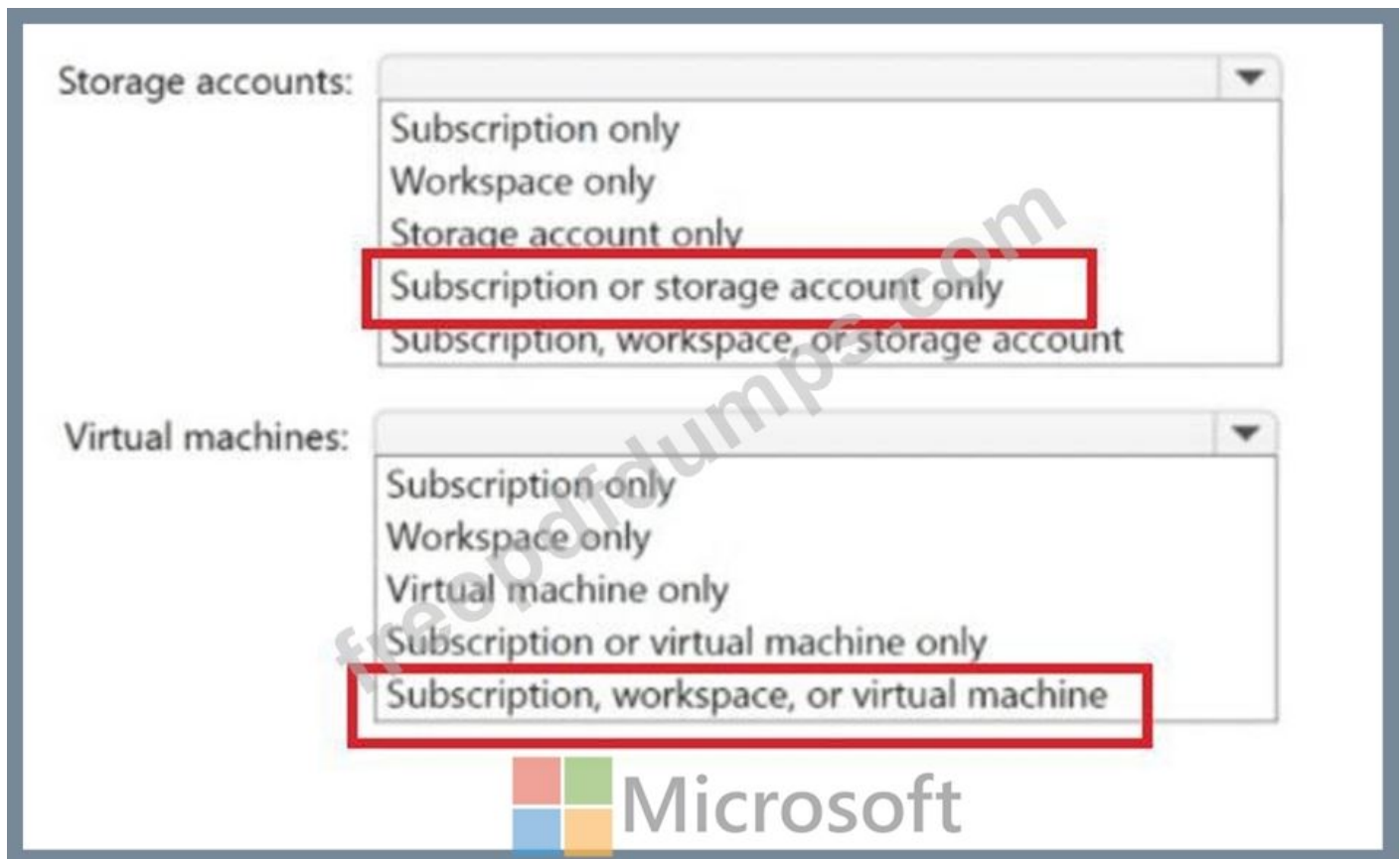
Storage accounts:

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

Virtual machines:

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

Explanation:



NEW QUESTION: 3

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

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

You have a storage account named contoso2024 that contains the following resources:

- * A container named Contained that contains a file named File1
- * A file share named Share1 that contains a file named File2

You create a private endpoint for contoso2024 as shown in the following exhibit.

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

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

Answer Area	Statements	Yes	No
	From VM1, you can 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: 4

You have an Azure subscription that contains a user named User1. You need to ensure that User1 can create managed identities. The solution must use the principle of least privilege. What should you do?

- A. Create management group and assign User1 the Hybrid Identity Administrator Azure AD role.
- B. Create a resource group and assign User1 to the Managed Identity Contributor role.
- C. Create a management group and assign User1 the Managed Identity Operator role.
- D. Create an organizational unit (OU) and assign User1 the User administrator Azure AD role.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 5

Your company has an Azure subscription named Subscription1 that contains the users shown in the following table.

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

The company is sold to a new owner.

The company needs to transfer ownership of Subscription1.

Which user can transfer the ownership and which tool should the user use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

User:

 Microsoft ▼
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:

User: ▼

- User1
- User2
- User3
- User4

Tool: ▼

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

Box 1; User2

Billing Administrator

Select Transfer billing ownership for the subscription that you want to transfer.

Enter the email address of a user who's a billing administrator of the account that will be the new owner for the subscription.

Box 2: Azure Account Center

Azure Account Center can be used.

Reference:

<https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transfer-billing-ownership-of-an-azure-subscription>

NEW QUESTION: 6

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

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

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

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

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

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

Answer:
Answer Area

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

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

Explanation:

Answer Area

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

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

NEW QUESTION: 7

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

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

All the users have devices that contain certificates issued by a certification authority (CA) named ContosoCA.

You create a Conditional Access policy that has the following settings:

- * Name: CAPolscy1
- * Assignments
 - o Users and groups: Group1
 - o Target resources
- * Include: All cloud apps
- o Access controls
- * Grant access: Require multi-factor authentication
- o Enable policy: On

You enable and target certificate-based authentication as shown in the Enable and Target exhibit. (Click the Enable and Target tab.)

Enable and Target **Configure**

Enable ☒

Include **Exclude**

Target ☐ All users ☒ Select groups

Add groups

Name	Type	Registration
Group1	Group	Optional

You configure certificate-based authentication as shown in the Configure exhibit. (Click the Configure tab.)

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

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

Statements

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

User1 can sign in without providing a password.

Yes

☐

No

☒

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

User1 can sign in without providing a password.

Yes

☐

No

☒

User2 can choose to use a certificate or a smart card to sign in.

☐
☒

User3 must use a certificate during sign-in.

☒
☐


NEW QUESTION: 8

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

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

Transparent Data Encryption (TDE) is disabled on SQL1.

You assign policies to the resource groups as shown in the following table.

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

You plan to deploy Azure SQL databases by using an Azure Resource Manager (ARM) template.

The databases will be configured as shown in the following table.

NOTE: Each correct selection is worth one point.

Answer Area



Statements

SQL1 will have TDE enabled automatically.

☐
☐

The deployment of SQL2 will fail.

☐
☐

SQL3 will be deployed and marked as noncompliant.

☐
☐

Answer:

Answer Area

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

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

NEW QUESTION: 9

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

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

The subscription contains Azure web app named WebApp1 that has the following configurations.

- * Region West Us
- * Virtual network VNet1
- * VNet integration on: Enabled
- * Outbound subnet: Subnet11
- * Windows plan (West US): ASP1

You plan to deploy an Azure web app named WebApp2 that will have the following settings:

- * Region: West US
- * VNet integration on-Enabled
- * Windows plan (West UAS): WebApp2?

To which subnets can you integrate WebApp2?

- A. Subnet11 only
- B. Subnet2 only
- C. Subnet11 or subnet12 only
- D. Subnet2 or Subnet21 only
- E. Subnet11, subnet2, or Subnet21

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

NEW QUESTION: 10

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

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

You need to ensure that App1 can access secrets in Azure Key Vault on behalf of the application users.

What should you configure?

- A. an application permission without admin consent
- B. a delegated permission without admin consent
- C. a delegated permission that requires admin consent
- D. an application permission that requires admin consent

Answer: ([SHOW ANSWER](#))

Delegated permissions - Your client application needs to access the web API as the signed-in user, but with access limited by the selected permission. This type of permission can be granted by a user unless the permission requires administrator consent.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis>

NEW QUESTION: 11

You have an Azure subscription.

You configure the subscription to use a different Azure Active Directory (Azure AD) tenant.

What are two possible effects of the change? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Role assignments at the subscription level are lost.
- B. Virtual machine managed identities are lost.
- C. Virtual machine disk snapshots are lost.
- D. Existing Azure resources are deleted.

Answer: ([SHOW ANSWER](#))

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-subscriptions-associated-directory>

NEW QUESTION: 12

You have a Microsoft Entra tenant.

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

- A. From the Properties blade, set Access management for Azure resources to No.
- B. From the User settings blade, set Users can register applications to No.
- C. From the Properties blade, set Enable Security defaults to Yes.
- D. From the User settings blade, set Restrict access to Microsoft Entra ID administration portal to Yes.

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

NEW QUESTION: 13

You have an Azure subscription that contains three storage accounts, an Azure SQL managed instance named SQL and three Azure SQL databases. The storage accounts are configured as shown in the following table.

SQ11 has the following settings:

- * Auditing: On
- * Audit log destination: storage1

The Azure SQL databases are configured as shown in the following table.

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

Answer:

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

Explanation:

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

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: 14

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

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

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

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

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

- A. App3 and App4 only
- B. App1, App2, App3, and App4
- C. App2, App3, and App4 only
- D. App4 only

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 15

You have been tasked with applying conditional access policies for your company's current Azure Active Directory (Azure AD).

The process involves assessing the risk events and risk levels.

Which of the following is the risk level that should be configured for users that have leaked credentials?

- A. None
- B. Low
- C. Medium
- D. High

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

These six types of events are categorized in to 3 levels of risks - High, Medium & Low:

Table Description automatically generated

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

Reference:

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

NEW QUESTION: 16

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure Subscription named Sub1. Sub1 contains an Azure virtual machine named VM1 that runs Windows Server 2016.

You need to encrypt VM1 disks by using Azure Disk Encryption.

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

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:

Actions

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

Answer Area

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

Explanation:

Create an Azure key vault.

Configure access policies for the Azure key vault.

Run Set-AzureRmVmDiskEncryptionExtension.

References:

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

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam!

Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (497 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 17

You are troubleshooting a security issue for an Azure Storage account You enable Azure Storage Analytics logs and archive It to a storage account. What should you use to retrieve the diagnostics logs?

- A. SQL query editor in Azure
- B. Azure Cosmos DB explorer
- C. Azure Storage Explorer
- D. Azure Monitor

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

NEW QUESTION: 18

You have a file named File1.yaml that contains the following contents.

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

You create an Azure container instance named container1 by using File1.yaml.

You need to identify where you can access the values of Variable1 and Variable2.

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

NOTE: Each correct selection is worth one point.

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: ▼

- 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

Reference:

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

NEW QUESTION: 19

Your on-premises network contains an Active Directory Domain Services (AD DS) domain and the devices shown in the following table.

You have a hybrid Microsoft Entra tenant that contains a synced user named User1.

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

User1 is assigned the Storage File Data SMB Share Contributor role for storage1 and storage2.

The Security settings for Share1 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](#).

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

Security

Protocol settings



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

Profile

Custom



SMB protocol versions

- ☐ SMB 2.1
☐ SMB 3.0
☒ SMB 3.1.1

SMB channel encryption

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

Authentication mechanisms

- ☐ NTLM v2
☒ Kerberos

Kerberos ticket encryption

- ☒ RC4-HMAC
☒ AES-256

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

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

Statements	Yes	No
User1 can 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: 20

You create an alert rule that has the following settings:

- * Resource: RG1
- * Condition: All Administrative operations

* Actions: Action groups configured for this alert rule: ActionGroup1

* Alert rule name: Alert1

You create an action rule that has the following settings:

* Scope: VM1

* Filter criteria: Resource Type = "Virtual Machines"

* Define on this scope: Suppression

* Suppression config: From now (always)

* Name: ActionRule1

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

Note: Each correct selection is worth one point.

Statements	Yes	No
If you start VM1, an alert is triggered.	☐	☐
If you start VM2, an alert is triggered.	☐	☐
If you add a tag to RG1, an alert is triggered.	☐	☐

Answer:

Statements	Yes	No
If you start VM1, an alert is triggered.	☐	☒
If you start VM2, an alert is triggered.	☒	☐
If you add a tag to RG1, an alert is triggered.	☐	☒

Explanation:



Statements

Yes

No

If you start VM1, an alert is triggered.

☐☐

If you start VM2, an alert is triggered.

☐☐

If you add a tag to RG1, an alert is triggered.

☐☐

Box 1:

The scope for the action rule is set to VM1 and is set to suppress alerts indefinitely.

Box 2:

The scope for the action rule is not set to VM2.

Box 3:

Adding a tag is not an administrative operation.

References:

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

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

NEW QUESTION: 21

You are evaluating the security of the network communication between the virtual machines in Sub2.

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements

Yes

No

From VM1, you can successfully ping the public IP address of VM2.

☐☐

From VM1, you can successfully ping the private IP address of VM3.

☐☐

From VM1, you can successfully ping the public IP address of VM5.

☐☐

Answer:

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

Explanation:

Yes,

Yes

No

NEW QUESTION: 22

You create an Azure subscription with Azure AD Premium P2.

You need to ensure that you can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to secure Azure roles.

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

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

Answer:

Actions

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

Answer Area

Verify your identity by using multi-factor authentication (MFA).
Consent to PIM.
Sign up PIM for Azure AD roles.

Explanation:

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

NEW QUESTION: 23

You have an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry.

You need to use the automatically generated service principal for the AKS cluster to authenticate to the Azure Container Registry.

What should you create?

- A. a secret in Azure Key Vault
- B. a role assignment
- C. an Azure AD group
- D. an Azure AD user

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

NEW QUESTION: 24

You have an Azure subscription that contains a Microsoft Defender External Attack Surface Management (Defender EASM) resource named EASM1. EASM1 has discovery enabled and contains several inventory assets.

You need to identify which inventory assets are vulnerable to the most critical web app security risks.

Which Defender EASM dashboard should you use?

- A. OWASP Top 10
- B. Attack Surface Summary
- C. GDPR Compliance
- D. Security Posture

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

NEW QUESTION: 25

You plan to configure Azure Disk Encryption for VM4. Which key vault can you use to store the encryption key?

- A. KeyVault1
- B. KeyVault3
- C. KeyVault2

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

The key vault needs to be in the same subscription and same region as the VM.

VM4 is in West US. KeyVault1 is the only key vault in the same region as the VM.

Reference:

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

NEW QUESTION: 26

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

Name	Type	Contains members
Group1	Security	Yes
Group2	Microsoft 365	No

You assign licenses to the groups as shown in the following table.

Group	License
Group1	Azure Active Directory Premium P2
Group2	Office 365 E5
Group3	Azure Active Directory Premium P2

On May 1, you delete Group1, Group2, and Group3.

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
On May 3, you can restore Group1.	☐	☐
On May 15, you can restore Group2.	☐	☐
On June 3, you can restore Group3.	☐	☐

Answer Area

Statements	Yes	No
On May 3, you can restore Group1.	☐	☐
On May 15, you can restore Group2.	☐	☐
On June 3, you can restore Group3.	☐	☐

Explanation:
Answer Area

Statements	Yes	No
On May 3, you can restore Group1.	☒	☐
On May 15, you can restore Group2.	☒	☐
On June 3, you can restore Group3.	☒	☐

NEW QUESTION: 27

You have the Azure virtual networks shown in the following table.

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

You have the Azure virtual machines shown in the following table.

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

The firewalls on all the virtual machines allow ping traffic.

NSG1 is configured as shown in the following exhibit.

Inbound security rules

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

Outbound security rules

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

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

NOTE: Each correct selection is worth one point.

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

Answer:

Statements	Yes	No
VM1 can ping VM3 successfully.	☒	☐
VM2 can ping VM4 successfully.	☐	☒
VM3 can be accessed by using Remote Desktop from the Internet.	☒	☐

Explanation:

Statements	Yes	No
VM1 can ping VM3 successfully.	☒	☐
VM2 can ping VM4 successfully.	☐	☒
VM3 can be accessed by using Remote Desktop from the Internet.	☒	☐

Box 1: Yes

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

Box 2: No

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

Box 3: Yes

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

NEW QUESTION: 28

You have an Azure subscription and the computers shown in the following table.

Name	Operating system	Description
VM1	Windows Server 2012 R2	Azure virtual machine
VM2	Red Hat Enterprise Linux (RHEL) 8.2	Azure virtual machine
Server1	Windows Server 2019	On-premises physical computer connected to Microsoft Defender for Cloud
VMSS1_0	Windows Server 2022	Azure virtual machine in a virtual machine scale set

You need to perform a vulnerability scan of the computers by using Microsoft Defender for Cloud. Which computers can you scan?

- A. VM1 only
- B. Server1 and VMSS1.0 only
- C. VM1, VM2, and Server1 only
- D. VM1, VM2, Server1, and VMSS1.0
- E. VM1 and VM2 only

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

NEW QUESTION: 29

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription that contains an Azure Kubernetes Service (AKS) cluster named AKS1 and an Azure container registry named AZCR1.

You need to ensure that AKS1 can deploy container images stored in AZCR1.

Solution: You assign the Kubernetes Agentless Operator role to the system-assigned managed identity of the agent pool for AKS1.

Does this meet the requirement?

- A. Yes
- B. No

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

NEW QUESTION: 30

You have an Azure subscription named Subscription1 that contains a resource group named RG1 and a user named User1. User1 is assigned the Owner role for RG1.

You create an Azure Blueprints definition named Blueprint1 that includes a resource group named RG2 as shown in the following exhibit.

Edit blueprint

Basics Artifacts

Add artifacts to the blueprint. Add resource groups to organize where the artifacts should be deployed and assigned.

NAME	ARTIFACT TYPE	PARAMETERS
▼  Subscription		 Microsoft
✚ Add artifact...		
▼  RG2	Resource group	2 out of 2 parameters populated
 User1 (User1@sk200628outlook.onmicrosoft.com) : Tag Contributor	Role assignment	1 out of 1 parameters populated
✚ Add artifact...		

You assign Blueprint1 to Subscription1 by using the following settings:

- * Lock assignment: Read Only
- * Managed Identity: System assigned

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
A locking mode of Read Only will be assigned to RG1.	☐	☐
User1 can add tags to RG2.	☐	☐
You can remove User1 from the Tag Contributor role for RG2.	☐	☐

Answer:

Statements	Yes	No
A locking mode of Read Only will be assigned to RG1.	☒	☐
User1 can add tags to RG2.	☒	☐
You can remove User1 from the Tag Contributor role for RG2.	☐	☒

Explanation:

Graphical user interface, text, application Description automatically generated

Statements	Yes	No
A locking mode of Read Only will be assigned to RG1.	☒	☐
User1 can add tags to RG2.	☒	☐
You can remove User1 from the Tag Contributor role for RG2.	☐	☒

Reference:

NEW QUESTION: 31

Your company uses cloud-based resources from the following platforms:

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

You plan to implement Microsoft Defender for Cloud.

On which platforms can you use Defender for Cloud to protect containers and storage? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Containers:

- Azure only
- Azure and AWS only
- Azure and GCP only
- Azure, AWS, and GCP**

Storage:

- Azure only
- Azure and AWS only
- Azure and GCP only
- Azure, AWS, and GCP**

Answer:

Answer Area

Containers:

- Azure only
- Azure and AWS only
- Azure and GCP only
- Azure, AWS, and GCP**

Storage:

- Azure only
- Azure and AWS only
- Azure and GCP only
- Azure, AWS, and GCP**

Explanation:

Answer Area

Containers:

Storage:

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam!
Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (497 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 32

You have 10 virtual machines on a single subnet that has a single network security group (NSG). You need to log the network traffic to an Azure Storage account.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Install the Network Performance Monitor solution.
- B. Enable Azure Network Watcher.
- C. Enable diagnostic logging for the NSG.
- D. Enable NSG flow logs.
- E. Create an Azure Log Analytics workspace.

Answer: D (LEAVE A REPLY)

A network security group (NSG) enables you to filter inbound traffic to, and outbound traffic from, a virtual machine (VM). You can log network traffic that flows through an NSG with Network Watcher's NSG flow log capability. Steps include:

- * Create a VM with a network security group
- * Enable Network Watcher and register the Microsoft.Insights provider
- * Enable a traffic flow log for an NSG, using Network Watcher's NSG flow log capability
- * Download logged data
- * View logged data

Reference:

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

NEW QUESTION: 33

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

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

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

Assignment☐ Allow permanent eligible assignment

Expire eligible assignments after

3 Months ☐ Allow permanent active assignment

Expire active assignments after

1 Month ☒ Require Multi-Factor Authentication on active assignment☒ Require justification on active assignment**Activation**

Activation maximum duration (hours)

 8☒ Require Multi-Factor Authentication on activation☒ Require justification on activation☐ Require ticket information on activation☐ Require approval to activate Select approversNo member or group selected 

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

Name	Assignment type
User1	Eligible
User2	Active
User3	Active

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

NOTE: Each correct selection is worth one point.

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

Answer:

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

Explanation:

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

References:

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

NEW QUESTION: 34

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

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

You create the Azure policy shown in the following exhibit.

Basics Parameters Remediation Non-compliance messages Review + create

Basics

Scope Azure Pass - Sponsorship/RG1

Exclusions Azure Pass - Sponsorship/RG1/NSG1

Policy definition Flow logs should be enabled for every network security group

Assignment name Flow logs should be enabled for every network security group

Description Description1

Policy enforcement Enabled

Assigned by Admin1

Parameters

effect Audit

Remediation

Create managed identity Yes

Managed identity location westeurope

Create a remediation task No

Non-compliance messages

Default non-compliance message Message1

You assign the policy to RG1.

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

- A. Flow logs will be enabled for NSG1 and NSG2.
- B. Flow logs will be enabled for NSG2 only.
- C. Flow logs will be enabled for NSG1 only.
- D. Flow logs will be disabled for NSG1 and NSG2.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 35

You plan to use Azure Log Analytics to collect logs from 200 servers that run Windows Server 2016.

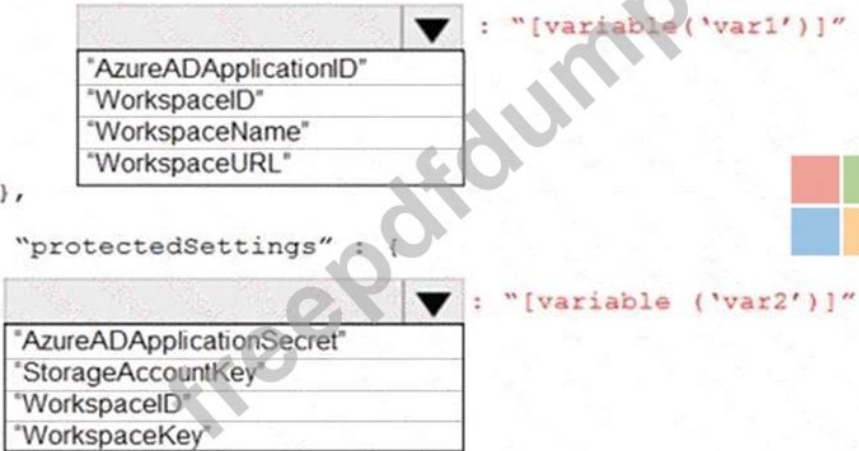
You need to automate the deployment of the Microsoft Monitoring Agent to all the servers by using an Azure Resource Manager template.

How should you complete the template? To answer, select the appropriate options in the answer

area.

NOTE: Each correct selection is worth one point.

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



Answer:

```

{
  "type" : "Microsoft.Compute/virtualMachines/extensions",
  "name" : "[concat(parameter('vmName'), '/OMSExtension')]",
  "apiVersion" : "[variables('apiVersion')]",
  "location" : "[resourceGroup().location]",
  "dependsOn" : [
    "[concat('Microsoft.Compute/virtualMachines/', parameters('vmName'))]"
  ],
  "properties" : {
    "publisher" : "Microsoft.EnterpriseCloud.Monitoring",
    "type" : "MicrosoftMonitoringAgent",
    "typeHandlerVersion" : "1.0",
    "autoUpgradeMinorVersion" : true,
    "settings" : {
      

|                        |   |                        |
|------------------------|---|------------------------|
|                        | ▼ | : "[variable('var1')]" |
| "AzureADApplicationID" |   |                        |
| "WorkspaceID"          |   |                        |
| "WorkspaceName"        |   |                        |
| "WorkspaceURL"         |   |                        |


    },
    "protectedSettings" : {
      

|                            |   |                        |
|----------------------------|---|------------------------|
|                            | ▼ | : "[variable('var2')]" |
| "AzureADApplicationSecret" |   |                        |
| "StorageAccountKey"        |   |                        |
| "WorkspaceID"              |   |                        |
| "WorkspaceKey"             |   |                        |


    }
  }
}

```

Explanation:

```

},
"properties" : {
  "publisher" : "Microsoft.EnterpriseCloud.Monitoring",
  "type" : "MicrosoftMonitoringAgent",
  "typeHandlerVersion" : "1.0",
  "autoUpgradeMinorVersion" : true,
  "settings" : {
    : "[variable('var1')]"
    "AzureADApplicationID"
    "WorkspaceID"
    "WorkspaceName"
    "WorkspaceURL"
  },
  "protectedSettings" : {
    : "[variable ('var2')]"
    "AzureADApplicationSecret"
    "StorageAccountKey"
    "WorkspaceID"
    "WorkspaceKey"
  }
}

```

References:

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

NEW QUESTION: 36

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

Name	Operating system
VM1	Windows 10
VM2	Windows Server 2016
VM3	Windows Server 2019
VM4	Ubuntu Server 18.04 LTS

You create an MDM Security Baseline profile named Profile1.

You need to identify to which virtual machines Profile1 can be applied.

Which virtual machines should you identify?

- A. VM1 only
- B. VM1, VM2, and VM3 only
- C. VM1 and VM3 only

D. VM1, VM2, VM3, and VM4

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

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines>

NEW QUESTION: 37

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

Name	Type	In resource group
cont1	Container instance	RG1
VNET1	Virtual network	RG1
App1	App Service app	RG1
VM1	Virtual machine	RG1
User1	User	Not applicable

You create a custom RBAC role in Subscription1 by using the following JSON file.

```
{
  "Name": "Role1",
  "IsCustom": true,
  "Description": "Role1 description",
  "Actions": [
    "*/Read",
    "Microsoft.Compute/*"
  ],
  "NotActions": [],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "/subscriptions/923a419a-4358-40fb-b4a9-b8af43dd0c92/resourceGroups/RG1"
  ]
}
```

You assign Role1 to User1 on RG1.

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

NOTE: Each correct selection is worth one point.

Microsoft Statements

	Yes	No
User1 can add VM1 to VNET1.	☐	☐
User1 can start and stop App1.	☐	☐
User1 can start and stop cont1.	☐	☐

Answer:

Microsoft Statements	Yes	No
User1 can add VM1 to VNET1.	☐	☒
User1 can start and stop App1.	☐	☒
User1 can start and stop cont1.	☐	☒

Explanation:

Text Description automatically generated

Statements	Yes	No
User1 can add VM1 to VNET1.	☐	☒
User1 can start and stop App1.	☐	☒
User1 can start and stop cont1.	☐	☒

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompute>

NEW QUESTION: 38

You have an Azure subscription that contains a virtual network named VNet1. The subscription contains an Azure App Service web app named App1.

You have an Azure Front Door profile named AFD1 that has an Azure Web Application Firewall

(WAF) policy.

You need to ensure that all inbound traffic to App1 is filtered through AFD1.

What should you do?

- A. Configure Microsoft Entra application proxy.
- B. For VNet1, configure network security group (NSG) rules.
- C. For App1, enable virtual network integration.
- D. For App1, configure the HTTP headers filter settings.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 39

You have the Azure virtual machines shown in the following table.

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

For which virtual machine can you enable Update Management?

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

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

References:

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

NEW QUESTION: 40

You have a Microsoft 365 tenant that uses an Azure Active Directory (Azure AD) tenant. The Azure AD tenant syncs to an on-premises Active Directory domain by using an instance of Azure AD Connect.

You create a new Azure subscription.

You discover that the synced on-premises user accounts cannot be assigned roles in the new subscription.

You need to ensure that you can assign Azure and Microsoft 365 roles to the synced Azure AD user accounts.

What should you do first?

- A. Change the Azure AD tenant used by the new subscription.
- B. Configure the Azure AD tenant used by the new subscription to use pass-through authentication.
- C. Configure a second instance of Azure AD Connect.

D. Configure the Azure AD tenant used by the new subscription to use federated authentication.

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

NEW QUESTION: 41

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure Subscription. The subscription contains 50 virtual machines that run Windows Server

2012 R2 or Windows Server 2016.

You need to deploy Microsoft Antimalware to the virtual machines.

Solution: You connect to each virtual machine and add a Windows feature.

Does this meet the goal?

A. Yes

B. No

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: 42

You need to configure WebApp1 to meet the data and application requirements.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Upload a public certificate.

B. Turn on the HTTPS Only protocol setting.

C. Set the Minimum TLS Version protocol setting to 1.2.

D. Change the pricing tier of the App Service plan.

E. Turn on the Incoming client certificates protocol setting.

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

Refer <https://docs.microsoft.com/en-us/azure/app-service/app-service-web-configure-tls-mutual-auth>

NEW QUESTION: 43

You have an Azure subscription.

You create a new virtual network named VNet1.

You plan to deploy an Azure web app named App1 that will use VNet1 and will be reachable by using private IP addresses. The solution must support inbound and outbound network traffic.

What should you do?

- A. Create an Azure application gateway.
- B. Configure regional virtual network integration.
- C. Create an App Service Environment
- D. Create an Azure App Service Hybrid Connection.

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

NEW QUESTION: 44

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

What should you do?

- A. Add a membership rule to Group1.
- B. Delete Group1. Create a new group named Group1 that has a membership type of Office 365. Add users and devices to the group.
- C. Modify the membership rule of Group1.
- D. Change the membership type of Group1 to Assigned. Create two groups that have dynamic memberships. Add the new groups to Group1.

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

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

Litware identifies the following identity and access requirements: All San Francisco users and their devices must be members of Group1.

The tenant currently contain this group:

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

References:

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

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-create-azure-portal>

NEW QUESTION: 45

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

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

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

Answer 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.	☐	☐

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	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.	☐	☒

NEW QUESTION: 46

You are evaluating the security of the network communication between the virtual machines in Sub2.

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

NOTE: Each correct selection is worth one point.

Answer Area

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

Answer:

Answer Area

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

Explanation:

Q1: No { and it should not be allowed as only TCP 80 is allowed from the "Internet" service tag

Q2: Yes {as it should be for VMs in the same local subnet pinging each other on private IP and no NSG configured}

Q3: Yes {VM5 is in subnet where 1st rule of NSG allows any traffic from any source to the destination}

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam!

Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (497 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 47

You need to perform the planned changes for OU2 and User1.

Which tools should you use? To answer, drag the appropriate tools to the correct resources. Each tool may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Tools	Answer Area
The Azure portal	OU2: Tool
Azure AD Connect	User1: Tool
The Active Directory admin center	
Active Directory Sites and Services	
Active Directory Users and Computers	



Answer:

Tools

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

Answer Area

OU2:	Azure AD Connect
User1:	The Azure portal

Explanation:

Table Description automatically generated

OU2:	Azure AD Connect
User1:	The Azure portal

NEW QUESTION: 48

You have an Azure subscription that contains a user named User1 and an Azure Container Registry named ConReg1.

You enable content trust for ConReg1.

You need to ensure that User1 can create trusted images in ConReg1. The solution must use the principle of least privilege.

Which two roles should you assign to User1? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. AcrQuarantineReader
- B. Contributor
- 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: 49

You have an Azure Sentinel deployment.

You need to create a scheduled query rule named Rule1.

What should you use to define the query rule logic for Rule1?

- A. a Transact-SQL statement
- B. a JSON definition
- C. GraphQL
- D. a Kusto query

Answer: ([SHOW ANSWER](#))

Reference:

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

NEW QUESTION: 50

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You use Azure Security Center for the centralized policy management of three Azure subscriptions.

You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create a policy definition and assignments that are scoped to resource groups.

Does this meet the goal?

- A. Yes
- B. No

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

References:

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

NEW QUESTION: 51

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

Name	Type
Key1	Key
Secret1	Secret
Cert1	Certificate

Which resources support the creation of a rotation policy?

- A. Key1, Secret1, and Cert1
- B. Key1 and Cert1 only
- C. Key 1 only
- D. Secret1 and Cert1 only
- E. Cert1 only
- F. Key1 and Secret1 only

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

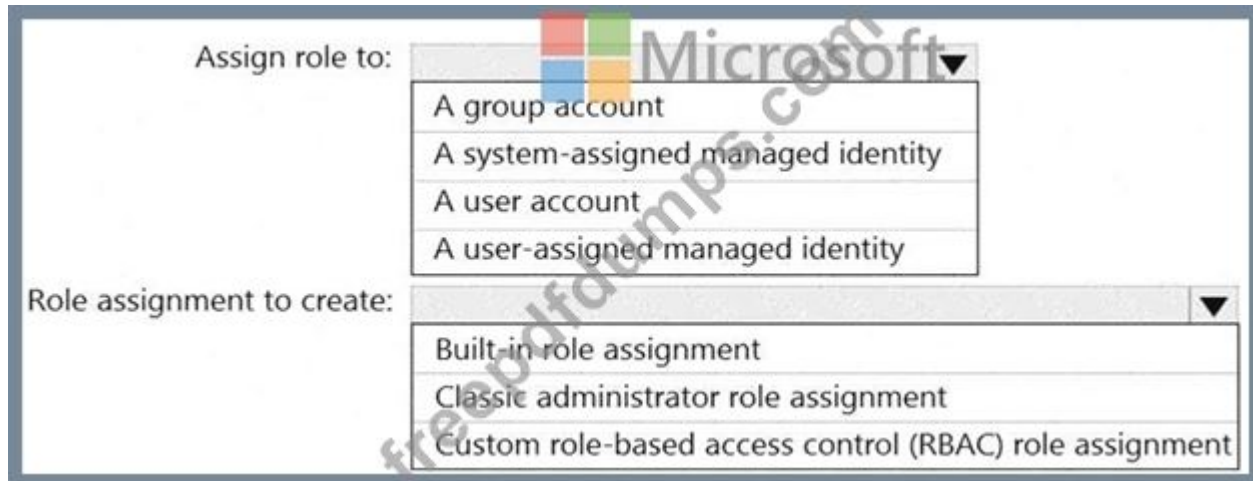
NEW QUESTION: 52

You plan to implement an Azure function named Function1 that will create new storage accounts for containerized application instances.

You need to grant Function1 the minimum required privileges to create the storage accounts. The solution must minimize administrative effort.

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

NOTE: Each correct selection is worth one point.



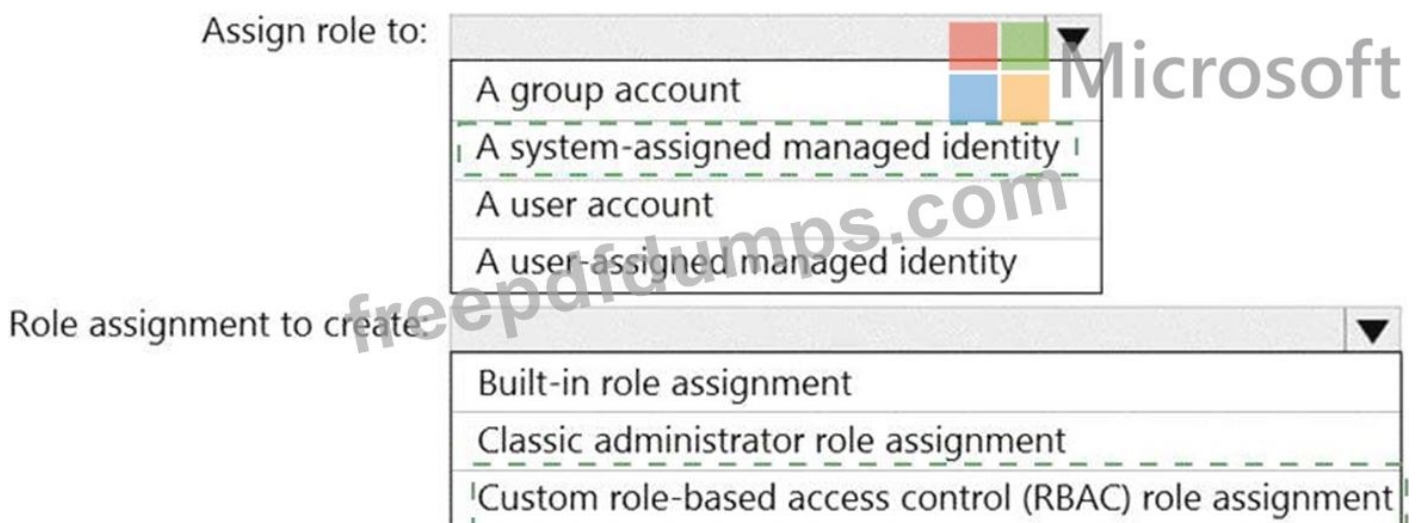
Assign role to:

- A group account
- A system-assigned managed identity
- A user account
- A user-assigned managed identity

Role assignment to create:

- Built-in role assignment
- Classic administrator role assignment
- Custom role-based access control (RBAC) role assignment

Answer:



Assign role to:

- A group account
- A system-assigned managed identity
- A user account
- A user-assigned managed identity

Role assignment to create:

- Built-in role assignment
- Classic administrator role assignment
- Custom role-based access control (RBAC) role assignment

Explanation:

Assign role to:

- A group account
- A system-assigned managed identity
- A user account
- A user-assigned managed identity

Role assignment to create:

- Built-in role assignment
- Classic administrator role assignment
- Custom role-based access control (RBAC) role assignment

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/howto-assign-access-portal>

NEW QUESTION: 53

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

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

You create an Azure Log Analytics workspace named Analytics1 in RG1 in the East US region. Which virtual machines can be enrolled in Analytics1?

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

Answer: C (LEAVE A REPLY)

Note: Create a workspace

* In the Azure portal, click All services. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics.

* Click Create, and then select choices for the following items:

Provide a name for the new Log Analytics workspace, such as DefaultLAWorkspace. OMS workspaces are now referred to as Log Analytics workspaces.

Select a Subscription to link to by selecting from the drop-down list if the default selected is not appropriate.

For Resource Group, select an existing resource group that contains one or more Azure virtual machines.

Select the Location your VMs are deployed to. For additional information, see which regions Log Analytics is available in.

References:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/manage-access>

NEW QUESTION: 54

You are evaluating the effect of the application security groups on the network communication between the virtual machines in Sub2.

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

NOTE: Each correct selection is worth one point.

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

Answer:

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

Explanation:

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

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

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

is allowed from ASG1.

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

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

Box 2: Yes.

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

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

NEW QUESTION: 55

You have an Azure subscription that contains a virtual network named VNet1 VNet1 contains a single subnet.

The subscription contains a virtual machine named VM1 that is connected to VNet1.

You plan to deploy an Azure SQL managed instance named SQL1.

You need to ensure that VM1 can access SQL1.

Which three components should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a route table
- B. a virtual network gateway
- C. a subnet
- D. a network security group (NSG)
- E. a network security perimeter

Answer: A,C,D (LEAVE A REPLY)

NEW QUESTION: 56

You have an Azure subscription that contains 100 virtual machines and has Azure Security Center Standard tier enabled.

You plan to perform a vulnerability scan of each virtual machine.

You need to deploy the vulnerability scanner extension to the virtual machines by using an Azure Resource Manager template.

Which two values should you specify in the code to automate the deployment of the extension to the virtual machines? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. the user-assigned managed identity
- B. the Key Vault managed storage account key
- C. the Azure Active Directory (Azure AD) ID
- D. the workspace ID
- E. the primary shared key
- F. the system-assigned managed identity

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 57

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

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

You have an Azure Cosmos DB account named cosmos1 configured as shown in the following exhibit.

Allow access from
☐ All networks ☒ Selected networks

[Configure network security for your Azure 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	Yes	No
VM1 can access cosmos1 over the internet.	☒	☐
VM2 can access cosmos1 over the internet.	☒	☐
VM3 can access cosmos1 over the internet.	☐	☒

Explanation:

Yes, Yes, No

NEW QUESTION: 58

You have an Azure Sentinel workspace that contains an Azure Active Directory (Azure AD) connector, an Azure Log Analytics query named Query1 and a playbook named Playbook1. Query1 returns a subset of security events generated by Azure AD.

You plan to create an Azure Sentinel analytic rule based on Query1 that will trigger Playbook1. You need to ensure that you can add Playbook1 to the new rule. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Create the rule and set the type to:

- Fusion
- Microsoft Security incident creation
- Scheduled

Configure the playbook to include:

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

Answer:

Create the rule and set the type to:

- Fusion
- Microsoft Security incident creation
- Scheduled

Configure the playbook to include:

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

Explanation:

Create the rule and set the type to:

Microsoft

Configure the playbook to include:

Fusion

Microsoft Security incident creation

Scheduled

A managed connector

A system-assigned managed identity

A trigger

Diagnostic settings

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: 59

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com.

The company is developing an application named App1. App1 will run as a service on server that runs Windows Server 2016. App1 will authenticate to contoso.com and access Microsoft Graph to read directory data.

You need to delegate the minimum required permissions to App1.

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

Actions

Grant permissions

Add a delegated permission.

Configure Azure AD Application Proxy

Add an application permission.

Create an app registration.

Answer Area

Microsoft

freepdfdumps.com

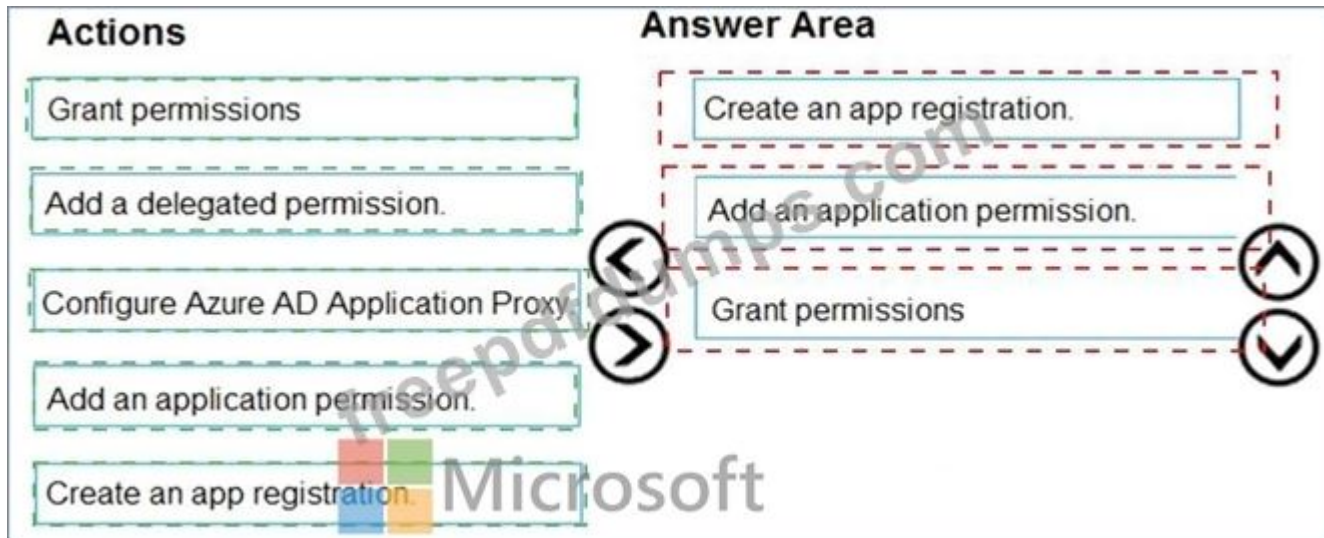
←

→

↑

↓

Answer:



Explanation:



Step 1: Create an app registration

First the application must be created/registered.

Step 2: Add an application permission

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

Step 3: Grant permissions

References:

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

NEW QUESTION: 60

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

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

Microsoft

You configure the Temporary Access Pass settings as shown in the following exhibit.

Temporary Access Pass settings Microsoft

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



You add the Temporary Access Pass authentication method to Admin2.

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

NOTE: Each correct selection is worth one point.

Answer Area



Statements

Yes

No

Admin1 can view the Temporary Access Pass of Admin2.

☐☐

Admin2 can add the Temporary Access Pass authentication method to User1.

☐☐

Admin2 can add the Temporary Access Pass authentication method to Admin1.

☐☐

Answer:

Answer Area

Statements

Yes

No

Admin1 can view the Temporary Access Pass of Admin2.

☐☒

Admin2 can add the Temporary Access Pass authentication method to User1.

☒☐

Admin2 can add the Temporary Access Pass authentication method to Admin1.

☐☒

Explanation:

Answer Area		Microsoft	Yes	No
Statements	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: 61

You create an Azure subscription.

You need to ensure that you can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to secure Azure AD roles.

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

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

Answer:

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

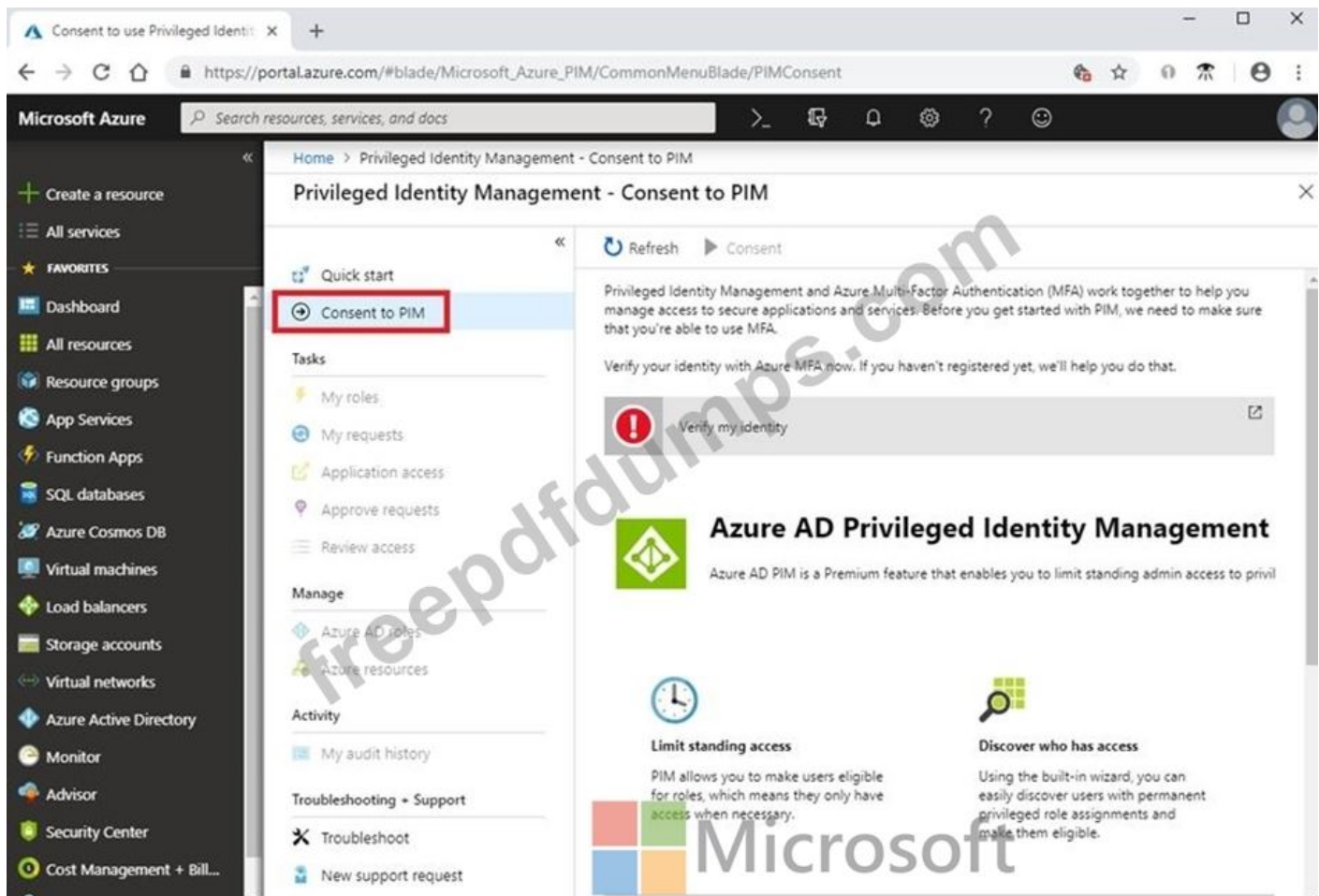
Explanation:

Consent to PIM.

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

Sign up PIM for Azure AD roles.

Step 1: Consent to PIM



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

Step 3: Sign up PIM for Azure AD roles

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

References:

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

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam!

Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (497 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 62

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets

might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure Subscription named Sub1.

You have an Azure Storage account named Sa1 in a resource group named RG1.

Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.

You discover that unauthorized users accessed both the file service and the blob service.

You need to revoke all access to Sa1.

Solution: You create a new stored access policy.

Does this meet the goal?

A. Yes

B. No

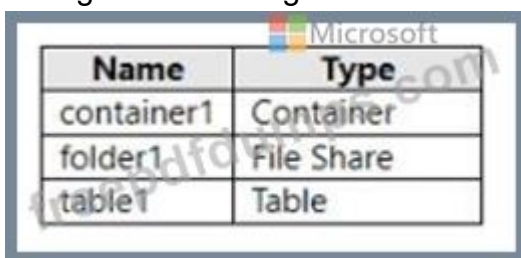
Answer: B ([LEAVE A REPLY](#))

Shared access signatures provides access to a particular resource such as blog. Stored access policies are a group of Shared Access Signatures (SAS). In order to revoke access to a SAS you can either:

1. Rotate the Key1 or Key 2, that is the access keys used to sign the SAS. Rotating the access keys used to sign the SAS, invalidates any previously signed SAS hence revoking the SAS issued before
2. Remove the stored access policy which an SAS is linked to. If a Stored Access Policy is removed, it also invalidates the SASs liked to the Stored Access Policy.

NEW QUESTION: 63

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



The image shows a screenshot of a table with two columns: 'Name' and 'Type'. The table lists three resources: 'container1' (Container), 'folder1' (File Share), and 'table1' (Table). The screenshot has a Microsoft logo and a watermark in the background.

Name	Type
container1	Container
folder1	File Share
table1	Table

In storage1, you create a shared access signature (SAS) named SAS1 as shown in the following exhibit.

Allowed services ⓘ
☐ Blob ☒ File ☐ Queue ☐ Table

Allowed resource types ⓘ
☒ Service ☒ Container ☒ Object

Allowed permissions ⓘ
☒ Read ☒ Write ☒ Delete ☒ List ☐ Add ☒ Create ☐ Update ☐ Process ☐ Immutable storage

Allowed blob index permissions ⓘ
☐ Read/Write ☐ Filter

Start and expiry date/time ⓘ
 Start
 End

Allowed IP addresses ⓘ

Allowed protocols ⓘ
☒ HTTPS only ☐ HTTPS and HTTP

Preferred routing tier ⓘ
☒ Basic (default) ☐ Microsoft network routing ☐ Internet routing

i Some routing options are disabled because the endpoints are not published.

Signing key ⓘ

Generate SAS and connection string

To which resources can User1 write on July 1, 2022 by using SAS1 and key 1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

SAS1:

Key1:

Answer:

Answer Area



Explanation:



NEW QUESTION: 64

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You use Azure Security Center for the centralized policy management of three Azure subscriptions.

You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create an initiative and an assignment that is scoped to a management group.

Does this meet the goal?

A. Yes

B. No

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

References:

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

NEW QUESTION: 65

You have an Azure subscription that uses Microsoft Defender for Cloud.

You have an Amazon Web Services (AWS) account.

You need to ensure that when you deploy a new AWS Elastic Compute Cloud (EC2) instance, the Microsoft Defender for Servers agent installs automatically.

What should you configure first?

- A. the classic cloud connector
- B. the log Analytics agent
- C. the native cloud connector
- D. the Azure Monitor agent

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 66

You have an Azure Container Registry named Registry1.

You add role assignment for Registry1 as shown in the following table.

User	Role
User1	AcrPush
User2	AcrPull
User3	AcrImageSigner
User4	Contributor

Which users can upload images to Registry1 and download images from Registry1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Upload images: ▼

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

Download images: ▼

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

Answer:

Upload images: ▼

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

Download images: ▼

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

Explanation:

Upload images: ▼

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

Download images: ▼

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

Box 1: User1 and User4 only

Owner, Contributor and AcrPush can push images.

Box 2: User1, User2, and User4

All, except AcrImagineSigner, can download/pull images.

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

References:

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

NEW QUESTION: 67

You have an Azure subscription.

You create an Azure Firewall policy that has the rules shown in the following table:

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

In which order should the rules be processed? To answer, move all rules from the list of rules to the answer area and arrange them in the correct order.

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: 68

You need to create an Azure key vault. The solution must ensure that any object deleted from the key vault be retained for 90 days.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

The screenshot shows the command `New-AzureRmKeyVault -VaultName 'KeyVault1' -ResourceGroupName 'RG1'` followed by `-Location 'East US'` and an unlabeled dropdown menu. The dropdown menu is open, showing the following options: `-EnabledForDeployment`, `-EnablePurgeProtection`, `-Tag`, `-Confirm`, `-DefaultProfile`, `-EnableSoftDelete`, and `-SKU`.

Answer:

The screenshot shows the command `New-AzureRmKeyVault -VaultName 'KeyVault1' -ResourceGroupName 'RG1'` followed by `-Location 'East US'` and an unlabeled dropdown menu. The dropdown menu is open, showing the following options: `-EnabledForDeployment`, `-EnablePurgeProtection`, `-Tag`, `-Confirm`, `-DefaultProfile`, `-EnableSoftDelete`, and `-SKU`.

Explanation:

The screenshot shows the command `New-AzureRmKeyVault -VaultName 'KeyVault1' -ResourceGroupName 'RG1'` followed by `-Location 'East US'` and an unlabeled dropdown menu. The dropdown menu is open, showing the following options: `-EnabledForDeployment`, `-EnablePurgeProtection`, `-Tag`, `-Confirm`, `-DefaultProfile`, `-EnableSoftDelete`, and `-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: 69

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

You need to create a custom Azure role-based access control (RBAC) role that will delegate permissions to manage the tags on all the objects in Group1.

What should you include in the role definition of Role1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



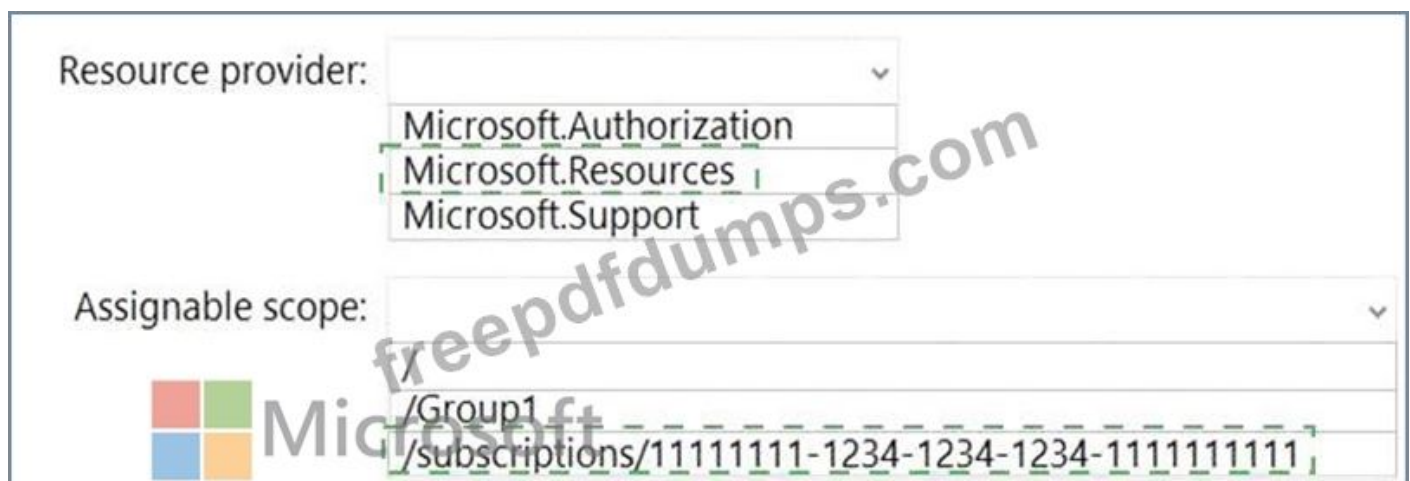
Resource provider: Microsoft

- Microsoft.Authorization
- Microsoft.Resources
- Microsoft.Support

Assignable scope: /

- /Group1
- /subscriptions/11111111-1234-1234-1111111111

Answer:



Resource provider: Microsoft

- Microsoft.Authorization
- Microsoft.Resources
- Microsoft.Support

Assignable scope: /

- /Group1
- /subscriptions/11111111-1234-1234-1111111111

Explanation:

Text, application Description automatically generated

Resource provider:

Microsoft.Authorization
Microsoft.Resources
Microsoft.Support

Assignable scope:

/

/Group1

/subscriptions/11111111-1234-1234-1234-111111111111

Note: Assigning a custom RBAC role as the Management Group level is currently in preview only. So, for now the answer to the assignable scope is the subscription level.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations>

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

<https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal#step-5-assignable-scopes>

NEW QUESTION: 70

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

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

From Azure AD Privileged Identity Management (PIM), you configure the settings for the Security Administrator role as shown in the following exhibit.

Assignment☒ Allow permanent eligible assignment

Expire eligible assignments after

3 Months

☒ Allow permanent active assignment

Expire active assignments after

1 Month

☐ Require Azure Multi-Factor Authentication on active assignment☒ Require justification on active assignment**Activation**

Activation maximum duration (hours)



5

☐ Require Azure Multi-Factor Authentication on activation☐ Require justification on activation☐ Require ticket information on activation☐ Require approval to activate

* Select approvers

No member or group selected



From PIM, you assign the Security Administrator role to the following groups:

* Group1: Active assignment type, permanently assigned

* Group2: Eligible assignment type, permanently eligible

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	☐	☐
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	☐	☐
User3 can activate the Security Administrator role.	☐	☐

Answer:

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	☐	☐
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	☐	☐
User3 can activate the Security Administrator role.	☐	☐

Explanation:

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	☐	☒
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	☒	☐
User3 can activate the Security Administrator role.	☐	☒

Box 1: Yes

Eligible Type: A role assignment that requires a user to perform one or more actions to use the role. If a user has been made eligible for a role, that means they can activate the role when they need to perform privileged tasks. There's no difference in the access given to someone with a permanent versus an eligible role assignment. The only difference is that some people don't need that access all the time.

You can choose from two assignment duration options for each assignment type (eligible and active) when you configure settings for a role. These options become the default maximum duration when a user is assigned to the role in Privileged Identity Management.

Use the Activation maximum duration slider to set the maximum time, in hours, that a role stays active before it expires. This value can be from one to 24 hours.

Box 2: Yes

Active Type: A role assignment that doesn't require a user to perform any action to use the role. Users assigned as active have the privileges assigned to the role
Box 3: Yes User3 is member of Group2.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

<https://docs.microsoft.com/bs-cyrl-ba/azure/active-directory/privileged-identity-management/pim-resource-roles-configure-role-settings>

NEW QUESTION: 71

You have an on-premises datacenter that contains multiple servers.

You have an Azure subscription.

You plan to onboard the on-premises servers to Microsoft Defender for Cloud by using a script.

You need to create an identity to enable the script to run without prompting for Microsoft Entra credentials.

Which type of identity should you create?

A. system-assigned managed identity

B. service principal

C. user account

D. user-assigned managed identity

E. group account

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

NEW QUESTION: 72

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.

com. The tenant contains the users shown in the following table.

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

You create a resource group named RG1.

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

NOTE: Each correct selection is worth one point.

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



Microsoft

Explanation:

Users who can modify the permissions for RG1:

Microsoft

- 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: 73

You have an Azure subscription that contains an Azure SQL database named SQL1.

You plan to deploy a web app named App1.

You need to provide App1 with read and write access to SQL1. The solution must meet the following requirements:

- * Provide App1 with access to SQL1 without storing a password.
- * Use the principle of least privilege.
- * Minimize administrative effort.

Which type of account should App1 use to access SQL1, and which database roles should you assign to App1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Account type: ▼

- Azure Active Directory User
- Managed identity
- Service Principal

Roles: ▼

- db_datawriter only
- db_datareader and db_datawriter
- db owner only

Answer:

Account type:  ▼

- Azure Active Directory User
- Managed identity
- Service Principal

Roles: ▼

- db_datawriter only
- db_datareader and db_datawriter
- db owner only

Explanation:

Graphical user interface, text, application Description automatically generated

Account type:

▼

Azure Active Directory User

Managed identity

Service Principal

Roles:

▼

db_datawriter only

db_datareader and db_datawriter

db owner only



Reference:

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

NEW QUESTION: 74

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

Name	Scoped to
Role1	MG1
Role2	RG1

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

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

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

Name	Role
User1	Role1
User2	Role1, Role2
User3	Role2

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

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: 75

You have an Azure subscription that contains a Microsoft Defender External Attack Surface Management (Defender EASM) resource named EASM1. You review the Attack Surface Summary dashboard. You need to identify the following insights:

- * Deprecated technologies that are no longer supported
- * Infrastructure that will soon expire

Which section of the dashboard should you review?

- A. attack surface composition
- B. Securing the Cloud
- C. Sensitive Services
- D. Attack Surface Priorities

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 76

You have an Azure subscription that contains a storage account and an Azure web app named App1.

App1 connects to an Azure Cosmos DB database named Cosmos1 that uses a private endpoint named Endpoint1. Endpoint1 has the default settings.

You need to validate the name resolution to Cosmos1.

Which DNS zone should you use?

- A. Endpoint1. Privatelink, blob, core, windows, net
- B. Endpoint1. Privatelink, azurewebsites, net
- C. Endpoint1. Privatelink, documents, azure, com
- D. Endpoint1. Privatelink, database, azure, com

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

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam!

Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (497 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 77

You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1.

You have 100 on-premises servers that run Windows Server 2012 R2 and Windows Server 2016. The servers connect to LAW1. LAW1 is configured to collect security-related performance counters from the connected servers.

You need to configure alerts based on the data collected by LAW1. The solution must meet the following requirements:

- * Alert rules must support dimensions.
- * The time it takes to generate an alert must be minimized.
- * Alert notifications must be generated only once when the alert is generated and once when the alert is resolved.

Which signal type should you use when you create the alert rules?

- A. Log
- B. Log (Saved Query)
- C. Metric
- D. Activity Log

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

Metric alerts in Azure Monitor provide a way to get notified when one of your metrics cross a threshold.

Metric alerts work on a range of multi-dimensional platform metrics, custom metrics, Application Insights standard and custom metrics.

Note: Signals are emitted by the target resource and can be of several types. Metric, Activity log,

Application Insights, and Log.

References:

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

NEW QUESTION: 78

Lab Task

Task 3

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

Answer:

see the task answer with step by step below:

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

NEW QUESTION: 79

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

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

Which two settings should you use? To answer, select the appropriate settings in the answer area

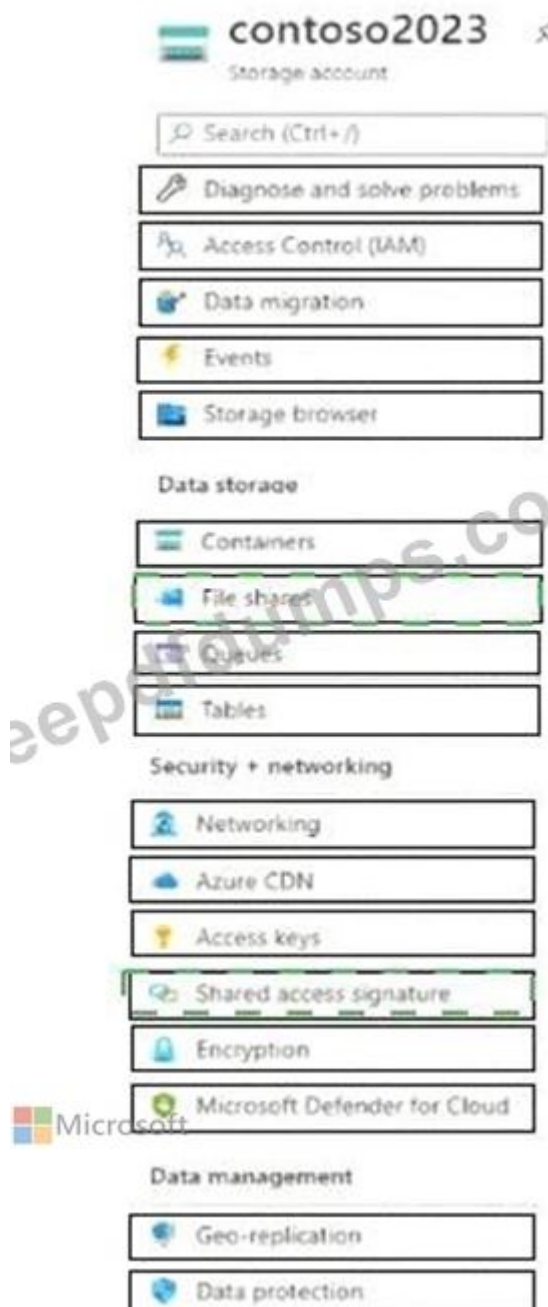
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Explanation:

A screenshot of a computer Description automatically generated

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

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

2. Share access signature

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

NEW QUESTION: 80

Lab Task

use the following login credentials as needed:

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

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

Azure Username: User1-28681041@ExamUsers.com

Azure Password: GpOAe4@IDg

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

The following information is for technical support purposes only:

Lab Instance: 28681041

Task 3

The developers at your company plan to create a web app named App28681041 and to publish the app to

<https://www.contoso.com>. You need to perform the following tasks:

- * Ensure that App28681041 is registered to Azure AD.
- * Generate a password for App28681041.

Answer:

Check below steps in explanation for Task.

Explanation

To register App28681041 to Azure AD and generate a password for it, you can follow these steps:

In the Azure portal, search for and select Azure Active Directory.

In the left pane, select App registrations.

Select New registration.

In the Register an application pane, enter the following information:

Name: App28681041

Supported account types: Select the appropriate account types for your scenario.

Redirect URI: Leave this field blank.

Select Register.

In the App registrations pane, select the newly created App28681041 application.

In the left pane, select Certificates & secrets.

Select New client secret.

In the Add a client secret pane, enter the following information:

Description: Enter a description for the client secret.

Expires: Select an appropriate expiration date for the client secret.

Select Add.

In the Certificates & secrets pane, copy the value of the newly created client secret.

You can find more information on this topic in the following Microsoft documentation: Quickstart: Register an application with the Microsoft identity platform.

NEW QUESTION: 81

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

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

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

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

You enable just in time (JIT) VM access for all the virtual machines.

You need to identify which virtual machines are protected by JIT.

Which virtual machines should you identify?

- A. VM4 only
- B. VM1 and VM3 only
- C. VM1, VM3 and VM4 only
- D. VM1, VM2, VM3, and 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: 82

You have a Microsoft Entra tenant named contoso.com.

You collaborate with a partner organization that has a Microsoft Entra tenant named fabrikam.com. Fabrikam.

com has multi-factor authentication (MFA) enabled for all users.

Contoso.com has the Cross-tenant access settings configured as shown in the Cross-tenant access settings exhibit. (Click the Cross-tenant access settings:

Inbound access settings

 Edit inbound defaults

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

Outbound access settings

 Edit outbound defaults

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

Contoso.com has the External collaboration settings configured as shown in the External collaboration settings exhibit. (Click the External collaboration settings tab.)

Guest user access

Guest user access restrictions

[Learn more](#)

- ☐ Guest users have the same access as members (most inclusive)
- ☐ Guest users have limited access to properties and memberships of directory objects
- ☒ Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

You create a Conditional Access policy that has the following settings:

* Name: CAPolicy1

* Assignments

o Guest or external users: B2B collaboration guest users

o Target resources

Include: All cloud apps o Access controls

Grant access

Require device to be marked as compliant

Require multi-factor authentication

Enable policy: On

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

NOTE: Each correct section is worth one point.

Answer Area

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

Answer:

Answer Area

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

Explanation:

Answer Area

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

NEW QUESTION: 83

You have an Azure subscription that uses Microsoft Defender for Cloud.

You plan to use the Secure Score Over Time workbook.

You need to configure the Continuous export settings for the Defender for Cloud data.

Which two settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.



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) ⓘ



Microsoft

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

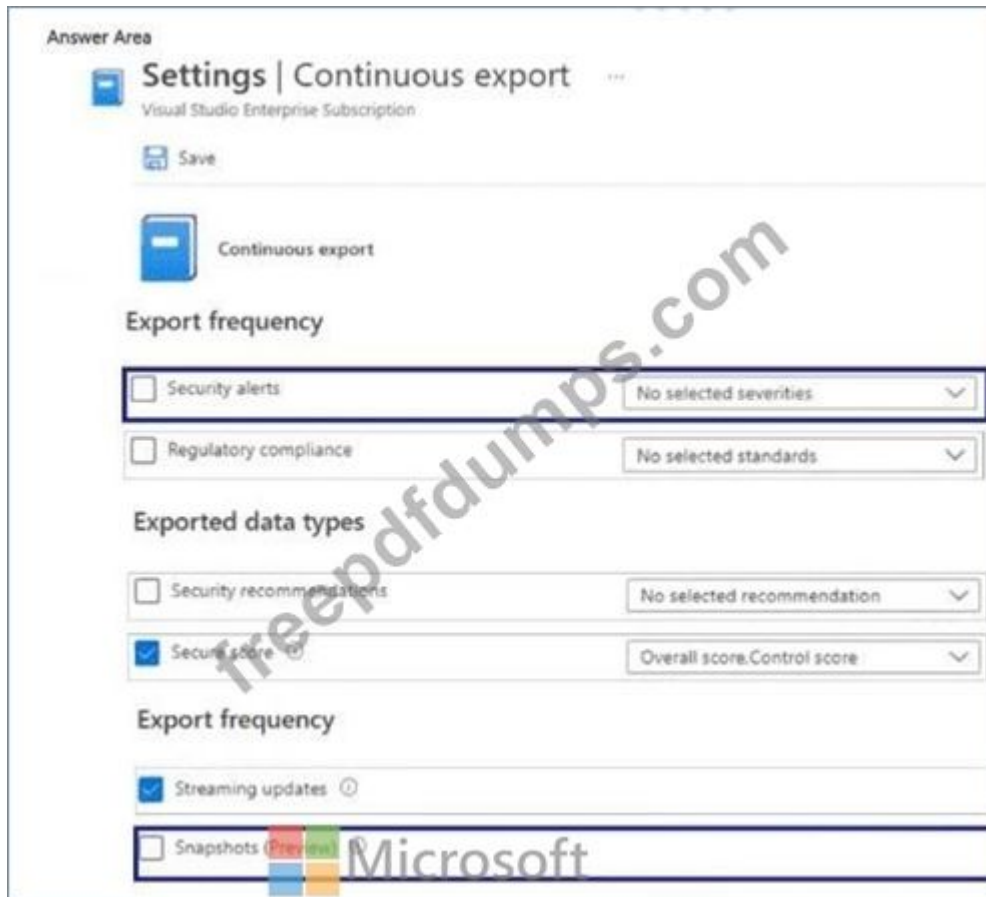
Exported data types

☐ 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: 84

You have an Azure subscription that contains a

You need to grant user1 access to blob1. The solution must ensure that the access expires after six days.

What should you use?

- A. a shared access policy
- B. a shared access signature (SAS)
- C. role-based access control (RBAC)
- D. a managed identity

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: 85

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

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

You need to identify which initiatives and policies you can add to Subscription1 by using Azure Security Center.

What should you identify?

- A. Policy1 and Policy2 only
- B. Initiative1 only
- C. Initiative1 and Initiative2 only
- D. Initiative1, Initiative2, Policy1, and Policy2

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

Reference:

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

NEW QUESTION: 86

You have an Azure Active Directory (Azure AD) tenant. The tenant contains users that are assigned Azure AD Premium Plan 2 licenses.

You have an partner company that has a domain named The fabrikam.com domain contains a user named user'. User' has an email address of userl@fabrikam.com.

You to provide User1 with to the resources in the tenant The solution must meet the following requirements:

- * user1 must be able to sign in by using the userl@fabrikam.com credentials
- * You must be able to grant User1 access to the resources in the tenant
- * Administrative effort must be minimized.

What should you do?

- A. To the tenant add fabrikamcom as a custom domain
- B. Create a user account for user1.
- C. Set Enable guest self-service sign up via user flows to Yes for the tenant.
- D. Create an invite for User1.

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

NEW QUESTION: 87

You are configuring network connectivity for two Azure virtual networks named VNET1 and VNET2.

You need to implement VPN gateways for the virtual networks to meet the following requirements:

- * VNET1 must have six site-to-site connections that use BGP.
- * VNET2 must have 12 site-to-site connections that use BGP.

* Costs must be minimized.

Which VPN gateway SKU should you use for each virtual network? To answer, drag the appropriate SKUs to the correct networks. Each SKU may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point

SKUs: Basic, VpnGw1, VpnGw2, VpnGw3

Answer Area: VNET1: SKU, VNET2: SKU

Microsoft

Answer:

SKUs: Basic, VpnGw1, VpnGw2, VpnGw3

Answer Area: VNET1: VpnGw1, VNET2: VpnGw1

Microsoft

Explanation:

VNET1: VpnGw1

VNET2: VpnGw1

References:

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

NEW QUESTION: 88

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

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

```

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

```

```

Name : StorageEA2Allow
ProvisioningState : Succeeded
Description :
Protocol : *
SourcePortRange : {*}
DestinationPortRange : {443}
SourceAddressPrefix : {*}
DestinationAddressPrefix : {Storage/EastUS2}
SourceApplicationSecurityGroups : []
DestinationApplicationSecurityGroups : []
Access : Allow
Priority : 104
Direction : Outbound

```

```

Name : Contoso_FTP
Description :
Protocol : TCP
SourcePortRange : {*}
DestinationPortRange : {21}
SourceAddressPrefix : {1.2.3.4/32}
DestinationAddressPrefix : {10.0.0.5/32}
SourceApplicationSecurityGroups : []
DestinationApplicationSecurityGroups : []
Access : Allow
Priority : 504
Direction : Inbound

```

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

NOTE: Each correct selection is worth one point.

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: 89

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

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

Both VM1 and VM2 connect to VNET1 and are configured to use NSG1.

You need to ensure that only VM1 and VM2 can access DB1.

What should you do?

- A. Add the IP address range of VNET1 to the Firewall setting of DB1.
- B. Create an application security group.
- C. Configure DB1 to allow access from only VNET1.

D. For NSG1, configure a rule that has a service tag.

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

NEW QUESTION: 90

Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD). Azure AD Connect is installed on a domain member server named Server1.

You need to ensure that a domain administrator for the adatum.com domain can modify the synchronization options. The solution must use the principle of least privilege.

Which Azure AD role should you assign to the domain administrator?

- A. Security administrator
- B. Global administrator
- C. User administrator

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

Reference:

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

NEW QUESTION: 91

You have an Azure Subscription that is connected to an on-premises datacenter and contains the resources shown in the following table.

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

You need to configure virtual network service endpoints for VNet1 and VNet2. The solution must meet the following requirements:

- * The virtual machines that connect to the subnet of VNet1 must access storage1, storage2, and Azure AD by using the Microsoft backbone network.
- * The virtual machines that connect to the subnet of VNet2 must access storage1 and KeyVault1 by using the Microsoft backbone network.
- * The virtual machines must use the Microsoft backbone network to communicate between VNet1 and VNet2.

How many service endpoints should you configure for each virtual network? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Microsoft

VNet1: 1

VNet2: 2

Answer:

Answer Area

Microsoft

VNet1: 1

VNet2: 2

Explanation:

Answer Area

Microsoft

VNet1: 1

VNet2: 2

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam!
Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500

exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:
https://www.actual4test.com/AZ-500_examcollection.html (497 Q&As Dumps, **30%OFF**
Special Discount: Freepdfdumps)

NEW QUESTION: 92

You have an Azure subscription that contains a storage account named storage1 and several virtual machines.

The storage account and virtual machines are in the same Azure region. The network configurations of the virtual machines are shown in the following table.

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

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

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

You configure the following Firewall and virtual networks settings for storage1:

- * Allow access from: Selected networks
- * Virtual networks: VNET3\Subnet3
- * Firewall - Address range: 52.233.129.0/24

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

NOTE: Each correct selection is worth one point.

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

Answer:

Statements	Yes	No
VM1 can connect to storage1.	☐	☒
VM2 can connect to storage1.	☒	☐
VM3 can connect to storage1.	☐	☒

Explanation:

Statements	Yes	No
VM1 can connect to storage1.	☐	☒
VM2 can connect to storage1.	☒	☐
VM3 can connect to storage1.	☐	☒

Box 1: No

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

Box 2: Yes

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

Box 3: No

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

NEW QUESTION: 93

You work at a company named Contoso, Ltd. that has the offices shown in the following table.

Name	IP address space
Boston	180.15.10.0/24
Seattle	132.32.15.0/24

Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com. All contoso.com users have Azure Multi-Factor Authentication (MFA) enabled. The tenant contains the users shown in the following table.

Name	User device	Last sign-in	During last sign-in, user selected Don't ask again for 14 days
User1	Device1	June 1	Yes
User2	Device2	June 3	No

The multi-factor settings for contoso.com are configured as shown in the following exhibit.

multi-factor authentication

[users](#) [service settings](#)

app passwords [\(learn more\)](#)

☒ Allow users to create app passwords to sign in to non-browser apps
☐ Do not allow users to create app passwords to sign in to non-browser apps

trusted ips [\(learn more\)](#)

☐ Skip multi-factor authentication for requests from federated users on my intranet
Skip multi-factor authentication for requests from following range of IP address subnets

180.15.10.0/24

verification options [\(learn more\)](#)

Methods available to users:

☐ call to phone
☒ Text message to phone
☒ Notification through mobile app
☒ Verification code from mobile app or hardware token



remember multi-factor authentication [\(learn more\)](#)

☒ Allow users to remember multi-factor authentication on devices they trust
Days before a device must re-authenticate (1-60):

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
When User1 signs in to Device1 from the Seattle office on June 10, the user will be prompted for MFA.	☐	☐
When User2 signs in to Device2 from the Boston office on June 5, the user will be prompted for MFA.	☐	☐
When User1 signs in to a new device from the Seattle office on June 7, the user will be prompted for MFA.	☐	☐

Answer:

Statements	Yes	No
When User1 signs in to Device1 from the Seattle office on June 10, the user will be prompted for MFA.	☐	☒
When User2 signs in to Device2 from the Boston office on June 5, the user will be prompted for MFA.	☒	☐
When User1 signs in to a new device from the Seattle office on June 7, the user will be prompted for MFA.	☒	☐

Explanation:

Answer Area



Statements

When User1 signs in to Device1 from the Seattle office on June 10, the user will be prompted for MFA.

When User2 signs in to Device2 from the Boston office on June 5, the user will be prompted for MFA.

When User1 signs in to a new device from the Seattle office on June 7, the user will be prompted for MFA.

Yes

No

NEW QUESTION: 94

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

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

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

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

```

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

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

Action IPAddressOrRange
-----
Allow 193.77.0.0/16

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

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

```

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

NOTE: Each correct selection is worth one point.

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

Answer:

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

Explanation:

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

Box 1: Yes

Access from Subnet1 is allowed.

Box 2: No

No access from Subnet2 is allowed.

Box 3: Yes

Access from IP address 193.77.10.2 is allowed.

NEW QUESTION: 95

You have 15 Azure virtual machines in a resource group named RG1.

All virtual machines run identical applications.

You need to prevent unauthorized applications and malware from running on the virtual machines.

What should you do?

- A. Apply an Azure policy to RG1.
- B. From Azure Security Center, configure adaptive application controls.
- C. Configure Azure Active Directory (Azure AD) Identity Protection.
- D. Apply a resource lock to RG1.

Answer: (SHOW ANSWER)

Adaptive application control is an intelligent, automated end-to-end application whitelisting solution from Azure Security Center. It helps you control which applications can run on your Azure and non-Azure VMs (Windows and Linux), which, among other benefits, helps harden your VMs against malware. Security Center uses machine learning to analyze the applications running on your VMs and helps you apply the specific whitelisting rules using this intelligence.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application>

NEW QUESTION: 96

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

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

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

What should you do?

- A. Create an Azure Private DNS zone.
- B. On VNet1. create a new subnet.
- C. For storage1, disable public network access.
- D. For storage1, create a new private endpoint.

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

NEW QUESTION: 97

You have an Azure subscription.

You need to ensure that you receive notifications regarding suspicious Azure DNS activity.

Which Microsoft Defender plan for Cloud Workload Protection (CWP) should you enable?

- A. Storage
- B. Resource Manager
- C. Servers
- D. APIs
- E. App Service

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

NEW QUESTION: 98

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a hybrid configuration of Azure Active Directory (Azure AD).

You have an Azure HDInsight cluster on a virtual network.

You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.

You need to configure the environment to support the planned authentication.

Solution: You deploy Azure Active Directory Domain Services (Azure AD DS) to the Azure subscription.

Does this meet the goal?

- A. Yes
- B. No

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

References:

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

NEW QUESTION: 99

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

You have the deleted objects shown in the following table.

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

On May 4, 2020, you attempt to restore the deleted objects by using the Azure Active Directory admin center.

Which two objects can you restore? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Group1
- B. Group2
- C. User2
- D. User1

Answer: B,C (LEAVE A REPLY)

Deleted users and deleted Office 365 groups are available for restore for 30 days.

You cannot restore a deleted security group.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-restore-deleted>

NEW QUESTION: 100

You have an Azure key vault.

You need to delegate administrative access to the key vault to meet the following requirements:

- * Provide a user named User1 with the ability to set advanced access policies for the key vault.
- * Provide a user named User2 with the ability to add and delete certificates in the key vault.
- * Use the principle of least privilege.

What should you use to assign access to each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

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:

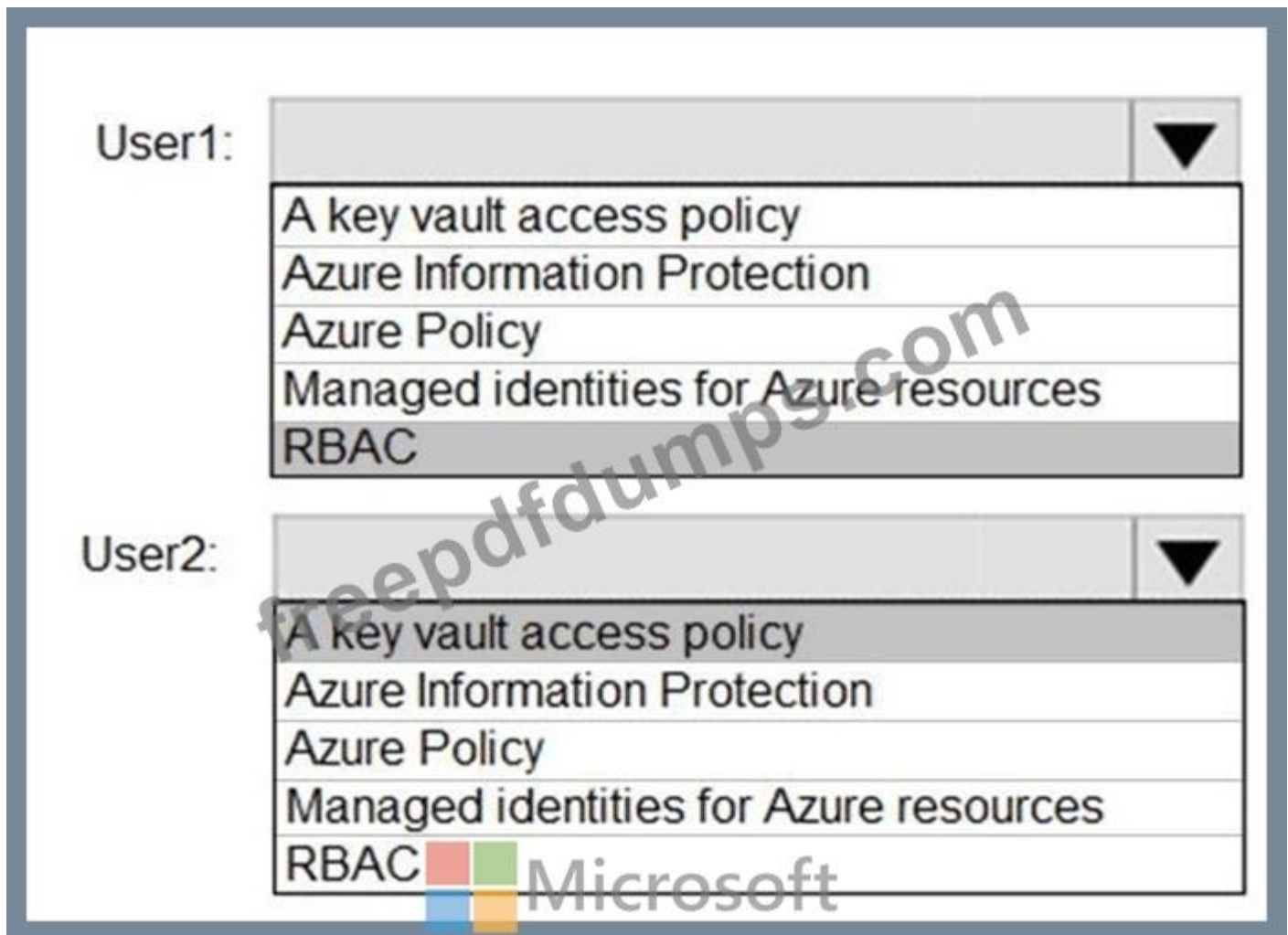
User1:

- 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: 101

Lab Task

Task 1

You need to ensure that connections from the Internet to VNET1\subnet0 are allowed only over TCP port

7777. The solution must use only currently deployed resources.

Answer:

see the task answer with step by step below:

Explanation:

You need to configure the Network Security Group that is associated with subnet0.

1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET1. Alternatively, browse to Virtual Networks in the left navigation pane.
2. In the properties of VNET1, click on Subnets. This will display the subnets in VNET1 and the Network Security Group associated to each subnet. Note the name of the Network Security Group associated to Subnet0.
3. Type Network Security Groups into the search box and select the Network Security Group associated with Subnet0.
4. In the properties of the Network Security Group, click on Inbound Security Rules.
5. Click the Add button to add a new rule.
6. In the Source field, select Service Tag.
7. In the Source Service Tag field, select Internet.
8. Leave the Source port ranges and Destination field as the default values (* and All).
9. In the Destination port ranges field, enter 7777.
10. Change the Protocol to TCP.
11. Leave the Action option as Allow.
12. Change the Priority to 100.
13. Change the Name from the default Port_8080 to something more descriptive such as Allow_TCP_7777_from_Internet. The name cannot contain spaces.
14. Click the Add button to save the new rule.

NEW QUESTION: 102

You are configuring just in time (JIT) VM access to a set of Azure virtual machines.

You need to grant users PowerShell access to the virtual machine by using JIT VM access.

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

NOTE: Each correct selection is worth one point.

Answer Area

Permission that must be granted to users on VM:

- Read
- Update
- View
- Write

TCP port that must be allowed:

- 22
- 25
- 3389
- 5986

Microsoft

Answer:

Answer Area

Permission that must be granted to users on VM:

☒ Read
☐ Update
☐ View
☐ Write

TCP port that must be allowed:

☐ 22
☐ 25
☐ 3389
☒ 5986



Microsoft

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: 103

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

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

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

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

NOTE: Each correct selection is worth one point.

Azure Active Directory Identity Protection:

AzureDiagnostics
CommonSecurityLog
SecurityAlert
SecurityEvent
Syslog

Azure Firewall:

AzureDiagnostics
CommonSecurityLog
SecurityAlert
SecurityEvent
Syslog

CEF:

AzureDiagnostics
CommonSecurityLog
SecurityAlert
SecurityEvent
Syslog

Answer:

Azure Active Directory Identity Protection:

AzureDiagnostics
CommonSecurityLog
SecurityAlert
SecurityEvent
Syslog

Azure Firewall:

AzureDiagnostics
CommonSecurityLog
SecurityAlert
SecurityEvent
Syslog

CEF:

AzureDiagnostics
CommonSecurityLog
SecurityAlert
SecurityEvent
Syslog

Explanation:

Graphical user interface, application, table Description automatically generated

Azure Active Directory Identity Protection:

Microsoft

AzureDiagnostics
CommonSecurityLog
SecurityAlert
SecurityEvent
Syslog

Azure Firewall:

AzureDiagnostics
CommonSecurityLog
SecurityAlert
SecurityEvent
Syslog

CEF:

AzureDiagnostics
CommonSecurityLog
SecurityAlert
SecurityEvent
Syslog

NEW QUESTION: 104

You plan to deploy a custom policy initiative for Microsoft Defender for Cloud.

You need to identify all the resource groups that have a Delete lock.

How should you complete the policy definition? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Microsoft

...

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

freepdfdumps.com

Answer:

Answer Area

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

Explanation:

A screenshot of a computer Description automatically generated

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"  
            }  
          }  
        }  
      }  
    }  
  }  
}
```

NEW QUESTION: 105

You have an Azure subscription that contains a SQL Server on Azure Virtual Machines instance named SQ1 and a Microsoft Sentinel workspace named Sentinel1.

You need to monitor security incidents on SQL1 by using Sentinel1.

What should you do first?

- A. From the Azure portal, create a Log Analytics workspace.
- B. On SQL1, install the Connected Machine agent for Azure Arc-enabled servers.
- C. On SQL1, enable SQL1 Server audit.
- D. From Sentinel1, enable VM insights.

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

NEW QUESTION: 106

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

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

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

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

NOTE: Each correct selection is worth one point.

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:

	▼
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	

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>

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam!

Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (497 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 107

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

You are assigned the Global administrator role for the tenant. You are responsible for managing Azure Security Center settings.

You need to create a custom sensitivity label.

What should you do first?

- A. Create a custom sensitive information type.
- B. Elevate access for global administrators in Azure AD.
- C. Upgrade the pricing tier of the Security Center to Standard.
- D. Enable integration with Microsoft Cloud App Security.

Answer: A (LEAVE A REPLY)

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

References:

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

NEW QUESTION: 108

You have an on-premises network and an Azure subscription.

You have the Microsoft SQL Server instances shown in the following table.

Name	Type	Microsoft
sql1	Azure SQL managed instance	
sql2	SQL Server 2019 on an Azure virtual machine that runs Windows Server 2019	
sql3	SQL Server 2019 on an Azure virtual machine that runs Red Hat Enterprise Linux (RHEL) 8.3	
sql4	On-premises physical server that runs Windows Server 2016 and has SQL Server 2016 installed	

You plan to implement Microsoft Defender for SQL.

Which SQL Server instances will be protected by Microsoft Defender for SQL?

- A. sql1, sql2, and sql3 only
- B. sql1 and sql2 only
- C. sql1, sql2, sql3, and sql4
- D. sql1 sql2 and so.14 only

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

NEW QUESTION: 109

You have an Azure subscription that contains an Azure key vault and an Azure Storage account. The key vault contains customer-managed keys. The storage account is configured to use the customer-managed keys stored in the key vault.

You plan to store data in Azure by using the following services:

- * Azure Files
- * Azure Blob storage
- * Azure Log Analytics
- * Azure Table storage
- * Azure Queue storage

Which two services data encryption by using the keys stored in the key vault? Each correct answer present a complete solution.

NOTE: Each correct selection is worth one point.

- A. Queue storage
- B. Table storage
- C. Azure Files
- D. Blob storage

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

<https://docs.microsoft.com/en-us/azure/storage/common/account-encryption-key-create?tabs=portal>

NEW QUESTION: 110

You have an Azure subscription.

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

- * Provide access to DDoS rapid response support during active attacks.
- * Project Basic SKU public IP addresses.

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

What should you recommend? To answer, drag the appropriate DDoS projection types to the

correct requirements. Each DDoS Projection type may be used once, or not at all. You may need to drag the split bar between panes or scroll to view connect.

NOTE: Each correct selection is worth one point.



Answer:



Explanation:



NEW QUESTION: 111

You have an Azure subscription that uses Azure AD Privileged Identity Management (PIM).

A user named User1 is eligible for the Billing administrator role.

You need to ensure that the role can only be used for a maximum of two hours.

What should you do?

- A. Update the end date of the user assignment
- B. Edit the role assignment settings.
- C. Edit the role activation settings.
- D. Create a new access review.

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

NEW QUESTION: 112

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

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

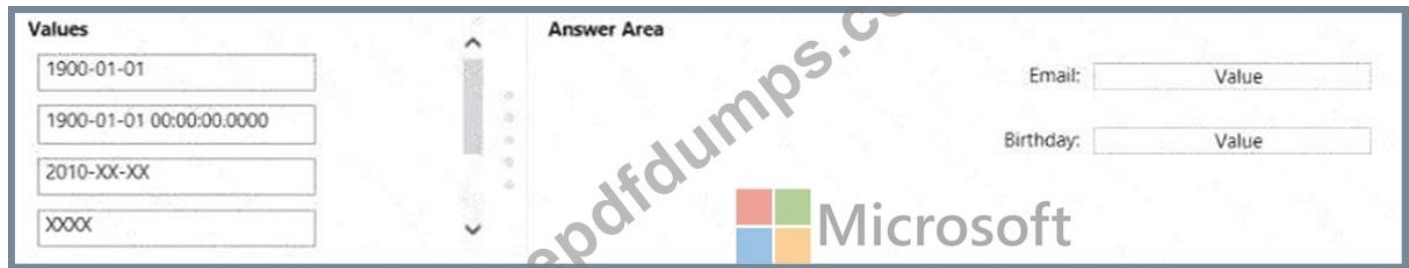
For the Email and Birthday columns, you implement dynamic data masking by using the default masking function.

Which value will the users see in each column? To answer, drag the appropriate values to the correct columns.

Each value may be used once, more than once, or not at all. You may need to drag the split bar

between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Answer:



Explanation:



NEW QUESTION: 113

You have an Azure subscription that uses Microsoft Defender for Cloud. The subscription contains the Azure Policy definitions shown in the following table.

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

Which definitions can be assigned as a security policy in Defender for Cloud?

- A. Policy1 and Initiative1 only
- B. Initiative1 and Initiative2 only
- C. Policy1, Policy2, Initiative1, and Initiative2
- D. Policy2 and Initiative2 only
- E. Policy1 and Policy2 only

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

NEW QUESTION: 114

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

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

You set the Key Vault access policy to Enable access to Azure Disk Encryption for volume encryption.

KeyVault1 is configured as shown in the following exhibit.

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: [+ Add](#)

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.](#)

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

NOTE: Each correct selection is worth one point.

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

Answer:

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

Explanation:

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

NEW QUESTION: 115

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

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

In Sub1, you create a virtual machine that has the following configurations:

- * Name: VM1
- * Size: DS2v2
- * Resource group: RG1
- * Region: West Europe
- * Operating system: Windows Server 2016

You plan to enable Azure Disk Encryption on VM1.

In which key vaults can you store the encryption key for VM1?

- A. Vault1 or Vault3 only
- B. Vault1, Vault2, Vault3, or Vault4
- C. Vault1 only
- D. Vault1 or Vault2 only

Answer: C (LEAVE A REPLY)

"Your key vault and VMs must be in the same subscription. Also, to ensure that encryption secrets don't cross regional boundaries, Azure Disk Encryption requires the Key Vault and the

VMs to be co-located in the same region." <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault>

NEW QUESTION: 116

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to create several security alerts by using Azure Monitor.

You need to prepare the Azure subscription for the alerts.

What should you create first?

- A. An Azure Storage account
- B. an Azure Log Analytics workspace
- C. an Azure event hub
- D. an Azure Automation account

Answer: ([SHOW ANSWER](#))

<https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-create-workspace>

NEW QUESTION: 117

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

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

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

What should you do?

- A. From Azure Security Center, view the Regulatory compliance assessment.
- B. From the Policy blade of the Azure Active Directory admin center, select Compliance.
- C. From Azure Security Center, view the Secure Score.
- D. From the Policy blade of the Azure Active Directory admin center, select Assignments.

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

Reference:

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

NEW QUESTION: 118

You have an Azure subscription that contains an Azure key vault named ContosoKey1.

You create users and assign them roles as shown in the following table.

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

You need to identify which users can perform the following actions:

- * Delegate permissions for ContosoKey1.
- * Configure network access to ContosoKey1.

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

NOTE: Each correct selection is worth one point.

Microsoft

Delegate permissions for 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

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:

▼

- 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:

Delegate permissions for 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	



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	

Reference:

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

NEW QUESTION: 119

You plan to create an Azure Kubernetes Service (AKS) cluster in an Azure subscription. The manifest of the registered server application is shown in the following exhibit.

Save Discard Upload Download

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

```
1 {
2   "id": "d6b00db3-7ef4-4f3c-b1e7-8346f0a59546",
3   "acceptMappedClaims": null,
4   "accessTokenAcceptedVersion": null,
5   "addIns": [],
6   "allowPublicClient": null,
7   "appId": "88137405-6a75-4c20-903a-f7b18ff7d496",
8   "appRoles": [],
9   "oauth2AllowUrlPathMatching": false,
10  "createdDateTime": "2019-07-15T21:09:20Z",
11  "groupMembershipClaims": null,
12  "identifierUris": [],
13  "informationalUrls": {
14    "termsOfService": null,
15    "support": null,
16    "privacy": null,
17    "marketing": null
18  },
19  "keyCredentials": [],
20  "knownClientApplications": [],
21  "logoUrl": null,
22  "logoutUrl": null,
23  "name": "AKSAzureADServer",
24  "oauth2AllowIdTokenImplicitFlow": false,
25  "oauth2AllowImplicitFlow": false,
26  "oauth2Permissions": [],
27  "oauth2RequirePostResponse": false,
28  "optionalClaims": null,
29  "orgRestrictions": [],
30  "parentalControlSettings": {
```

You need to ensure that the AKS cluster and Azure Active Directory (Azure AD) are integrated. Which property should you modify in the manifest?

- A. accessTokenAcceptedVersion
- B. keyCredentials
- C. groupMembershipClaims
- D. acceptMappedClaims

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

Reference:

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

<https://www.codeproject.com/Articles/3211864/Operation-and-Maintenance-of-AKS-Applications>

NEW QUESTION: 120

You onboard Azure Sentinel. You connect Azure Sentinel to Azure Security Center.

You need to automate the mitigation of incidents in Azure Sentinel. The solution must minimize administrative effort.

What should you create?

- A. a function app
- B. a runbook
- C. a playbook
- D. an alert rule

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

NEW QUESTION: 121

You are configuring and securing a network environment.

You deploy an Azure virtual machine named VM1 that is configured to analyze network traffic.

You need to ensure that all network traffic is routed through VM1.

What should you configure?

- A. a system route
- B. a network security group (NSG)
- C. a user-defined route

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

Although the use of system routes facilitates traffic automatically for your deployment, there are cases in which you want to control the routing of packets through a virtual appliance. You can do so by creating user defined routes that specify the next hop for packets flowing to a specific subnet to go to your virtual appliance instead, and enabling IP forwarding for the VM running as the virtual appliance.

Note: User Defined Routes

For most environments you will only need the system routes already defined by Azure. However, you may need to create a route table and add one or more routes in specific cases, such as:

- * Force tunneling to the Internet via your on-premises network.
- * Use of virtual appliances in your Azure environment.
- * In the scenarios above, you will have to create a route table and add user defined routes to it.

Reference:

[https://github.com/uglide/azure-content/blob/master/articles/virtual-network/virtual-networks-udr-overview.](https://github.com/uglide/azure-content/blob/master/articles/virtual-network/virtual-networks-udr-overview.md)

md

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam!

Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (497 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 122

From Azure Security, you create a custom alert rule.

You need to configure which users will receive an email message when the alert is triggered.

What should you do?

- A. From Azure Monitor, create an action group.
- B. From Security Center, modify the Security policy settings of the Azure subscription.
- C. From Azure Active Directory (Azure AD), modify the members of the Security Reader role group.
- D. From Security Center, modify the alert rule.

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

References:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups>

NEW QUESTION: 123

You have an Azure subscription named Sub1 that has Security defaults disabled. The subscription contains the following users:

- * Five users that have owner permissions for Sub1.
- * Ten users that have owner permissions for Azure resources.

None of the users have multi-factor authentication (MFA) enabled.

Sub1 has the secure score as shown in the Secure Score exhibit. (Click the Secure Score tab.)

You plan to enable MFA for the following users:

- * Five users that have owner permissions for Sub1.
- * Five users that have owner permissions for Azure resources.

By how many points will the secure score increase after you perform the planned changes?

- A. 7.5
- B. 5
- C. 10
- D. 14
- E. 0

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

NEW QUESTION: 124

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

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

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

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

On NIC1, you configure an application security group named ASG1.

On which other network interfaces can you configure ASG1?

- A. NIC2 only
- B. NIC2, NIC3, NIC4, and NIC5
- C. NIC2 and NIC3 only
- D. NIC2, NIC3, and NIC4 only

Answer: ([SHOW ANSWER](#))

Only network interfaces in NVET1, which consists of Subnet11 and Subnet12, can be configured in ASG1, as all network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in.

Reference:

<https://azure.microsoft.com/es-es/blog/applicationsecuritygroups/>

NEW QUESTION: 125

You have an Azure subscription that contains an Azure SQL database named DB1 in the East US Azure region. You create the storage accounts shown in the following table.

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

You plan to enable auditing for DB1.

Which storage accounts can you use as the auditing destination for DB1?

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

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

NEW QUESTION: 126

You have an Azure subscription that contains a managed identity named Identity1 and the Azure key vaults shown in the following table.

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

Key Vault1 contains an access policy that grants Identity1 the following key permissions:

- * Get
- * List

* Wrap

* Unwrap

You need to provide Identity1 with the same permissions for KeyVault2. The solution must use the principle of least privilege.

Which role should you assign to Identity1?

- A. Key Vault Crypto Officer
- B. Key Vault Crypto Service Encryption User
- C. Key Vault Reader
- D. Key Vault Crypto User

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

NEW QUESTION: 127

You have an Azure subscription.

You plan to deploy the virtual machines shown in the following table.

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

You need to identify the virtual machines and operating systems that can be deployed as confidential virtual machines?

Which Windows virtual machines and which Linux virtual machines should you identify?

Answer Area

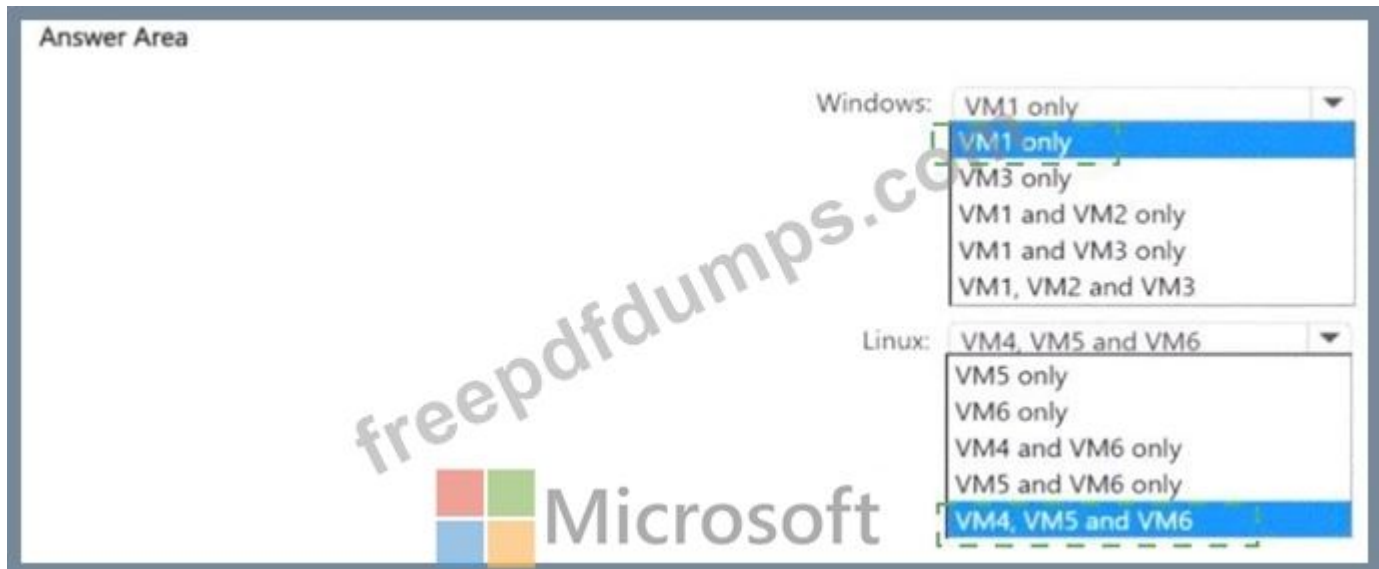
Windows: VM1 only

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

Linux: VM4, VM5 and VM6

- VM5 only
- VM6 only
- VM4 and VM6 only
- VM5 and VM6 only
- VM4, VM5 and VM6

Answer:



Explanation:



NEW QUESTION: 128

You have a Azure subscription that contains an Azure Container Registry named Registry1. The subscription uses the Standard use tier of Azure Security Center.

You upload several container images to Register1.

You discover that vulnerability security scans were not performed

You need to ensured that the images are scanned for vulnerabilities when they are uploaded to Registry1.

What should you do?

- A. From the Azure portal modify the Pricing tier settings.
- B. From Azure CLI, lock the container images.
- C. Upload the container images by using AzCopy
- D. Push the container images to Registry1 by using Docker

Answer: ([SHOW ANSWER](#))

Reference:

<https://charbelnemnom.com/scan-container-images-in-azure-container-registry-with-azure-security-center/>

NEW QUESTION: 129

You have an Azure subscription that contains four Azure SQL managed instances.

You need to evaluate the vulnerability of the managed instances to SQL injection attacks.

What should you do first?

- A. Add the SQL Health Check solution to Azure Monitor.
- B. Create an Azure Sentinel workspace.

C. Enable Advanced Data Security.

D. Create an Azure Advanced Threat Protection (ATP) instance.

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

NEW QUESTION: 130

You have a Microsoft Entra tenant that contains three users named User1, User2, and User3. You configure Microsoft Entra Password Protection as shown in the following exhibit.

Save Discard

Custom smart lockout

Lockout threshold ⓘ 10

Lockout duration in seconds ⓘ 60

Custom banned passwords

Enforce custom list ⓘ Yes No

Custom banned password list ⓘ

Contoso Product
Fabrikam

Microsoft

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ Yes No

Mode ⓘ Enforced Audit

The users perform the following tasks:

- * User1 attempts to reset her password to COnToSo
- * User2 attempts to reset her password to F@brikamHQ
- * User3 attempts to reset her password to PrOduct123.

Which password reset attempts fail?

- A. User1 only
- B. User1 and User3 only
- C. User2 only
- D. User3 only
- E. User1, User2, and User3

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

NEW QUESTION: 131

Lab Task

Task 6

You need to configure a Microsoft SQL server named Web3l 330471 only to accept connections from the Subnet0 subnet on the VNET01 virtual network.

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: 132

You have an Azure Active Directory (Azure AD) tenant that contains two administrative units named AU1 and AU2.

Users are assigned to the administrative units as shown in the following table.

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

Statements	Yes	No
Admin1 can reset the password of User1.	☐	☐
Admin2 can reset the password of User3.	☐	☐
Admin3 can reset the password of Admin4.	☐	☐

Answer:

Statements	Yes	No
Admin1 can reset the password of User1.	☐	☐
Admin2 can reset the password of User3.	☐	☐
Admin3 can reset the password of Admin4.	☐	☐

Explanation:

Statements	Yes	No
Admin1 can reset the password of User1.	☒	☐
Admin2 can reset the password of User3.	☒	☐
Admin3 can reset the password of Admin4.	☐	☒

NEW QUESTION: 133

You have an Azure subscription that contains a web app named App1.

Users must be able to select between a Google identity or a Microsoft identity when authenticating to App1.

You need to add Google as an identity provider in Azure AD.

Which two pieces of information should you configure? Each correct answer presents part of the solution.

Each correct selection is worth one point

- A. a tenant name
- B. a tenant ID
- C. the endpoint URL Of an application
- D. a client ID
- E. a client secret

Answer: ([SHOW ANSWER](#))

<https://learn.microsoft.com/en-us/azure/app-service/configure-authentication-provider-google>

NEW QUESTION: 134

You have an Azure Sentinel workspace that has an Azure Active Directory (Azure AD) data connector.

You are threat hunting suspicious traffic from a specific IP address.

You need to annotate an intermediate event stored in the workspace and be able to reference the IP address when navigating through the investigation graph.

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

Actions

Add the query to Favorites.

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

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

Add a bookmark and assign a tag.

Add a bookmark and map an entity.

From Azure Monitor, run an Azure Log Analytics query.

Select a query result.

Answer Area

Answer:

Actions

Add the query to Favorites.

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

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

Add a bookmark and assign a tag.

Add a bookmark and map an entity.

From Azure Monitor, run an Azure Log Analytics query.

Select a query result.

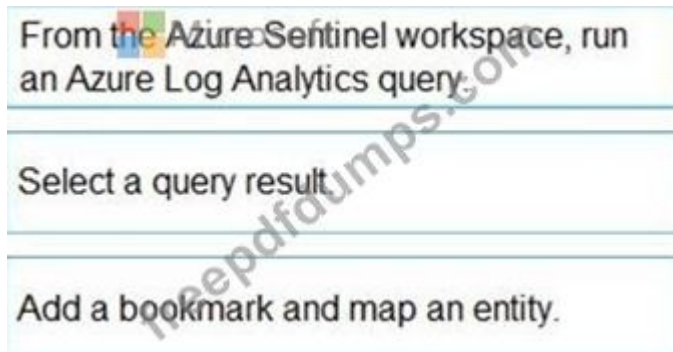
Answer Area

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

Select a query result.

Add a bookmark and map an entity.

Explanation:



Reference:

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

NEW QUESTION: 135

Your company has an Active Directory forest with a single domain, named weyländindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.

After syncing all on-premises identities to Azure AD, you are informed that users with a givenName attribute starting with LAB should not be allowed to sync to Azure AD.

Which of the following actions should you take?

- A. You should make use of the Synchronization Rules Editor to create an attribute-based filtering rule.
- B. You should configure a DNAT rule on the Firewall.
- C. B. You should configure a network traffic filtering rule on the Firewall.
- D. You should make use of Active Directory Users and Computers to create an attribute-based filtering rule.

Answer: 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: 136

You have multiple development teams that will create apps in Azure.

You plan to create a standard development environment that will be deployed for each team.

You need to recommend a solution that will enforce resource locks across the development environments and ensure that the locks are applied in a consistent manner.

What should you include in the recommendation?

- A. an Azure policy
- B. an Azure Resource Manager template
- C. a management group
- D. an Azure blueprint

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

Reference:

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam!
Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:
https://www.actual4test.com/AZ-500_examcollection.html (497 Q&As Dumps, **30%OFF**
Special Discount: Freepdfdumps)

NEW QUESTION: 137

You have an Azure subscription that uses Microsoft Defender for Cloud.
Defender for Cloud has the security alerts shown in the following exhibit.

3 Open alerts 3 Active alerts 0 In progress alerts 1 Affected resources

Search by ID, IP, name, or affected resource... Subscription == All Status == Active, Resolved, In Progress Severity == Low, Medium, High Add filter No grouping

Severity	Alert name	Affected resource	Resour...	Activity start time (...)	MITRE ATT&...	Status
Medium	Suspicious authentication activity	VM-4	RG9	01/29/24, 05:11 PM	Pre-attack	Active
Medium	Suspicious authentication activity	VM-4	RG9	12/02/23, 11:39 PM	Pre-attack	Active
Medium	Suspicious authentication activity	VM-4	RG9	12/02/23, 11:18 PM	Pre-attack	Active
Medium	Suspicious authentication activity	VM-4	RG9	12/01/23, 12:44 PM	Pre-attack	Resolved

If you change the status of the alert that was triggered at 05:11 PM to Dismissed. [answer choice],

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

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

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

Answer:

Answer Area

If you change the status of the alert that was triggered at 05:11 PM to Dismissed, [answer choice].

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

the alert will no longer be visible

the alert activity start time will change

the alert severity will change to Low

the alert will no longer be visible

the status of all four alerts will change

can be changed to Active, In Progress, or Dismissed

can be changed to Active only

can be changed to Active or Dismissed only

can be changed to Active, In Progress, or Dismissed

can be changed to InProgress or Dismissed only

cannot be changed

Explanation:

Answer Area

If you change the status of the alert that was triggered at 05:11 PM to Dismissed, [answer choice].

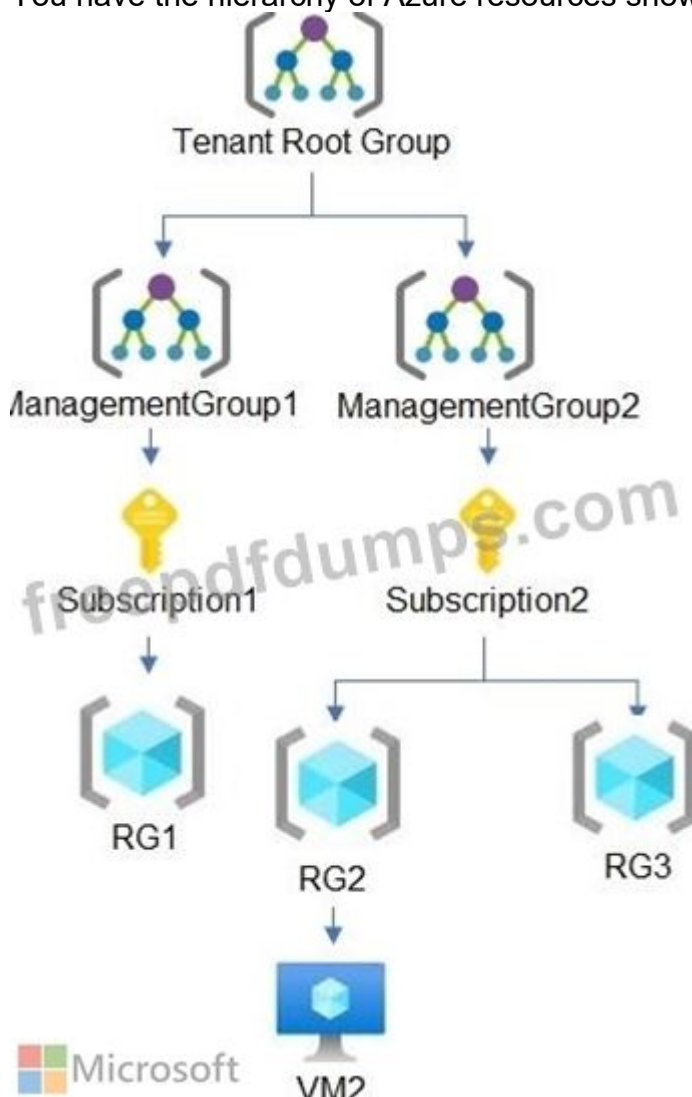
The status of the alert that was triggered at 12:44 PM [answer choice].

the alert will no longer be visible

can be changed to Active, In Progress, or Dismissed

NEW QUESTION: 138

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



RG1, RG2, and RG3 are resource groups.

RG2 contains a virtual machine named VM1.

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

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

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

NOTE: Each correct selection is worth one point.

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

Answer:

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

Explanation:

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

NEW QUESTION: 139

You have an Azure subscription that uses Azure Active Directory (Azure AD) Privileged Identity Management (PIM).

A PIM user that is assigned the User Access Administrator role reports receiving an authorization error when performing a role assignment or viewing the list of assignments.

You need to resolve the issue by ensuring that the PIM service principal has the correct permissions for the subscription. The solution must use the principle of least privilege.

Which role should you assign to the PIM service principle?

- A. Contributor
- B. User Access Administrator
- C. Resource Policy Contributor
- D. Managed Application Operator

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

NEW QUESTION: 140

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

Name	Location
RG1	West US
RG2	East US

You create the Azure Policy definition shown in the following exhibit.

```
1 {
2   "mode": "All",
3   "policyRule": {
4     "if": {
5       "anyOf": [
6         {
7           "field": "location",
8           "notEquals": "[resourceGroup().location]"
9         },
10        {
11          "field": "name",
12          "notContains": "obj"
13        }
14      ],
15      "then": {
16        "effect": "deny"
17      }
18    },
19    "parameters": {}
20  }
21 }
```

You assign the policy to Sub1.

You plan to create the resources shown in the following table.

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

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

NOTE: Each correct selection is worth one point.

Answer Area



Statements

You can create IPobject1.

You can create obj1.

You can create OBJ3.

Yes

No

☐

☐

☐

☐

☐

☐

Answer:

Answer Area

Statements	Yes	No
You can create IPObject1.	☐	☐
You can create obj1.	☐	☐
You can create OBJ3.	☐	☐

Explanation:

Statements	Yes	No
You can create IPObject1.	☐	☒
You can create obj1.	☐	☒
You can create OBJ3.	☐	☒

NEW QUESTION: 141

You have an Azure subscription that contains a web app named App1 and an Azure key vault named Vault1.

You need to configure App1 to store and access the secrets in Vault1.

How should you configure App1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

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

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: 142

You have the role assignments shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

 [answer choice] can delete VM1.

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

[answer choice] can create new resource groups.

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

Answer:

 [answer choice] can delete VM1.

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

[answer choice] can create new resource groups.

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

NEW QUESTION: 143

Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD).

The Azure AD tenant contains the users shown in the following table.

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

You configure the Authentication methods - Password Protection settings for adatum.com as shown in the following exhibit.

Custom smart lockout

Lockout threshold ✓

Lockout duration in seconds ✓

Custom banned passwords

Enforce custom list ☒ Yes ☐ No

Custom banned password list ✓

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ☒ Yes ☐ No

Mode ☐ Enforced ☒ Audit

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

NOTE: Each correct selection is worth one point.

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

Answer:

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

Explanation:

Text Description automatically generated

Statements

Yes

No

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

☐☒

User2 can change the password to @d@t@m_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: 144

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

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

Group3 is a member of Group2.

In contoso.com, you register an enterprise application named App1 that has the following settings:

* Owners: User1

* Users and groups: Group2

You configure the properties of App1 as shown in the following exhibit.

Save Discard Delete Got feedback

Enabled for users to sign-in? ☒ Yes ☐ No

Name *

Homepage URL

Logo 



Application ID 

Object ID 

User assignment required? ☐ Yes ☒ No

Visible to users ☒ Yes ☐ No

Notes

 Microsoft

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

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

Answer:

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

Explanation:
Text Description automatically generated

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

Reference:

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

NEW QUESTION: 145

You have an Azure subscription that is linked to a Microsoft Entra tenant named contoso.com. In contoso.

com, you register an app named App1. You need to perform the following tasks for App1:

- * Add and configure the Mobile and desktop applications platform.
- * Add the ipaddr optional claim.

Which two settings should you select for App1? To answer, select the appropriate settings in the answer area.

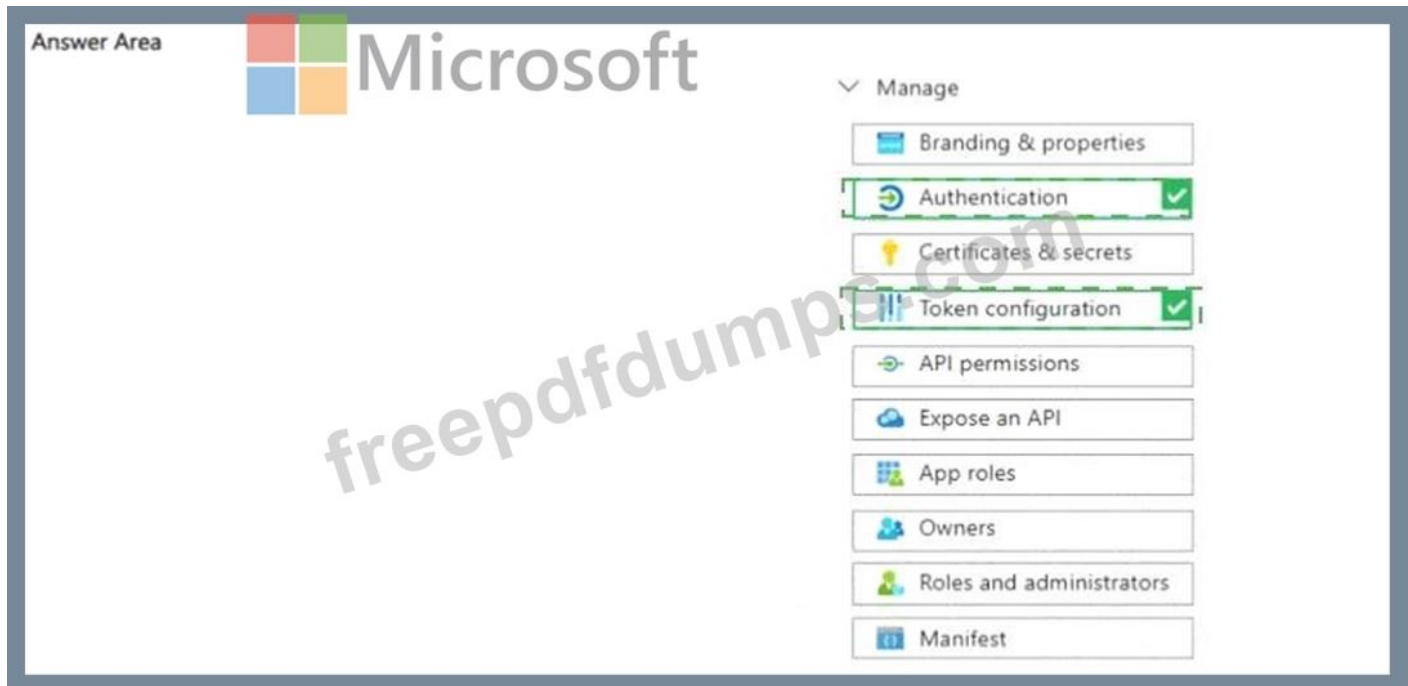
NOTE; Each correct selection is worth one point.

Answer Area

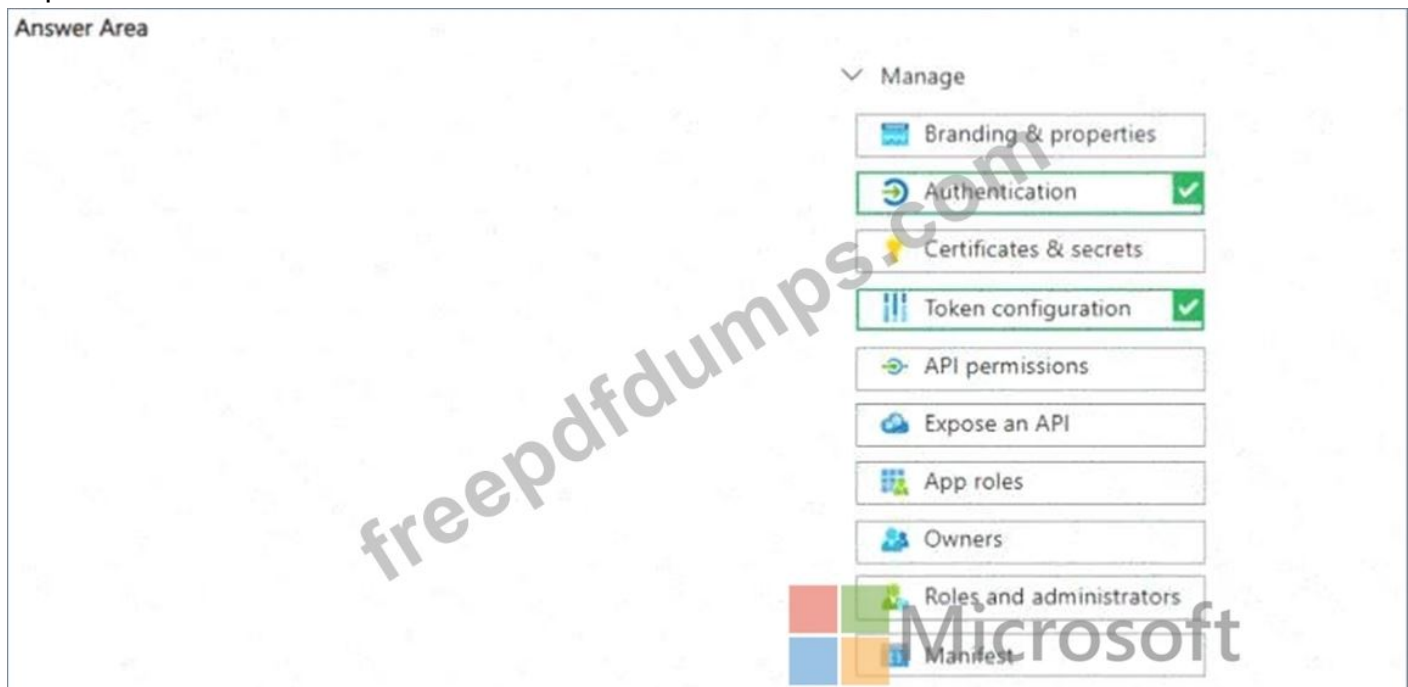
Manage

- Branding & properties
- Authentication ☒
- Certificates & secrets
- Token configuration ☒
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Answer:



Explanation:



NEW QUESTION: 146

Lab Task

use the following login credentials as needed:

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

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

Azure Username: User1-28681041@ExamUsers.com

Azure Password: GpOAe4@IDg

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

The following information is for technical support purposes only:

Lab Instance: 28681041

Task 4

You need to ensure that a user named user2-28681041 can manage the properties of the virtual machines in the RG1lod28681041 resource group. The solution must use the principle of least privilege.

Answer:

Check below steps in explanation for Task

Explanation:

To ensure that a user named user2-28681041 can manage the properties of the virtual machines in the RG1lod28681041 resource group using the principle of least privilege, you can follow these steps:

In the Azure portal, search for and select the resource group named RG1lod28681041.

In the left pane, select Access control (IAM).

Select Add.

In the Add role assignment pane, enter the following information:

Role: Select the appropriate role for your scenario. For example, Virtual Machine Contributor.

Assign access to: Select User, group, or service principal.

Select: Enter the name of the user you want to assign the role to. For example, user2-28681041.

Select Save.

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

NEW QUESTION: 147

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

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

You need to ensure that ServerAdmins can perform the following tasks:

- * Create virtual machines in RG1 only.
- * Connect the virtual machines to the existing virtual networks in RG2 only.

The solution must use the principle of least privilege.

Which two role-based access control (RBAC) roles should you assign to ServerAdmins? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a custom RBAC role for RG2
- B. the Network Contributor role for RG2
- C. the Contributor role for the subscription
- D. a custom RBAC role for the subscription
- E. the Network Contributor role for RG1

F. the Virtual Machine Contributor role for RG1

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

Reference:

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

NEW QUESTION: 148

You have been tasked with configuring an access review, which you plan to assigned to a new collection of reviews. You also have to make sure that the reviews can be reviewed by resource owners.

You start by creating an access review program and an access review control.

You now need to configure the Reviewers.

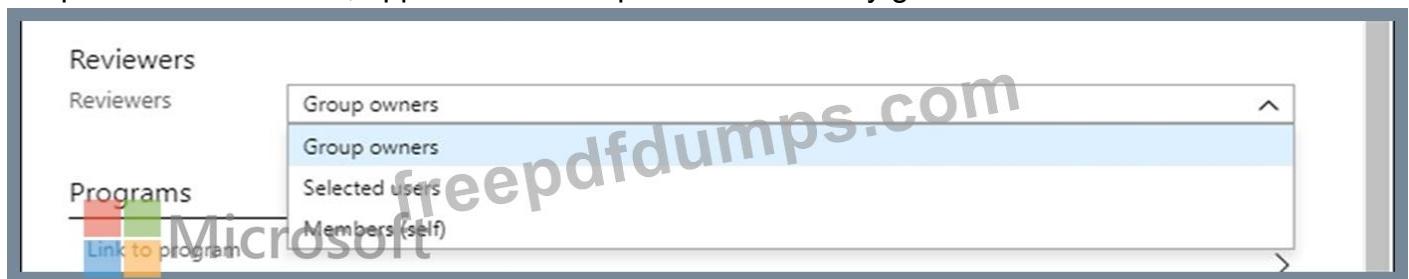
Which of the following should you set Reviewers to?

- A. Selected users.
- B. Members (Self).
- C. Group Owners.
- D. Anyone.

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

In the Reviewers section, select either one or more people to review all the users in scope. Or you can select to have the members review their own access. If the resource is a group, you can ask the group owners to review.

Graphical user interface, application Description automatically generated with medium confidence



Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

<https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-programs-controls>

NEW QUESTION: 149

You have an Azure subscription that contains a user named Admin1 and a virtual machine named VM1.

VM1 runs Windows Server 2019 and was deployed by using an Azure Resource Manager template. VM1 is the member of a backend pool of a public Azure Basic Load Balancer.

Admin1 reports that VM1 is listed as Unsupported on the Just in time VM access blade of Azure Security Center.

You need to ensure that Admin1 can enable just in time (JIT) VM access for VM1.

What should you do?

- A. Create and configure an additional public IP address for VM 1.

B. Replace the Basic Load Balancer with an Azure Standard Load Balancer.

C. Assign an Azure Active Directory Premium Plan 1 license to Admin1.

D. Create and configure a network security group (NSG).

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

Reference:

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

NEW QUESTION: 150

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription named Sub1.

You have an Azure Storage account named Sa1 in a resource group named RG1.

Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.

You discover that unauthorized users accessed both the file service and the blob service.

You need to revoke all access to Sa1.

Solution: You create a lock on Sa1.

Does this meet the goal?

A. Yes

B. No

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: 151

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

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

Which resources can be assigned the Contributor role for VM1?

- A. Group1 and Managed1 only
- B. Group1, Managed1, VM1. and App1 only
- C. Group1, Managed1, and VM2only
- D. Managed1 and App1 only

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

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam!

Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (497 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 152

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

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

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

```

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

```

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

```

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

```

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

Answer:

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

Explanation:

Answer Area

Statements

User1 can read data in storage1.

Yes

No

☒☐

User2 can read data in storage1.

☒☐

User3 can restore storage1 from a backup in Azure Backup.

☒

NEW QUESTION: 153

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

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

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

Save Discard

Allow access from:

☐ All networks ☒ Selected networks

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

Virtual networks: 0

+ Add existing virtual networks + Add new virtual network

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

Firewall: 0

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.](#)

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

NOTE: Each correct selection is worth one point.

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

Answer:

Answer Area



From VM1, users can manage the keys and secrets stored in KeyVault1.

Yes

No

☐☐

From VM2, users can manage the keys and secrets stored in KeyVault1.

☐☐

VM2 can use KeyVault1 for Azure Disk Encryption.

☐☐

Explanation:

Answer Area

Statements

Yes

No

From VM1, users can manage the keys and secrets stored in KeyVault1.

☒☐

From VM2, users can manage the keys and secrets stored in KeyVault1.

☒☐

VM2 can use KeyVault1 for Azure Disk Encryption.

☒☐

NEW QUESTION: 154

You have an Azure subscription.

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

- * Create three secured virtual hubs located in the East US, West US, and North Europe Azure regions.
- * Ensure that security rules sync between the regions.

What should you use?

- A. Azure Firewall Manager
- B. Azure Network Function Manager
- C. Azure Front Door
- D. Azure Virtual Network Manager

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

NEW QUESTION: 155

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

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

All the virtual networks are peered.

You deploy Azure Bastion to VNET2.

Which virtual machines can be protected by the bastion host?

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

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

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

NEW QUESTION: 156

You have an Azure subscription.

You plan to create a storage account.

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

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

Cmdlets

New-AzStorageAccountKey

New-AzStorageTable

Register-AzProviderFeature

New-AzStorageAccount

Register-AzResourceProvider

Answer Area

Answer:

Cmdlets

New-AzStorageAccountKey

New-AzStorageTable

Register-AzProviderFeature

New-AzStorageAccount

Register-AzResourceProvider

Answer Area

New-AzStorageAccount

New-AzStorageAccountKey

New-AzStorageTable

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: 157

You have an Azure subscription that uses Microsoft Defender for Cloud.

You have an Amazon Web Services (AWS) account.

You need to add the AWS account to Defender for Cloud.

What should you do first?

- A. From Defender for Cloud, configure the Environment settings.
- B. From Defender for Cloud, configure the Security solutions settings.
- C. From the AWS account, enable a security hub.
- D. From the Azure portal, add the AWS enterprise application.

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

NEW QUESTION: 158

You have an Azure subscription name Sub1 that contains an Azure Policy definition named Policy1. Policy1 has the following settings:

Definition location: Tenant Root Group

Category: Monitoring

You need to ensure that resources that are noncompliant with Policy1 are listed in the Azure Security Center dashboard.

What should you do first?

- A. Change the Category of Policy1 to Security Center.
- B. Add Policy1 to a custom initiative.
- C. Change the Definition location of Policy1 to Sub1.
- D. Assign Policy1 to Sub1.

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

Reference:

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

NEW QUESTION: 159

You have an Azure subscription that contains an Azure firewall named AzFW1. AzFW1 has a firewall policy named FWPolicy1. You need to add rule collections to FWPolicy1 to meet the following requirements:

- * Allow traffic based on the FQDN of the destination.
- * Allow TCP traffic.

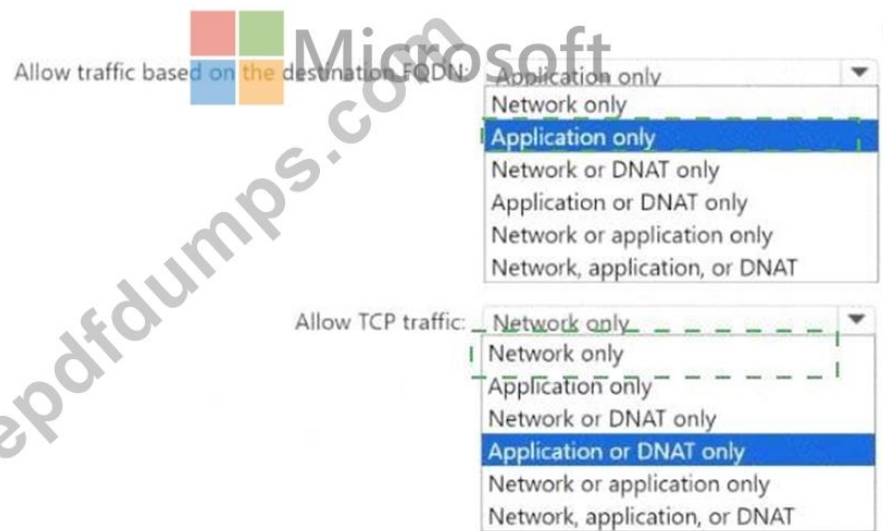
Which types of rule collections should you add for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Answer Area



Explanation:



NEW QUESTION: 160

You have an Azure subscription named Sub1. Sub1 contains a virtual network named VNet1 that contains one subnet named Subnet1.

You create a service endpoint for Subnet1.

Subnet1 contains an Azure virtual machine named VM1 that runs Ubuntu Server 18.04.

You need to deploy Docker containers to VM1. The containers must be able to access Azure Storage resources and Azure SQL databases by using the service endpoint.

- A. Create an application security group and a network security group (NSG).
- B. Edit the docker-compose.yml file.
- C. Install the container network interface (CNI) plug-in.

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

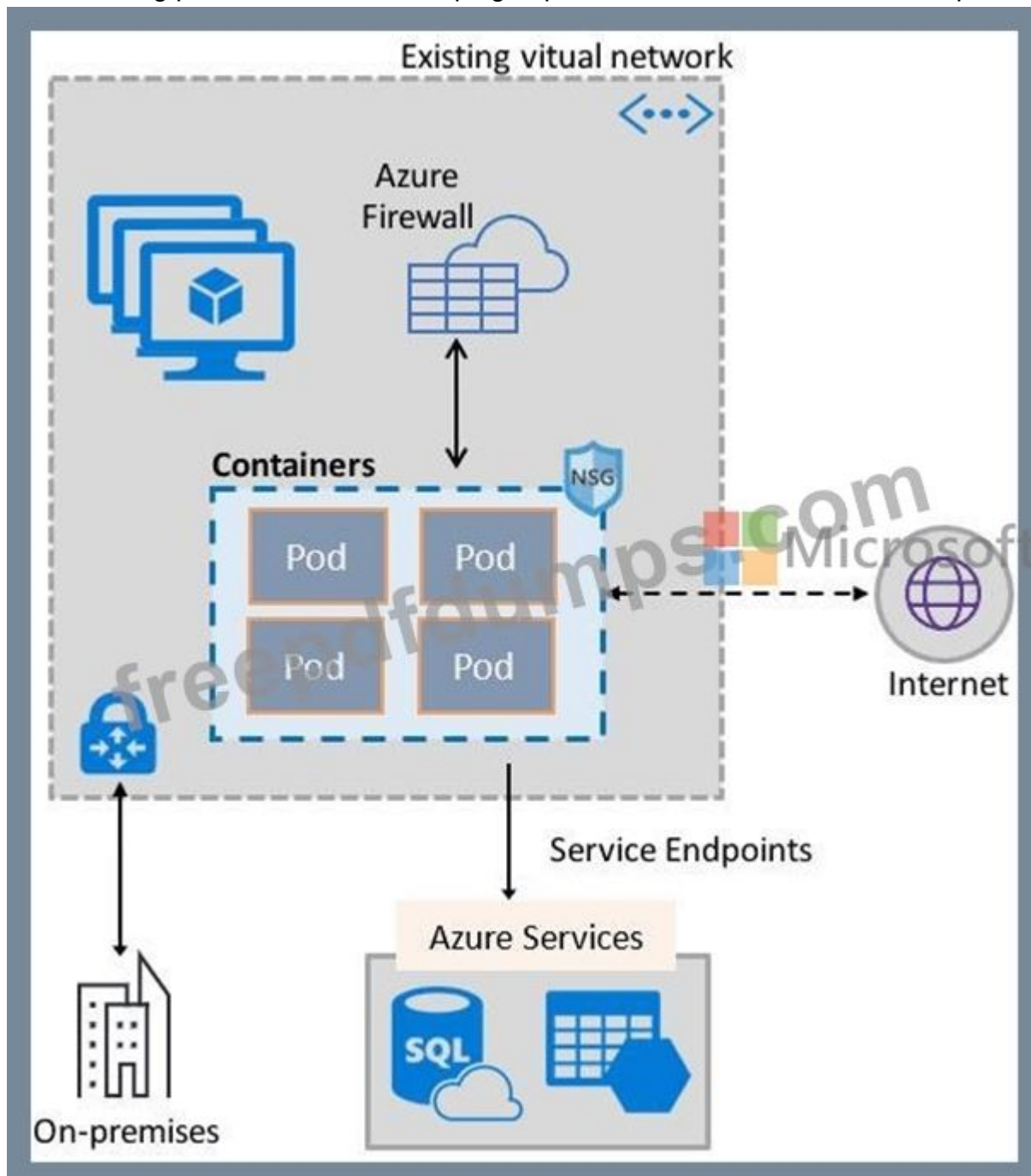
The Azure Virtual Network container network interface (CNI) plug-in installs in an Azure Virtual

Machine.

The plug-in supports both Linux and Windows platform.

The plug-in assigns IP addresses from a virtual network to containers brought up in the virtual machine, attaching them to the virtual network, and connecting them directly to other containers and virtual network resources. The plug-in doesn't rely on overlay networks, or routes, for connectivity, and provides the same performance as virtual machines.

The following picture shows how the plug-in provides Azure Virtual Network capabilities to Pods:



References:

<https://docs.microsoft.com/en-us/azure/virtual-network/container-networking-overview>

NEW QUESTION: 161

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains the

subnets shown in the following table.

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

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

Name	Connected to
VM1	Subnet1
VM2	Subnet2
VM3	Subnet3

VM3 contains a service that listens for connections on port 8080.

For VM1, you configure just-in-time (JIT) VM access as shown in the following exhibit.

Home > Just-in-time VM access >

JIT VM access configuration

VM1

+ Add Save X Discard

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

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

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

NOTE; Each correct selection is worth one point.

Answer Area

Statements	Yes	No
You can establish a Remote Desktop connection from VM1 to VM3 for a maximum of three hours.	☐	☐
You can establish a Remote Desktop connection from VM2 to VM1 after requesting access.	☐	☐
You can establish a Remote Desktop connection from VM3 to VM1 without requesting access.	☐	☐

Answer:

Answer Area

Statements	Yes	No
You can establish a Remote Desktop connection from VM1 to VM3 for a maximum of three hours.	☐	☒
You can establish a Remote Desktop connection from VM2 to VM1 after requesting access.	☒	☐
You can establish a Remote Desktop connection from VM3 to VM1 without requesting access.	☒	☐

Explanation:



Statements

You can establish a Remote Desktop connection from VM1 to VM3 for a maximum of three hours.

Yes

☐

No

☒

You can establish a Remote Desktop connection from VM2 to VM1 after requesting access.

☒
☐

You can establish a Remote Desktop connection from VM3 to VM1 without requesting access.

☒
☐
NEW QUESTION: 162

Your on-premises network contains the servers shown in the following table.

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

You have an Azure subscription That contains multiple virtual machines that run either Windows Server 2019 Of SLES.

Operating systems:

Windows Server only

SLES and Windows Server

Platforms:

Azure virtual machines and Hyper-V virtual machines only

Azure Arc-enabled servers and Azure virtual machines only

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

Answer:

Operating systems:

SLES only

Windows Server only

SLES and Windows Server

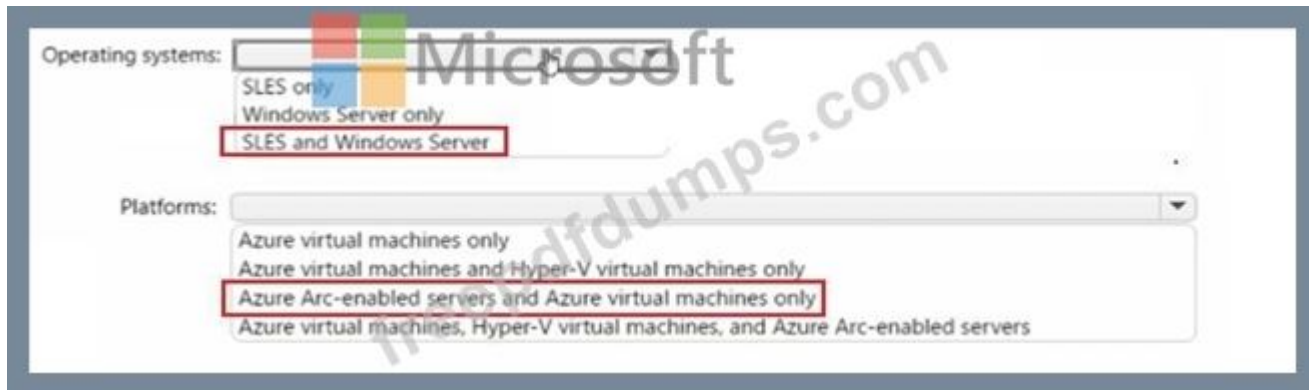
Platforms:

Azure virtual machines 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

Explanation:



NEW QUESTION: 163

You have an Azure SQL database named DB1 that contains a table named Table.

You need to configure DB1 to meet the following requirements;

- * Sensitive data in Table1 must be identified automatically.
- * Only the first character and last character of the sensitive data must be displayed in query results.

Which two features should you configure? To answer, select the features in the answer area.

NOTE: Each correct selection is worth one point.



 Performance recommendations

 Query Performance Insight

 Automatic tuning

Monitoring

 Alerts

 Metrics

 Diagnostic settings  Microsoft

 Logs

Answer:



DB1

SQL database



Auditing



Ledger



Data Discovery & Classification



Dynamic Data Masking



Microsoft Defender for Cloud



Transparent data encryption

Intelligent Performance



Performance overview



Performance recommendations



Query Performance Insight



Automatic tuning



Microsoft

Monitoring



Alerts



Metrics



Diagnostic settings



Logs

Explanation:

1. Data Discovery & Classification

2. Dynamic Data Masking

<https://learn.microsoft.com/en-us/azure/azure-sql/database/data-discovery-and-classification-overview?>

view=azuresql

Data Discovery & Classification is built into Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics. It provides basic capabilities for discovering, classifying, labeling, and reporting the sensitive data in your databases.

NEW QUESTION: 164

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

Name	Description
App1	Azure App Service app in a Premium plan
SQL1	Azure SQL managed instance
storage1	Azure Storage account
Function1	Azure Functions function in a Consumption plan

App1 uses Function 1, SQL1, and storage 1.

You need to secure the traffic between App1, Function1, SQL1. and storage1, by using private endpoints.

With which resources can App1 communicate by using a private endpoint?

- A. storage1 and Function1 only
- B. storage1 only
- C. Function1 only
- D. storage1, SQL1, and Function1
- E. SQL1 only
- F. SQL1 and storage1 only

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 165

You have an Azure subscription named Sub 1 that is associated to an Azure AD Tenant named contoso.com.

The tenant contains the users shown in the following table.

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

Each user is assigned an Azure AD Premium P2 license.

You plan to onboard and configure Azure AD Identity Protection.

Which users can onboard Azure AD Identity Protection, remediate users, and configure policies?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Microsoft

Users who can onboard Azure AD Identity Protection:

User1 only
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 User2 only
User1 and User3 only
User1, User 2, and User3 only
User1, User 2, User3, and User 4

Answer:

Answer Area

Users who can onboard Azure AD Identity Protection:

User1 only
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 User2 only
User1 and User3 only
User1, User 2, and User3 only
User1, User 2, User3, and User 4

Explanation:

Answer Area

Users who can onboard Azure AD Identity Protection:

User1 only

Users who can remediate users and configure policies:

User1 and User2 only

NEW QUESTION: 166

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a hybrid configuration of Azure Active Directory (Azure AD).

You have an Azure HDInsight cluster on a virtual network.

You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.

You need to configure the environment to support the planned authentication.

Solution: You deploy an Azure AD Application Proxy.

Does this meet the goal?

A. Yes

B. No

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>

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam!

Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (497 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 167

You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant.

From the Azure portal, you register an enterprise application.

Which additional resource will be created in Azure AD?

- A. a service principal
- B. an X.509 certificate
- C. a managed identity
- D. a user account

Answer: A (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 168

Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant. The tenant contains the users shown in the following table.

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

The tenant contains the groups shown in the following table.

Name	Members
Group1	User1, User2, User3
Group2	User2

You configure a multi-factor authentication (MFA) registration policy that and the following settings:

* Assignments:

* Include: Group1

* Exclude Group2

Controls: Require Azure MFA registration

Enforce Policy: On

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

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

Answer:

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

Explanation:

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

NEW QUESTION: 169

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

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

You create the Azure policies shown in the following table.

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

You create the resource locks shown in the following table.

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

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

NOTE: Each correct selection is worth one point.

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

Answer:

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

Explanation:

NO

NO

NO

1.) cannot perform write operation because following scope(s) are locked:

'subscriptions/xxxx/resourceGroups/xxx' Please remove the lock and try again.

2.) When creating a VM in a resource group with a Read Only lock an error is shown:

"The selected resource group is read only"

3.) Because of the read only lock virtual machines cannot be started nor stopped when the lock is added after the machine started. (not part of this use case, but still good to know.

The article referenced in the answer states different because that is scoped to blueprints.

In the Lock Resources pages is states the following regarding starting VMs:

"A ReadOnly lock on a resource group that contains a virtual machine prevents all users from starting or restarting the virtual machine. These operations require a POST request."

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources>

NEW QUESTION: 170

From the Azure portal, you are configuring an Azure policy.

You plan to assign policies that use the DeployIfNotExist, AuditIfNotExist, Append, and Deny effects.

Which effect requires a managed identity for the assignment?

- A. AuditIfNotExist
- B. Append
- C. DeployIfNotExist
- D. Deny

Answer: (SHOW ANSWER)

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

References:

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

NEW QUESTION: 171

You are testing an Azure Kubernetes Service (AKS) cluster. The cluster is configured as shown in the exhibit.

(Click the Exhibit tab.)

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

You plan to deploy the cluster to production. You disable HTTP application routing.

You need to implement application routing that will provide reverse proxy and TLS termination for AKS services by using a single IP address.

What should you do?

- A. Create an AKS Ingress controller.
- B. Install the container network interface (CNI) plug-in.
- C. Create an Azure Standard Load Balancer.
- D. Create an Azure Basic Load Balancer.

Answer: A (LEAVE A REPLY)

An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services.

References:

<https://docs.microsoft.com/en-us/azure/aks/ingress-tls>

NEW QUESTION: 172

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure Subscription named Sub1.

You have an Azure Storage account named Sa1 in a resource group named RG1.

Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.

You discover that unauthorized users accessed both the file service and the blob service.

You need to revoke all access to Sa1.

Solution: You generate new SASs.

Does this meet the goal?

A. Yes

B. No

Answer: B (LEAVE A REPLY)

Instead you should create a new stored access policy.

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: 173

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

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

VNET1, VNET2, and VNET3 are peered with each other. You perform the following actions:

- * Create two application security groups named ASG1 and ASG2 in the West US region.
- * Add the network interface of VM1 to ASG1.

Answer Area

ASG1:

ASG2:

Microsoft

Answer:

see the answer below in explanation.

Explanation:

Answer as below.

ASG1: VM2, VM3, and VM4 only

ASG2: VM1, VM2, and VM4 only

**NEW QUESTION: 174**

You need to ensure that you can meet the security operations requirements.

What should you do first?

- A. Turn on Auto Provisioning in Security Center.
- B. Integrate Security Center and Microsoft Cloud App Security.
- C. Upgrade the pricing tier of Security Center to Standard.
- D. Modify the Security Center workspace configuration.

Answer: 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>

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 Subnet1.3
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: 175

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription named Sub1.

You have an Azure Storage account named sa1 in a resource group named RG1.

Users and applications access the blob service and the file service in sa1 by using several shared access signatures (SASs) and stored access policies.

You discover that unauthorized users accessed both the file service and the blob service.

You need to revoke all access to sa1.

Solution: You regenerate the Azure storage account access keys.

Does this meet the goal?

A. Yes

B. No

Answer: A (LEAVE A REPLY)

Generating new storage account keys will invalidate all SAS's that were based on the previous

keys.

NEW QUESTION: 176

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

Name	Type	Description
EventHub1	Azure Event Hubs	Not applicable
Adf1	Azure Data Factory	Not applicable
NVA1	Network virtual appliance (NVA)	The NVA sends security event messages in the Common Event Format (CEF).

You have an Azure subscription named Subscription2 that contains the following resources:

- * An Azure Sentinel workspace
- * An Azure Event Grid instance

You need to ingest the CEF messages from the NVAs to Azure Sentinel.

What should you configure for each subscription? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Subscription1:

- An Azure Log Analytics agent on a Linux virtual machine
- A Data Factory pipeline
- An Event Hubs namespace
- An Azure Service Bus queue

Subscription2:

- A new Azure Log Analytics workspace
- A new Azure Sentinel data connector
- A new Azure Sentinel playbook
- A new Event Grid resource provider

Answer:

Subscription1:

- An Azure Log Analytics agent on a Linux virtual machine
- A Data Factory pipeline
- An Event Hubs namespace
- An Azure Service Bus queue

Subscription2:

- A new Azure Log Analytics workspace
- A new Azure Sentinel data connector
- A new Azure Sentinel playbook
- A new Event Grid resource provider

Explanation:

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

Subscription1:

- An Azure Log Analytics agent on a Linux virtual machine
- A Data Factory pipeline
- An Event Hubs namespace
- An Azure Service Bus queue

Subscription2:

- A new Azure Log Analytics workspace
- A new Azure Sentinel data connector
- A new Azure Sentinel playbook
- A new Event Grid resource provider

NEW QUESTION: 177

You have an Azure subscription that contains the following resources:

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

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

How should you configure Azure Sentinel to meet the requirements? To answer, drag the appropriate components to the correct requirements. Each component may be used once, more than once, or not at all.

You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Components	Answer Area
A data connector for Security Center	Enable alert notifications from Security Center
A data connector for the firewall software	Create an incident:
A playbook	Initiate a script to configure the firewall rule:
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: 178

You plan to deploy an app that will modify the properties of Azure Active Directory (Azure AD) users by using Microsoft Graph. You need to ensure that the app can access Azure AD. What should you configure first?

- A. a custom role-based access control (RBAC) role
- B. an external identity
- C. an Azure AD Application Proxy
- D. an app registration

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

Reference:

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

NEW QUESTION: 179

You have a Microsoft Sentinel deployment.

You need to connect a third-party security solution to the deployment. The third-party solution will send Common Event Format (CEF-formatted messages).

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

NOTE: Each correct selection is worth one point.

Answer Area

Deploy:

Forward events to Microsoft Sentinel by using:

Answer:

See the answer below at Explanation.

Explanation:

Answer is as image below.

Answer Area

Deploy:

Forward events to Microsoft Sentinel by using:

NEW QUESTION: 180

Your network contains an on-premises Active Directory domain named adatum.com that syncs to a Microsoft Entra tenant.

The Microsoft Entra tenant contains the users shown in the following table.

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

You configure the Microsoft Entra Password Protection settings for adatum.com as shown in the following exhibit.

Custom smart lockout

Lockout threshold

Lockout duration in seconds

Custom banned passwords

Enforce custom list ☒ Yes ☐ No

Custom banned password list

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ☒ Yes ☐ No

Mode ☐ Enforced ☒ Audit

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

NOTE: Each correct selection is worth one point.

Answer Area

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

Answer:

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

Explanation:

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: 181

You have an Azure subscription that uses Microsoft Defender for Cloud.

You have an Amazon Web Service (AWS) account named AWS1 that is connected to defender for Cloud.

You need to ensure that AWS foundational Security Best Practices. The solution must minimize administrative effort.

What should do you in Defender for Cloud?

- A. Create a new custom standard.
- B. Assign a built-in assessment.
- C. Create a new customer assessment.
- D. Assign a built-in compliance standard.

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

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam!

Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (497 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 182

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

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

You configure an access review named Review1 as shown in the following exhibit.

Create an access review

Access reviews enable reviewers to attest to users access.

* Review name

Description

* Start date

Frequency

Duration in days

End

* Number of times

* End date

Users

Scope ☒ Everyone

* Review role membership

Reviewers

Reviewers

Upon completion settings

Auto apply results to resource

Should reviewer not respond

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

NOTE: Each correct selection is worth one point.

User3 can perform Review1 for

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

If User2 fails to complete Review1 by March 20, 2019

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

Answer:

User3 can perform Review1 for

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

If User2 fails to complete Review1 by March 20, 2019

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

Explanation:

User3 can perform Review1 for

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

If User2 fails to complete Review1 by March 20, 2019

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

Box 1: User3 only

Use the Members (self) option to have the users review their own role assignments.

Box 2: User3 will receive a confirmation request

Use the Should reviewer not respond list to specify what happens for users that are not reviewed by the reviewer within the review period. This setting does not impact users who have been reviewed by the reviewers manually. If the final reviewer's decision is Deny, then the user's access will be removed.

No change - Leave user's access unchanged

Remove access - Remove user's access

Approve access - Approve user's access

Take recommendations - Take the system's recommendation on denying or approving the user's continued access

References:

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review>

NEW QUESTION: 183

You have an Azure subscription that contains an Azure key vault named Vault1.

In Vault1, you create a secret named Secret1.

An application developer registers an application in Azure Active Directory (Azure AD).

You need to ensure that the application can use Secret1.

What should you do?

- A. In Azure AD, create a role.
- B. In Azure Key Vault, create a key.
- C. In Azure Key Vault, create an access policy.
- D. In Azure AD, enable Azure AD Application Proxy.

Answer: C (LEAVE A REPLY)

"You may need to configure the target resource to allow access from your application. For example, if you request a token to Key Vault, you need to make sure you have added an access policy that includes your application's identity. Otherwise, your calls to Key Vault will be rejected, even if they include the token"

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

NEW QUESTION: 184

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

You do not have access



Access denied

You do not have access

You don't have permission to register applications in the sk200510outlook (Default Directory) directory. To request access, contact your administrator.

Summary



Session ID
f8e55e67d10141b4bf0c7ac5115b3be7

Extension
Microsoft_AAD_RegisteredApps

Error code
403

Resource ID
Not available

Content
CreateApplicationBlade



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

What should you do for the tenant?

- A.** Modify the User settings
- B.** Set Enable Security default to Yes.

C. Modify the Directory properties.

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

Answer: A (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 185

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

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

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

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

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

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

Microsoft

Answer:

Answer Area

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

Microsoft

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: 186

You have an Azure environment.

You need to identify any Azure configurations and workloads that are non-compliant with ISO 27001:2013 standards.

What should you use?

- A. Microsoft Sentinel
- B. Microsoft Defender for Cloud
- C. Microsoft Defender for Identity
- D. Azure Active Directory (Azure AD) Identity Protection

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

NEW QUESTION: 187

You have a web app named WebApp1.

You create a web application firewall (WAF) policy named WAF1.

You need to protect WebApp1 by using WAF1.

What should you do first?

- A. Deploy an Azure Front Door.
- B. Add an extension to WebApp1.
- C. Deploy Azure Firewall.

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

References:

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

NEW QUESTION: 188

You have an Azure subscription named Sub1.

You create a virtual network that contains one subnet. On the subnet, you provision the virtual machines shown in the following table.

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

Currently, you have not provisioned any network security groups (NSGs).

You need to implement network security to meet the following requirements:

- * Allow traffic to VM4 from VM3 only.
- * Allow traffic from the Internet to VM1 and VM2 only.

* Minimize the number of NSGs and network security rules.

How many NSGs and network security rules should you create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

NSGs: 1

Network security rules: 3

Answer:

NSGs: 1

Network security rules: 3

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: 189

You have an Azure subscription.

You configure Microsoft Sentinel to use multiple data sources.

You need to create analytic rules that meet the following requirements:

* Rule 1: Automatically match Common Event Format (CEF) logs and syslog data with domain, IP address, and URL indicators.

* Rule 2: Use Microsoft proprietary algorithms.

Which type of detection should you use for each rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

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

Answer:

Answer Area

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: 190

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

Subnet1 and Subnet2 have a network security group (NSG). The NSG has an outbound rule that has the following configurations:

* Port; Any

- * Source: Any
- * Priority: 100
- * Action: Deny
- * Protocol: Any
- * Destination: Storage

The subscription contains a storage account named storage1.

You create a private endpoint named Private1 that has the following settings:

- * Resource type: Microsoft.Storage/storageAccounts
- * Resource: storage1
- * Target sub-resource: blob
- * Virtual network: VNet1
- * Subnet: Subnet1

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

NOTE: Each correct selection is worth one point.

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

Answer:

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

Explanation:

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

NEW QUESTION: 191

You have Azure Resource Manager templates that you use to deploy Azure virtual machines. You need to disable unused Windows features automatically as instances of the virtual machines are provisioned.

What should you use?

- A. device compliance policies in Microsoft Intune
- B. Azure Automation State Configuration
- C. application security groups
- D. Azure Advisor

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

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

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

References:

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

NEW QUESTION: 192

You have an Azure subscription that contains an Azure SQL server named sqlsrv1 and an Azure SQL database named DB1. Sqlsrv1 is configured for Microsoft Entra authentication only.

You have the Microsoft Entra identities shown in the following table.

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

Which users can create scoped credentials for DB1?

- A. User1, User2, and User3
- B. User1 only
- C. User1 and User2 only

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

NEW QUESTION: 193

You have an Azure AD tenant.

You plan to implement an authentication solution to meet the following requirements:

- * Require number matching.
- * Display the geographical location when signing in.

Which authentication method should you include in the solution?

- A. SMS
- B. FID02 security key
- C. Temporary Access Pass
- D. Microsoft Authenticator

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

NEW QUESTION: 194

You have a Microsoft Entra tenant that contains a user named User1.

You plan to enable passwordless authentication for the tenant.

You need to ensure that User1 can enable the combined registration experience. The solution must use the principle of least privilege.

Which role should you assign to User1?

- A. Global Administrator
- B. Privileged Role Administrator
- C. Authentication Administrator
- D. Security Administrator

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

NEW QUESTION: 195

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

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

You need to configure network connectivity to meet the following requirements:

- * Communication from VM1 to storage1 must traverse an optimized Microsoft backbone network.
- * All the outbound traffic from VM1 to the internet must be denied.
- * The solution must minimize costs and administrative effort

What should you configure for VNet1 and NSG1? To answer, drag the appropriate components to the correct resources. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content NOTE: Each correct selection is worth one point.

Answer:

Components

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

Answer Area

VNet1: A service tag

NSG1: A private endpoint

Explanation:

Components

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

Answer Area

VNet1: A service tag

NSG1: A private endpoint

NEW QUESTION: 196

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

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

You have an Azure Virtual Network Manager instance that has the following settings:

- * Name: NetMgr1
- * Region: East US
- * Features: Connectivity
- * Management scope: Sub1

For NetMgr1, you create the target network groups shown in the following table.

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

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

NOTE; Each correct selection is worth one point.

Answer Area

Statements

You can add VNet1 to Group2.

You can add VNet2 to Group1.

You can add Subnet3 to Group3.

Yes

No

Answer:

Answer Area

Microsoft

Statements

You can add VNet1 to Group2.

You can add VNet2 to Group1.

You can add Subnet3 to Group3.

Yes No

☐ ☐

☐ ☐

☐ ☐

Explanation:

Answer Area

Microsoft

Statements

You can add VNet1 to Group2.

You can add VNet2 to Group1.

You can add Subnet3 to Group3.

Yes No

☒ ☐

☐ ☒

☒ ☐

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam!

Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (497 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 197

Your network contains an Active Directory forest named contoso.com. You have an Azure Directory (Azure AD) tenant named contoso.com.

You plan to configure synchronization by using the Express Settings installation option in Azure AD Connect.

You need to identify which roles and groups are required to perform the planned configurations. The solution must use the principle of least privilege.

Which two roles and groups should you identify? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. the Domain Admins group in Active Directory
- B. the Security administrator role in Azure AD
- C. the Global administrator role in Azure AD
- D. the User administrator role in Azure AD
- E. the Enterprise Admins group in Active Directory

Answer: (SHOW ANSWER)

References:

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

NEW QUESTION: 198

You have an Azure web app named WebApp1.

You upload a certificate to WebApp1.

You need to make the certificate accessible to the app code of WebApp1.

What should you do?

- A. Enable system-assigned managed identity for the WebApp1.
- B. Add an app setting to the WebApp1 configuration.
- C. Configure the TLS/SSL binding for WebApp1.
- D. Add a user-assigned managed identity to WebApp1.

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

Reference:

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

NEW QUESTION: 199

You have an Azure subscription that contains a key vault and an Azure SQL server.

You need to deploy an Azure SQL database that uses Transparent Data Encryption (TDE) and a customer-managed key.

What should you create before you deploy the database?

- A. A user-assigned managed identity
- B. An app registration
- C. A standard general-purpose v2 storage account
- D. A user account that is assigned the SQL Security Manager role

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

NEW QUESTION: 200

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1.

You plan to publish several apps in the tenant.

You need to ensure that User1 can grant admin consent for the published apps.

Which two possible user roles can you assign to User1 to achieve this goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Application developer
- B. Security administrator
- C. Application administrator
- D. User administrator
- E. Cloud application administrator

Answer: ([SHOW ANSWER](#))

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent>

NEW QUESTION: 201

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

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

The subscription contains Azure web app named WebApp1 that has the following configurations.

- * Region West Us
- * Virtual network VNet1
- * VNet integration on: Enabled
- * Outbound subnet: Subnet11
- * Windows plan (West US): ASP1

You plan to deploy an Azure web app named WebApp2 that will have the following settings:

- * Region: West US
- * VNet integration on-Enabled
- * Windows plan (West UAS): WebApp2?

To which subnets can you integrate WebApp2?

- A. Subnet11 only
- B. Subnet11 or subnet12 only
- C. Subnet11, subnet2, or Subnet21
- D. Subnet2 only
- E. Subnet2 or Subnet21 only

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

NEW QUESTION: 202

You need to configure SQLDB1 to meet the data and application requirements.

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

Actions

Answer Area

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.



Microsoft



Answer:

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

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

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

In SQLDB1, create contained database users.

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: 203

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

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

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

Name	Owner	Users and groups
App1	User3	User4
App2	User4	User3

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

Answer Area

App1:
User1 only
User1 and User2 only
User1 and User3 only
User1, User2, and User3 only
User1, User2, User3, and User4

App2:
User1 only
User1 and User2 only
User1 and User4 only
User1, User2, and User4 only
User1, User2, User3, and User4

Answer:

Answer Area

App1:
User1 only
User1 and User2 only
User1 and User3 only
User1, User2, and User3 only
User1, User2, User3, and User4

App2:
User1 only
User1 and User2 only
User1 and User4 only
User1, User2, and User4 only
User1, User2, User3, and User4



Explanation:

Answer Area

App1:
App2:



NEW QUESTION: 204

You have an Azure subscription.

You create an Azure web app named Contoso1812 that uses an S1 App service plan.

You create a DNS record for www.contoso.com that points to the IP address of Contoso1812.

You need to ensure that users can access Contoso1812 by using the https://www.contoso.com URL.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Turn on the system-assigned managed identity for Contoso1812.
- B. Add a hostname to Contoso1812.
- C. Scale out the App Service plan of Contoso1812.
- D. Add a deployment slot to Contoso1812.

E. Scale up the App Service plan of Contoso1812.

F. Upload a PFX file to Contoso1812

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

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

A root "A" record pointing to `contoso.com`

A root "TXT" record for verification

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

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

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

NEW QUESTION: 205

You have an Azure subscription.

You plan to deploy a new Conditional Access policy named CAPolicy1.

You need to use the What If tool to evaluate how CAPolicy1 will affect user1. The solution must minimize the impact of CAPolicy1 on the users.

To what should you set the Enable policy setting for CAPolicy1?

A. Report only

B. Off

C. On

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

NEW QUESTION: 206

You have an Azure subscription that uses Microsoft Sentinel.

You need to create a Microsoft Sentinel notebook that will use the Guided Investigation - Anomaly Lookup template.

What should you create first?

A. a Log Analytics workspace

B. an Azure Machine Learning workspace

C. an analytics rule

D. a hunting query

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

NEW QUESTION: 207

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

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

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

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

You create the resources shown in the following table.

Name	Type
storage1	Azure Storage account
Vault1	Azure Key Vault

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements

Connections from VM1 to storage1 always use IP address 10.1.1.5.

Yes

☐

No

☐

Connections from VM2 to Vault1 always use IP address 20.224.219.230.

☐
☐

Authentication from VM3 to the tenant uses either IP address 10.11.1.5 or 40.122.155.212.

☐
☐

Answer:

Answer Area

Statements

Connections from VM1 to storage1 always use IP address 10.1.1.5.

Yes

☒

No

☐

Connections from VM2 to Vault1 always use IP address 20.224.219.230.

☐
☒

Authentication from VM3 to the tenant uses either IP address 10.11.1.5 or 40.122.155.212.

Yes

☒

No

☐

Explanation:

Statements	Yes	No
Connections from VM1 to storage1 always use IP address 10.1.1.5.	☐	☒
Connections from VM2 to Vault1 always use IP address 20.224.219.230.	☐	☒
Authentication from VM3 to the tenant uses either IP address 10.11.1.5 or 40.122.155.212.	☒	☐

NEW QUESTION: 208

You have a web app hosted on an on-premises server that is accessed by using a URL of <https://www.contoso.com>. You plan to migrate the web app to Azure. You will continue to use

<https://www.contoso.com>. You need to enable HTTPS for the Azure web app. What should you do first?

- A. Export the public key from the on-premises server and save the key as a P7b file.
- B. Export the private key from the on-premises server and save the key as a PFX file that is encrypted by using TripleDES.
- C. Export the public key from the on-premises server and save the key as a CER file.
- D. Export the private key from the on-premises server and save the key as a PFX file that is encrypted by using AES256.

Answer: ([SHOW ANSWER](#))

<https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate#private-certificate-requirements>

Valid AZ-500 Dumps shared by Actual4test.com for Helping Passing AZ-500 Exam!

Actual4test.com now offer the **newest AZ-500 exam dumps**, the Actual4test.com AZ-500 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-500 dumps with Test Engine here:

https://www.actual4test.com/AZ-500_examcollection.html (497 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)