

Microsoft.AZ-500.v2025-01-29.q426

Exam Code:	AZ-500
Exam Name:	Microsoft Azure Security Technologies
Certification Provider:	Microsoft
Free Question Number:	426
Version:	v2025-01-29
# of views:	2676
# of Questions views:	4260
https://www.freepdfdumps.com/Microsoft.AZ-500.v2025-01-29.q426.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.

☐☒

Reference:

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

NEW QUESTION: 2

You have an Azure subscription that contains an Azure Sentinel workspace.

Azure Sentinel is configured to ingest logs from several Azure workloads. A third-party service management platform is used to manage incidents.

You need to identify which Azure Sentinel components to configure to meet the following requirements:

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

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

Which component should you identify for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

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

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

Analytics
Data connectors
Playbooks
Workbooks

Analytics
Data connectors
Playbooks
Workbooks

Answer:

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

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

Analytics
Data connectors
Playbooks
Workbooks

Analytics
Data connectors
Playbooks
Workbooks

Reference:

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

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

NEW QUESTION: 3

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



Microsoft

Answer:

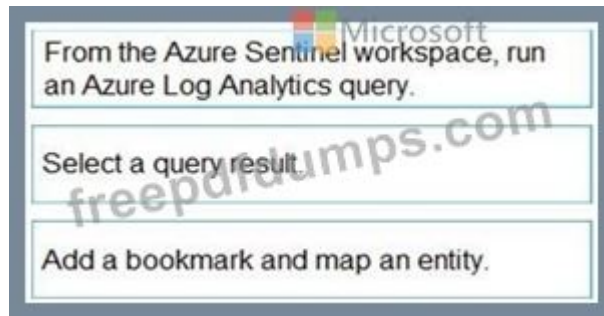
Resource provider:

Microsoft.Authorization
Microsoft.Resources
Microsoft.Support

Assignable scope:

/
/Group1
/subscriptions/11111111-1234-1234-1234-111111111111

Explanation



Reference:

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

NEW QUESTION: 4

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 (AzureAD).

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 create a site-to-site VPN between the virtual network and the on-premises network.

Does this meet the goal?

A. Yes

B. No

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

You can connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.

Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:

- * Create Azure Virtual Network.
- * Create a custom DNS server in the Azure Virtual Network.
- * Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.
- * Configure forwarding between the custom DNS server and your on-premises DNS server.

References:

<https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network>

NEW QUESTION: 5

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



Microsoft

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: 6

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

NEW QUESTION: 7

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

- 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

Answer:

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

Explanation

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

NEW QUESTION: 8

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

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 Area

 Microsoft

⏪

⏩

⏴

⏵

Consent to PIM.

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

Sign up PIM for Azure AD roles.

Answer:

Answer Area

 Microsoft

Consent to PM.

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

Sign up PIM for Azure AD roles.

- 1 - Consent to PM.
- 2 - Verify your indentity by using multi-factor authentication (MFA).
- 3 - Sign up PIM for Azure AD roles.

Reference:

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

NEW QUESTION: 9

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

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

You need to configure authorization access.

Which authorization types can you use for each storage account? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

storage1:	▼ Shared Key only Shared access signature (SAS) only Azure Active Directory (Azure AD) only Shared Key and shared access signature (SAS) only Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)
storage2:	▼ Shared Key only Shared access signature (SAS) only Shared Key and shared access signature (SAS)
storage3:	▼ Shared Key only Shared access signature (SAS) only Azure Active Directory (Azure AD) only Shared Key and shared access signature (SAS) only Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

Answer:

storage1:

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

storage2:

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

storage3:

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

Reference:

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

NEW QUESTION: 10

You have 20 Azure subscriptions and a security group named Group1. The subscriptions are children of the root management group.

Each subscription contains a resource group named RG1.

You need to ensure that for each subscription RG1 meets the following requirements:

The members of Group1 are assigned the Owner role.

The modification of permissions to RG1 is prevented.

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

NOTE: Each correct selection is worth one point.

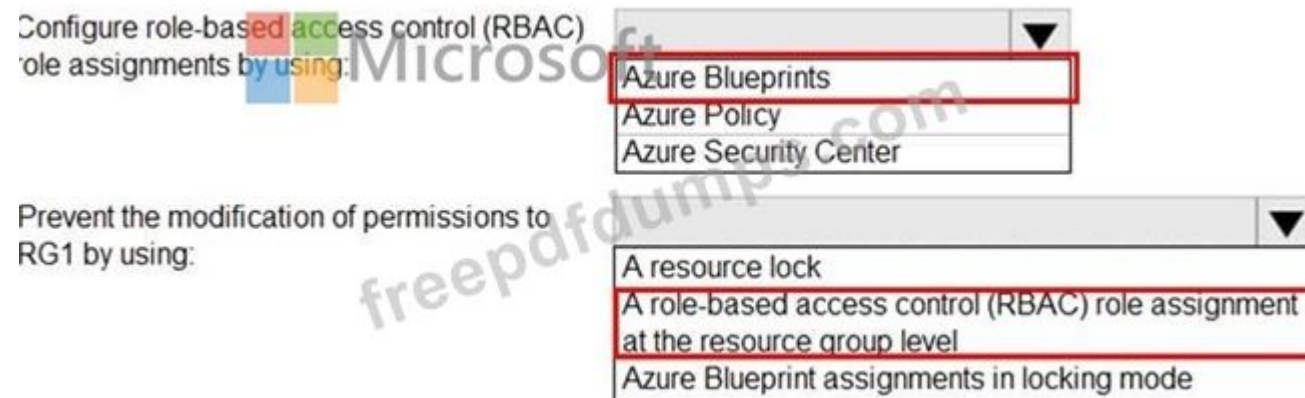
Configure role-based access control (RBAC) role assignments by using:

	▼
Azure Blueprints	
Azure Policy	
Azure Security Center	

Prevent the modification of permissions to RG1 by using:

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

Answer:



NEW QUESTION: 11

You plan to use Azure Disk Encryption for several virtual machine disks.

You need to ensure that Azure Disk Encryption can retrieve secrets from the KeyVault11641655 Azure key vault.

To complete this task, sign in to the Azure portal and modify the Azure resources.

Answer:

See the explanation below.

Explanation

1. In the Azure portal, type Key Vaults in the search box, select Key Vaults from the search results then select KeyVault11641655. Alternatively, browse to Key Vaults in the left navigation pane.
2. In the Key Vault properties, scroll down to the Settings section and select Access Policies.
3. Select the Azure Disk Encryption for volume encryption



4. Click Save to save the changes.

NEW QUESTION: 12

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](#))

Explanation/Reference:

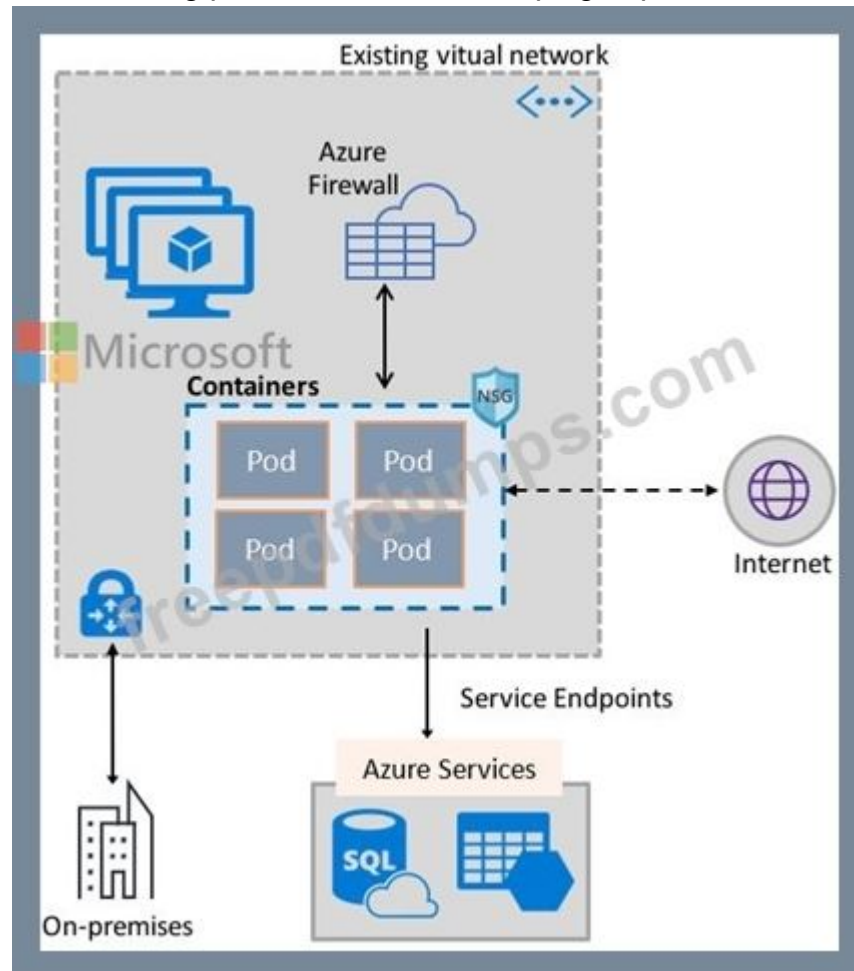
Explanation:

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: 13

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

Explanation

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.

NEW QUESTION: 14

You are implementing conditional access policies.

You must evaluate the existing Azure Active Directory (Azure AD) risk events and risk levels to configure and implement the policies.

You need to identify the risk level of the following risk events:

- * Users with leaked credentials
- * Impossible travel to atypical locations
- * Sign ins from IP addresses with suspicious activity

Which level should you identify for each risk event? To answer, drag the appropriate levels to the correct risk events. Each level 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.

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

Answer:

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

Explanation

Medium

High

Medium

Refer

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

NEW QUESTION: 15

You suspect that users are attempting to sign in to resources to which they have no access.

You need to create an Azure Log Analytics query to identify failed user sign-in attempts from the last three days. The results must only show users who had more than five failed sign-in attempts.

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

NOTE: Each correct selection is worth one point.

```
let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AccountType == 'User' and [dropdown] == 4625
| Summarize failed_login_attempts= [dropdown]
latest_failed_login=arg_max(TimeGenerated by Account
| where failed_login_attempts > 5
```

Answer:

```
let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AccountType == 'User' and [dropdown] == 4625
| Summarize failed_login_attempts= [dropdown]
latest_failed_login=arg_max(TimeGenerated by Account
| where failed_login_attempts > 5
```

Explanation


```

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

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

```

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

```

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

```

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

NEW QUESTION: 16

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.	☐	☒

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 (517 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 17

You have an Azure subscription named Sub 1 that is associated to an Azure Active Directory (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

Users who can onboard Azure AD Identity Protection:

- User1 only
- User1 and User2 only
- User1, User 2, and User3 only
- User1, User 2, User3, and User 4 only

Users who can remediate users and configure policies:

- User1 and User2 only
- User1 and User3 only
- User1, User 2, and User3 only
- User1, User 2, User3, and User 4

Answer:

Answer Area

Users who can onboard Azure AD Identity Protection:

- User1 only
- User1 and User2 only
- User1, User 2, and User3 only
- User1, User 2, User3, and User 4 only

Users who can remediate users and configure policies:

- User1 and User2 only
- User1 and User3 only
- User1, User 2, and User3 only
- User1, User 2, User3, and User 4

Explanation:

Users who can onboard Azure AD Identity Protection:

User1 only

User1 and User2 only

User1, User2, and User3 only

User1, User2, User3, and User4 only

Users who can remediate users and configure policies:

User1 and User2 only

User1 and User3 only

User1, User2, and User3 only

User1, User2, User3, and User4

NEW QUESTION: 18

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. You plan to implement an application that will consist of the resources shown in the following table.

Name	Type	Description
CosmosDBAccount1	Azure Cosmos DB account	A Cosmos DB account containing a database named CosmosDB1 that serves as a back-end tier of the application
WebApp1	Azure web app	A web app configured to serve as the middle tier of the application

Users will authenticate by using their Azure AD user account and access the Cosmos DB account by using resource tokens.

You need to identify which tasks will be implemented in CosmosDB1 and WebApp1.

Which task should you identify for each resource? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

CosmosDB1:

▼

☐

Authenticate Azure AD users and generate resource tokens.

☐

Authenticate Azure AD users and relay resource tokens.☐

WebApp1:

▼

☐

Authenticate Azure AD users and generate resource tokens.

☒

Authenticate Azure AD users and relay resource tokens.

☒

Create database users and generate resource tokens.

Answer:

Microsoft

CosmosDB1:

▼

☐

Authenticate Azure AD users and generate resource tokens.

☐

Authenticate Azure AD users and relay resource tokens.

☐

Create database users and generate resource tokens.

WebApp1:

▼

☐

Authenticate Azure AD users and generate resource tokens.

☒

Authenticate Azure AD users and relay resource tokens.

☒

Create database users and generate resource tokens.

Explanation

CosmosDB1:

Authenticate Azure AD users and generate resource tokens.
Authenticate Azure AD users and relay resource tokens.
Create database users and generate resource tokens.

WebApp1:

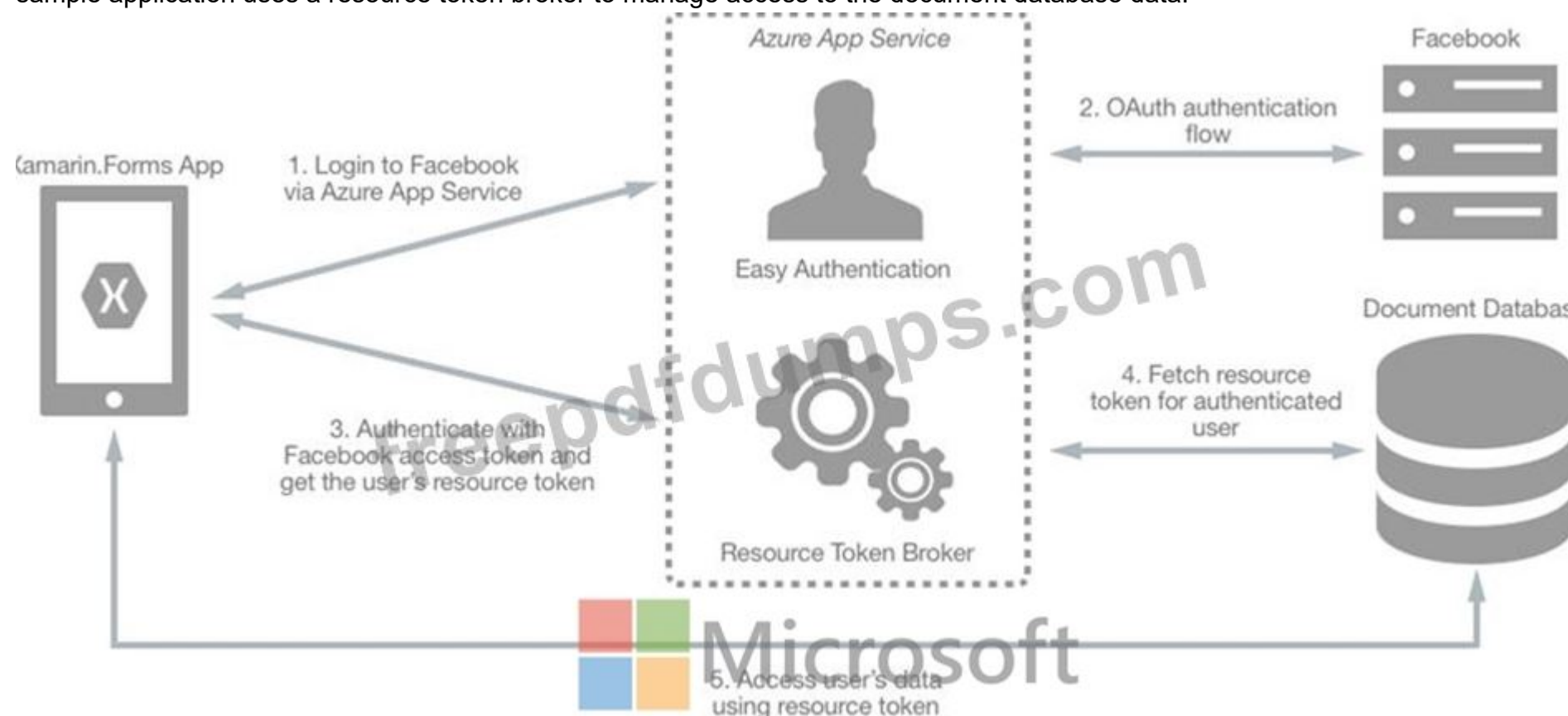
Authenticate Azure AD users and generate resource tokens.
Authenticate Azure AD users and relay resource tokens.
Create database users and generate resource tokens.

CosmosDB1: Create database users and generate resource tokens.

Azure Cosmos DB resource tokens provide a safe mechanism for allowing clients to read, write, and delete specific resources in an Azure Cosmos DB account according to the granted permissions.

WebApp1: Authenticate Azure AD users and relay resource tokens

A typical approach to requesting, generating, and delivering resource tokens to a mobile application is to use a resource token broker. The following diagram shows a high-level overview of how the sample application uses a resource token broker to manage access to the document database data:



References:

<https://docs.microsoft.com/en-us/xamarin/xamarin-forms/data-cloud/cosmosdb/authentication>

NEW QUESTION: 19

You are evaluating the security of VM1, VM2, and VM3 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 the Internet, you can connect to the web server on VM1 by using HTTP.	☐	☐
From the Internet, you can connect to the web server on VM2 by using HTTP.	☐	☐
From the Internet, you can connect to the web server on VM3 by using HTTP.	☐	☐

Answer:

Answer Area

Statements	Yes	No
From the Internet, you can connect to the web server on VM1 by using HTTP.	☒	☐
From the Internet, you can connect to the web server on VM2 by using HTTP.	☐	☒
From the Internet, you can connect to the web server on VM3 by using HTTP.	☒	☐

NEW QUESTION: 20

You have an Azure subscription that contains the following resources:

A virtual network named VNET1 that contains two subnets named Subnet1 and Subnet2.

A virtual machine named VM1 that has only a private IP address and connects to Subnet1.

You need to ensure that Remote Desktop connections can be established to VM1 from the internet.

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 a network security group (NSG).	
Create a network rule collection.	
Create a NAT rule collection.	
Create a new subnet.	
Deploy Azure Application Gateway.	
Deploy Azure Firewall.	

Answer:

Actions	Answer Area
Configure a network security group (NSG).	
Create a network rule collection.	
Create a NAT rule collection.	
Create a new subnet.	
Deploy Azure Application Gateway.	
Deploy Azure Firewall.	

Explanation

Create a new subnet.
Deploy Azure Firewall.
Create a NAT rule collection.

NEW QUESTION: 21

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	10.1.1.4	13.80.73.87
VM2	VNET2/Subnet2	10.2.1.4	213.199.133.190
VM3	VNET2/Subnet2	10.2.1.5	None

Subnet1 and Subnet2 have a Microsoft.Storage service endpoint configured.

You have an Azure Storage account named storageacc1 that is configured as shown in the following exhibit.

Save X Discard Refresh

Allow access from

☐ All networks ☒ Selected networks

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

Virtual networks

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

[+ Add new virtual network](#)

VIRTUAL NETWORK	SUBNET	ADDRESS RANGE	ENDPOINT STATUS	RESOURCE GROUP	SUBSCRIPTION
No network selected.					

Firewall

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

Address Range

13.80.73.87

IP address or CIDR

Exceptions

☒ Allow trusted Microsoft services to access this storage account ⓘ

☐ Allow read access to storage logging from any network

☐ Allow read access to storage metrics from any network

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

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

Answer:

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

Reference:

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

NEW QUESTION: 22

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>

NEW QUESTION: 23

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:  Microsoft

- 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

NEW QUESTION: 24

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.

Update1:

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

Update2:

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

Answer:

Update1:

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

Update2:

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

Explanation:

Update1: VM1 and VM2 only

VM3: Windows Server 2016 West US RG2

Update2: VM4 and VM5 only

VM6: CentOS 7.5 East US RG1

For Linux, the machine must have access to an update repository. The update repository can be private or public.

References:

<https://docs.microsoft.com/en-us/azure/automation/automation-update-management>

NEW QUESTION: 25

You create a new Azure subscription.
You need to ensure that you can create custom alert rules in Azure Security Center.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

- A. Onboard Azure Active Directory (Azure AD) Identity Protection.
- B. Create an Azure Storage account.
- C. Implement Azure Advisor recommendations.
- D. Create an Azure Log Analytics workspace.
- E. Upgrade the pricing tier of Security Center to Standard.

Answer: (SHOW ANSWER)

D: You need write permission in the workspace that you select to store your custom alert.

Reference:

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

NEW QUESTION: 26

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: 27

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.

☐☒

Reference:

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

NEW QUESTION: 28

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

Name	Member of	Mobile phone	Multi-factor authentication (MFA) status
User1	Group1	123 555 7890	Disabled
User2	Group1, Group2	None	Enabled
User3	Group1	123 555 7891	Required

You create and enforce an Azure AD Identity Protection user risk policy that has the following settings:

Assignment: Include Group1, Exclude Group2

Conditions: Sign-in risk of Medium and above

Access: Allow access, Require password change

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 User1 signs in from an unfamiliar location, he must change his password.	☐	☐
If User2 signs in from an anonymous IP address, she must change her password.	☐	☐
If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password.	☐	☐

Answer:

Statements	Yes	No
If User1 signs in from an unfamiliar location, he must change his password.	☒	☐
If User2 signs in from an anonymous IP address, she must change her password.	☒	☐
If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password.	☐	☒

Reference:

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

NEW QUESTION: 29

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

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

From Azure Security Center, you turn on Auto Provisioning.

You deploy the virtual machines shown in the following table.

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

On which virtual machines is the Log Analytics agent installed?

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

Answer: ([SHOW ANSWER](#))

Explanation

When automatic provisioning is On, Security Center provisions the Log Analytics Agent on all supported Azure VMs and any new ones that are created.

Supported Operating systems include: Ubuntu 14.04 LTS (x86/x64), 16.04 LTS (x86/x64), and 18.04 LTS (x64) and Windows Server 2008 R2, 2012, 2012 R2, 2016, version 1709 and 1803

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection>

NEW QUESTION: 30

You need to deploy Microsoft Antimalware to meet the platform protection requirements.

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

NOTE: Each correct selection is worth one point.

Create a custom policy definition that has effect set to:

▼

Append
Deny
DeployIfNotExists

Create a policy assignment and modify:

▼

The Create a Managed Identify setting
The exclusion settings
The scope

Answer:

Create a custom policy definition that has effect set to:

▼

Append
Deny
DeployIfNotExists

Create a policy assignment and modify:

▼

The Create a Managed Identify setting
The exclusion settings
The scope

NEW QUESTION: 31

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:

Answer Area		
Statements	Yes	No
From VM2, you can create a container in storage1.	☐	☒
From VM1, you can upload data to the blob storage of storage1.	☒	☐
From VM2, you can upload data to the blob storage of storage1.	☐	☒

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 (517 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 32

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

Section: [none]

Explanation:

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.

Incorrect Answers:

A, D: Application permissions - Your client application needs to access the web API directly as itself (no user context). This type of permission requires administrator consent and is also not available for public (desktop and mobile) client applications.

Reference:

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

NEW QUESTION: 33

You implement the planned changes for ASG1 and ASG2.

In which NSGs can you use ASG1. and the network interfaces of which virtual machines can you assign to ASG2?

Answer Area



NSGs:

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

Virtual machines:

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

Answer:

Answer Area

NSGs:

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

Virtual machines:

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

NEW QUESTION: 34

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

Name	Role
Admin1	Global administrator
Admin2	Group administrator
Admin3	User administrator

Contoso.com contains a group naming policy. The policy has a custom blocked word list rule that includes the word Contoso.

Which users can create a group named Contoso Sales in contoso.com? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Users who can create a security group named Contoso Sales:

Admin1 only

Admin1 and Admin2 only

Admin1 and Admin3 only

Admin1, Admin2, and Admin3

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

Admin1 only

Admin1 and Admin2 only

Admin1 and Admin3 only

Admin1, Admin2, and Admin3

Answer:

Users who can create a security group named Contoso Sales:

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

Explanation

Users who can create a security group named Contoso Sales:

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

Reference:

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

NEW QUESTION: 35

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

Name	Member of	Mobile phone	Multi-factor authentication (MFA) status
User1	Group1	123 555 7890	Disabled
User2	Group1, Group2	None	Enabled
User3	Group1	123 555 7891	Required

You create and enforce an Azure AD Identity Protection user risk policy that has the following settings:

- * Assignment: Include Group1, Exclude Group2
- * Conditions: Sign-in risk of Medium and above
- * Access: Allow access, Require password change

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 User1 signs in from an unfamiliar location, he must change his password.	☐	☐
If User2 signs in from an anonymous IP address, she must change her password.	☐	☐
If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password.	☐	☐

Answer:

Statements	Yes	No
If User1 signs in from an unfamiliar location, he must change his password.	☒	☐
If User2 signs in from an anonymous IP address, she must change her password.	☒	☐
If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password.	☐	☒

Explanation

Statements	Yes	No
If User1 signs in from an unfamiliar location, he must change his password.	☒	☐
If User2 signs in from an anonymous IP address, she must change her password.	☒	☐
If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password.	☐	☒

Box 1: Yes

User1 is member of Group1. Sign in from unfamiliar location is risk level Medium.

Box 2: Yes

User2 is member of Group1. Sign in from anonymous IP address is risk level Medium.

Box 3: No

Sign-ins from IP addresses with suspicious activity is low.

Note:

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

Azure AD Identity protection can detect six types of suspicious sign-in activities:

- * Users with leaked credentials
- * Sign-ins from anonymous IP addresses
- * Impossible travel to atypical locations
- * Sign-ins from infected devices
- * Sign-ins from IP addresses with suspicious activity
- * Sign-ins from unfamiliar locations

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

References:

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

NEW QUESTION: 36

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

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

NEW QUESTION: 37

You need to deploy AKS1 to meet the platform protection requirements.

Which four 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.

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

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

Answer:

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

Reference:

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

NEW QUESTION: 38

You have an Azure Storage account that contains a blob container named container1 and a client application named App1.

You need to enable App1 access to container1 by using Azure Active Directory (Azure AD) authentication.

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

NOTE: Each correct selection is worth one point.

The screenshot shows two dropdown menus for selecting actions. The first dropdown, labeled 'From Azure AD:', has four options: 'Register App1.', 'Create an access package.', 'Implement an application proxy.', and 'Modify the authentication methods.'. The second dropdown, labeled 'From the storage account:', has four options: 'Add a private endpoint.', 'Regenerate the access key.', 'Configure Access control (IAM).', and 'Generate a shared access signature (SAS)'. The Microsoft logo is visible in the bottom left corner.

Answer:

The screenshot shows the same configuration interface as above, but with two options highlighted with red boxes: 'Register App1.' in the 'From Azure AD:' dropdown and 'Configure Access control (IAM).' in the 'From the storage account:' dropdown. The Microsoft logo is visible in the bottom left corner.

Reference:

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

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/storage/common/storage-auth-aad-rbac-portal.md>

NEW QUESTION: 39

You need to configure an access review. The review will be assigned to a new collection of reviews and reviewed by resource owners.

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

- Create an access review program.
- Set Reviewers to Selected users.
- Create an access review audit.
- Create an access review control.
- Set Reviewers to Group owners.
- Set Reviewers to Members.

Answer Area

Navigation arrows: Left (←), Right (→), Up (↑), Down (↓)

Microsoft

Answer:

Actions

- Create an access review program.
- Set Reviewers to Selected users.
- Create an access review audit.
- Create an access review control.
- Set Reviewers to Group owners.
- Set Reviewers to Members.

Answer Area

- Create an access review program.
- Create an access review control.
- Set Reviewers to Group owners.

Navigation arrows: Left (←), Right (→), Up (↑), Down (↓)

Microsoft

Explanation

Answer Area

- Create an access review program.
- Create an access review control.
- Set Reviewers to Group owners.

Microsoft

Step 1: Create an access review program

Step 2: Create an access review control

Step 3: Set Reviewers to Group owners

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.



References:

<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: 40

You need to deploy Microsoft Antimalware to meet the platform protection requirements.

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

NOTE: Each correct selection is worth one point.

Create a custom policy definition that has effect set to:

▼

Append

Deny

DeployIfNotExists

Create a policy assignment and modify:

▼

The Create a Managed Identify setting

The exclusion settings

The scope

Answer:

Create a custom policy definition that has effect set to:

Append

Deny

DeployIfNotExists

Create a policy assignment and modify:

The Create a Managed Identify setting

The exclusion settings

The scope



Microsoft

Topic 1, Litware, inc
Existing Environment
Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.
Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices.
Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.
The tenant contains the groups shown in the following table.

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

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

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

Azure Security Center is set to the Free tier.

Planned changes

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

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

Litware identifies the following identity and access requirements:

All San Francisco users and their devices must be members of Group1.

The members of Group2 must be assigned the Contributor role to Resource Group2 by using a permanent eligible assignment.

Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.

Platform Protection Requirements

Litware identifies the following platform protection requirements:

Microsoft Antimalware must be installed on the virtual machines in Resource Group1.

The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.

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

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.

A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.

Security Operations Requirements

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

NEW QUESTION: 41

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.

Answer Area**Statements****Yes****No**

You can start VM1.

☒☐

You can start VM2.

☐☐

You can create a virtual machine in RG2.

☐☐

Answer:

Answer Area 

Statements	Yes	No
You can start VM1.	☐	☒
You can start VM2.	☒	☐
You can create a virtual machine in RG2.	☒	☐

Explanation

Answer Area 

Statements	Yes	No
You can start VM1.	☐	☒
You can start VM2.	☒	☐
You can create a virtual machine in RG2.	☒	☐

References:

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

NEW QUESTION: 42

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.	☐	☒

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: 43

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](#))

Explanation

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	networkSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

Sub2

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

Sub2 contains the virtual machines shown in the following table.

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

All virtual machines have the public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests. Sub2 contains the network security groups (NSGs) shown in the following table.

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

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

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

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

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

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

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

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

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

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

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

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

NEW QUESTION: 44

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

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

Azure AD Privileged Identity Management (PIM) is enabled for the tenant.

In PIM, the Password Administrator role has the following settings:

Maximum activation duration (hours): 2

Send email notifying admins of activation: Disable

Require incident/request ticket number during activation: Disable

Require Azure Multi-Factor Authentication for activation: Enable

Require approval to activate this role: Enable

Selected approver: Group1

You assign users the Password Administrator role as shown in the following table.

Name	Assignment type
User1	Active
User2	Eligible
user3	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
When User1 signs in, the user is assigned the Password Administrator role automatically.	☐	☐
User2 can request to activate the Password Administrator role.	☐	☐
If User3 wants to activate the Password Administrator role, the user can approve their own request.	☐	☐

Answer:

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

NEW QUESTION: 45

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

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

You need to configure authorization access.

Which authorization types can you use for each storage account? To answer, select the appropriate options in the answer area NOTE Each correct selection is worth one point.

Answer:

storage1:	Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)
storage2:	Shared Key only
storage3:	Shared access signature (SAS) only

NEW QUESTION: 46

You have an Azure subscription named Sub1. Sub1 has an Azure Storage account named Storage1 that contains the resources shown in the following table.

Name	Type
Container1	Blob container
Share1	File share

You generate a shared access signature (SAS) to connect to the blob service and the file service.

Which tool can you use to access the contents in Container1 and Share1 by using the SAS? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Tools for Container1:

- Robocopy.exe
- Azure Storage Explorer
- File Explorer

Tools for Share1:

- Robocopy.exe
- Azure Storage Explorer
- File Explorer



Answer:
Actions

- Publish an Azure Blueprints version
- Assign an Azure blueprint.
- Create a policy assignment.
- Create a custom role-based access control (RBAC) role.
- Create a dedicated management subscription.
- Create an Azure Blueprints definition.
- Create an initiative assignment.

Answer Area

- Create an Azure Blueprints definition.
- Publish an Azure Blueprints version
- Assign an Azure blueprint.



Explanation

Tools for Container1:

Tools for Share1:

Robocopy.exe

Azure Storage Explorer

File Explorer

Robocopy.exe

Azure Storage Explorer

File Explorer

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 (517 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 47

You need to create Role1 to meet the platform protection requirements.

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

NOTE: Each correct selection is worth one point.

```
{
  "Name": "Role1",
  "Id": "11111111-1111-1111-1111-111111111111",
  "IsCustom": true,
  "Description": "VM storage operator"
  "Actions": [
```

▼	▼
Microsoft.Compute/	disks/**,
Microsoft.Resources/	storageAccounts/**,
Microsoft.Storage/	virtualMachines/disks/**

],

```
  "NotActions": [
  ],
```

```
  "AssignableScopes": [
```

▼
/*
/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4/resourceGroups/Resource Group1
/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4

]

```
}
```

Answer:

```
{
  "Name": "Role1",
  "Id": "11111111-1111-1111-1111-111111111111",
  "IsCustom": true,
  "Description": "VM storage operator"
  "Actions": [
```

▼	▼
Microsoft.Compute/	disks/**,
Microsoft.Resources/	storageAccounts/**,
Microsoft.Storage/	virtualMachines/disks/**

],

```
  "NotActions": [
  ],
```

```
  "AssignableScopes": [
```

▼
/*
/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4/resourceGroups/Resource Group1
/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4

]

```
}
```


Explanation

1) Microsoft.Compute/

2) disks

3) /subscription/{subscriptionId}/resourceGroups/{Resource Group Id}

A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.

NEW QUESTION: 48

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:  Microsoft

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: 49

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

No,

Yes,

Yes

Topic 2, Litware, inc

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

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question on this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next sections of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question on this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

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

Existing Environment

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

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

The tenant contains the groups shown in the following table.

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

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

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

Azure Security Center is set to the Free tier.

Planned changes

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

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

Litware identifies the following identity and access requirements:

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

- * that access company information on the users' behalf.
- Platform Protection Requirements
- Litware identifies the following platform protection requirements:
- * Microsoft Antimalware must be installed on the virtual machines in Resource Group1.
 - * The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.
 - * Azure AD users must be to authenticate to AKS1 by using their Azure AD credentials.
 - * Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.
 - * A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.
- Security Operations Requirements
- Litware must be able to customize the operating system security configurations in Azure Security Center.

NEW QUESTION: 50

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.

New-AzureRmKeyVault

-VaultName 'KeyVault1' -ResourceGroupName 'RG1'

-Location 'East US'

-EnabledForDeployment

-EnablePurgeProtection

-Tag

-Confirm

-DefaultProfile

-EnableSoftDelete

-SKU

Answer:

New-AzureRmKeyVault

-VaultName 'KeyVault1' -ResourceGroupName 'RG1'

-Location 'East US'

-EnabledForDeployment

-EnablePurgeProtection

-Tag

-Confirm

-DefaultProfile

-EnableSoftDelete

-SKU

Reference:

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

NEW QUESTION: 51

From Azure Security Center, you enable Azure Container Registry vulnerability scanning of the images in

Registry1.

You perform the following actions:

Push a Windows image named Image1 to Registry1.

Push a Linux image named Image2 to Registry1.

Push a Windows image named Image3 to Registry1.

Modify Image1 and push the new image as Image4 to Registry1.

Modify Image2 and push the new image as Image5 to Registry1.

Which two images will be scanned for vulnerabilities? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Image2

B. Image3

C. Image4

D. Image1

E. Image5

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 52

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: 53

You have an Azure subscription that contains 100 virtual machines. Azure Diagnostics is enabled on all the virtual machines.

You are planning the monitoring of Azure services in the subscription.

You need to retrieve the following details:

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

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

What should you use in Azure Monitor? To answer, drag the appropriate configuration settings to the correct details. Each configuration setting 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.

Settings

Activity log

Logs

Metrics

Service Health

Answer Area

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

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

Answer:

Settings

Activity log

Logs

Metrics

Service Health

Answer Area

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

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

Reference:

<https://docs.microsoft.com/en-us/azure/security/azure-log-audit>

NEW QUESTION: 54

You need to ensure that User2 can implement PIM.

What should you do first?

A. Assign User2 the Global administrator role.

- B. Configure authentication methods for contoso.com.
- C. Configure the identity secure score for contoso.com.
- D. Enable multi-factor authentication (MFA) for User2.

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

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

1. Sign in to the Azure portal as a Global Administrator of your directory.

You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com), to enable PIM for a directory.

Scenario: Technical requirements include: Enable Azure AD Privileged Identity Management (PIM) for contoso.com

References:

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-started>

Manage identity and access

Question Set 3

NEW QUESTION: 55

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

Name	Description
User1	Uses app password authentication for the Mail and Calendar app in Windows 10
User2	Uses Outlook on the web

You need to ensure that the users cannot create app passwords. The solution must ensure that User1 can continue to use the Mail and Calendar app.

What should you do?

- A. Create a new app registration.
- B. Enable Azure AD Password Protection.
- C. Assign User! the Authentication Policy Administrator role.
- D. Configure a multi-factor authentication (MFA) registration policy.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 56

You need to meet the technical requirements for VNetwork1.

What should you do first?

- A. Create a new subnet on VNetwork1.
- B. Configure DDoS protection for VNetwork1.
- C. Associate an NSG to Subnet12.
- D. Remove the NSGs from Subnet11 and Subnet13.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 57

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

Microsoft

Statements

User1 can set Purge protection to Enable for Vault1.

User2 can configure firewalls and virtual networks for Vault1.

User3 can add access policies to Vault1.

Yes

No

☐
☐

☐
☐

☐
☐

Answer:

Answer Area

Microsoft

Statements

User1 can set Purge protection to Enable for Vault1.

User2 can configure firewalls and virtual networks for Vault1.

User3 can add access policies to Vault1.

Yes

No

☒
☐

☐
☒

☐
☒

NEW QUESTION: 58

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

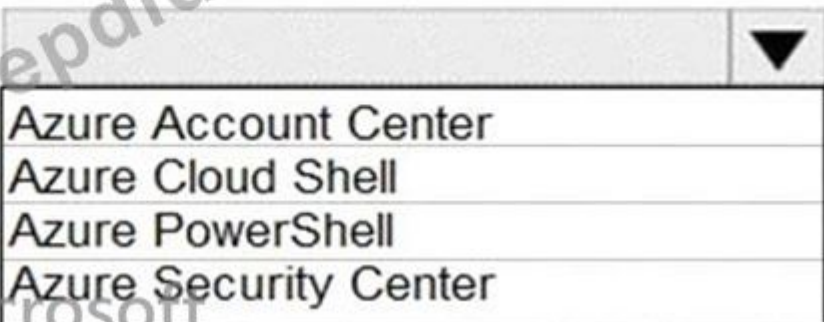
The company is sold to a new owner.

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.

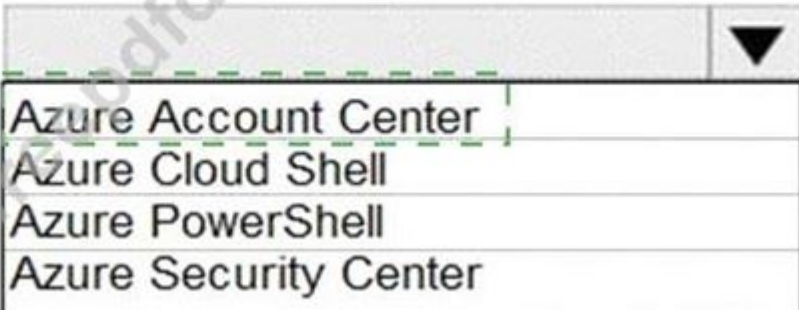
User: 

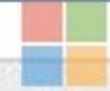
Tool: 

 Microsoft

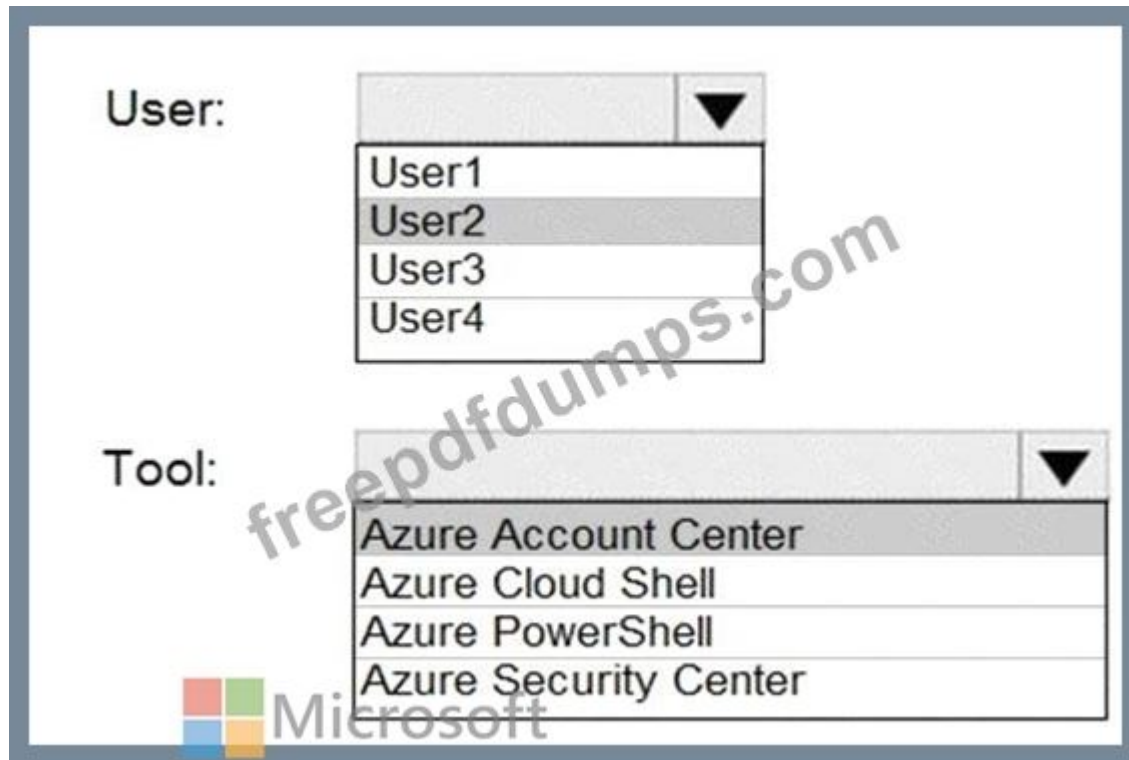
Answer:

User: 

Tool: 

 Microsoft

Explanation



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-azu>

NEW QUESTION: 59

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 1

You need to configure Azure to allow RDP connections from the Internet to a virtual machine named VM1. The solution must minimize the attack surface of VM1.

Answer:

Check below steps in explanation for Task

Explanation:

To configure Azure to allow RDP connections from the Internet to a virtual machine named VM1, you can follow the steps below:

Create a new inbound security rule in the network security group (NSG) that is associated with the virtual network subnet that contains VM1. The rule should allow RDP traffic from the Internet to the virtual network subnet. You can use the Azure portal, Azure PowerShell, or Azure CLI to create the rule.

Configure the network security group (NSG) to associate it with the virtual network subnet that contains VM1.

Configure the virtual machine to allow RDP traffic. You can use the Azure portal, Azure PowerShell, or Azure CLI to configure the virtual machine.

To minimize the attack surface of VM1, you can use the following best practices:

- Use a strong password for the local administrator account on the virtual machine.
- Use Network Security Groups (NSGs) to restrict traffic to only the necessary ports and protocols.
- Use Azure Security Center to monitor and protect your virtual machines.

NEW QUESTION: 60

You assign User8 the Owner role for RG4, RG5, and RG6.

In which resource groups can User8 create virtual networks and NSGs? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

User8 can create virtual networks in:

RG4 only

RG6 only

RG4 and RG6 only

RG4, RG5, and RG6

User8 can create NSGs in:

RG4 only

RG4 and RG5 only

RG4 and RG6 only

RG4, RG5, and RG6

Answer:

User8 can create virtual networks in:

RG4 only

RG6 only

RG4 and RG6 only

RG4, RG5, and RG6

User8 can create NSGs in:

RG4 only

RG4 and RG5 only

RG4 and RG6 only

RG4, RG5, and RG6

NEW QUESTION: 61

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:



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 (517 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 62

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 Active Directory (Azure AD) user
- D. an Azure Active Directory (Azure AD) group

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

Section: [none]

Explanation/Reference:

<https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal>

NEW QUESTION: 63

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.

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:

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.	☒	☐

NEW QUESTION: 64

You have an Azure subscription that contains 100 virtual machines. Azure Diagnostics is enabled on all the virtual machines.

You are planning the monitoring of Azure services in the subscription.

You need to retrieve the following details:

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

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

What should you use in Azure Monitor? To answer, drag the appropriate configuration settings to the correct details. Each configuration setting 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.

Settings

Activity log
Logs
Metrics
Service Health

Answer Area

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

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

Answer:

Settings

Activity log
Logs
Metrics
Service Health

Answer Area

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

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

Reference:

<https://docs.microsoft.com/en-us/azure/security/azure-log-audit>

NEW QUESTION: 65

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

Answer:

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

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: 66

You are implementing conditional access policies.

You must evaluate the existing Azure Active Directory (Azure AD) risk events and risk levels to configure and implement the policies.

You need to identify the risk level of the following risk events:

- * Users with leaked credentials
- * Impossible travel to atypical locations
- * Sign ins from IP addresses with suspicious activity

Which level should you identify for each risk event? To answer, drag the appropriate levels to the correct risk events. Each level 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.

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

Answer:

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

Explanation

Answer Area

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

Azure AD Identity protection can detect six types of suspicious sign-in activities:

- * Users with leaked credentials
- * Sign-ins from anonymous IP addresses
- * Impossible travel to atypical locations
- * Sign-ins from infected devices
- * Sign-ins from IP addresses with suspicious activity
- * Sign-ins from unfamiliar locations

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

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

References:

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

NEW QUESTION: 67

You are implementing conditional access policies.

You must evaluate the existing Azure Active Directory (Azure AD) risk events and risk levels to configure and implement the policies.

You need to identify the risk level of the following risk events:

- * Users with leaked credentials
- * Impossible travel to atypical locations
- * Sign ins from IP addresses with suspicious activity

Which level should you identify for each risk event? To answer, drag the appropriate levels to the correct risk events. Each level 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.

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

Answer:

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

Explanation

Answer Area

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

Azure AD Identity protection can detect six types of suspicious sign-in activities:

- * Users with leaked credentials
- * Sign-ins from anonymous IP addresses
- * Impossible travel to atypical locations
- * Sign-ins from infected devices
- * Sign-ins from IP addresses with suspicious activity
- * Sign-ins from unfamiliar locations

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

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

References:

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

NEW QUESTION: 68

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.)

Role settings

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 approvers

No 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>

NEW QUESTION: 69

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:

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.	☒	☐

NEW QUESTION: 70

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

The company develops a mobile application named App1. App1 uses the OAuth 2 implicit grant type to acquire Azure AD access tokens.

You need to register App1 in Azure AD.

What information should you obtain from the developer to register the application?

- A. a redirect URI
- B. a reply URL
- C. a key
- D. an application ID

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

Section: [none]

Explanation:

For Native Applications you need to provide a Redirect URI, which Azure AD will use to return token responses.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/v1-protocols-oauth-code>

NEW QUESTION: 71

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

Configure secrets for the Azure key vault.

Create an Azure key vault.

Run Set-AzureRmStorageAccount.

Configure access policies for the Azure key vault.

Run Set-AzureRmVmDiskEncryptionExtension.

Answer Area

Answer:

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.

References:

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

NEW QUESTION: 72

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.

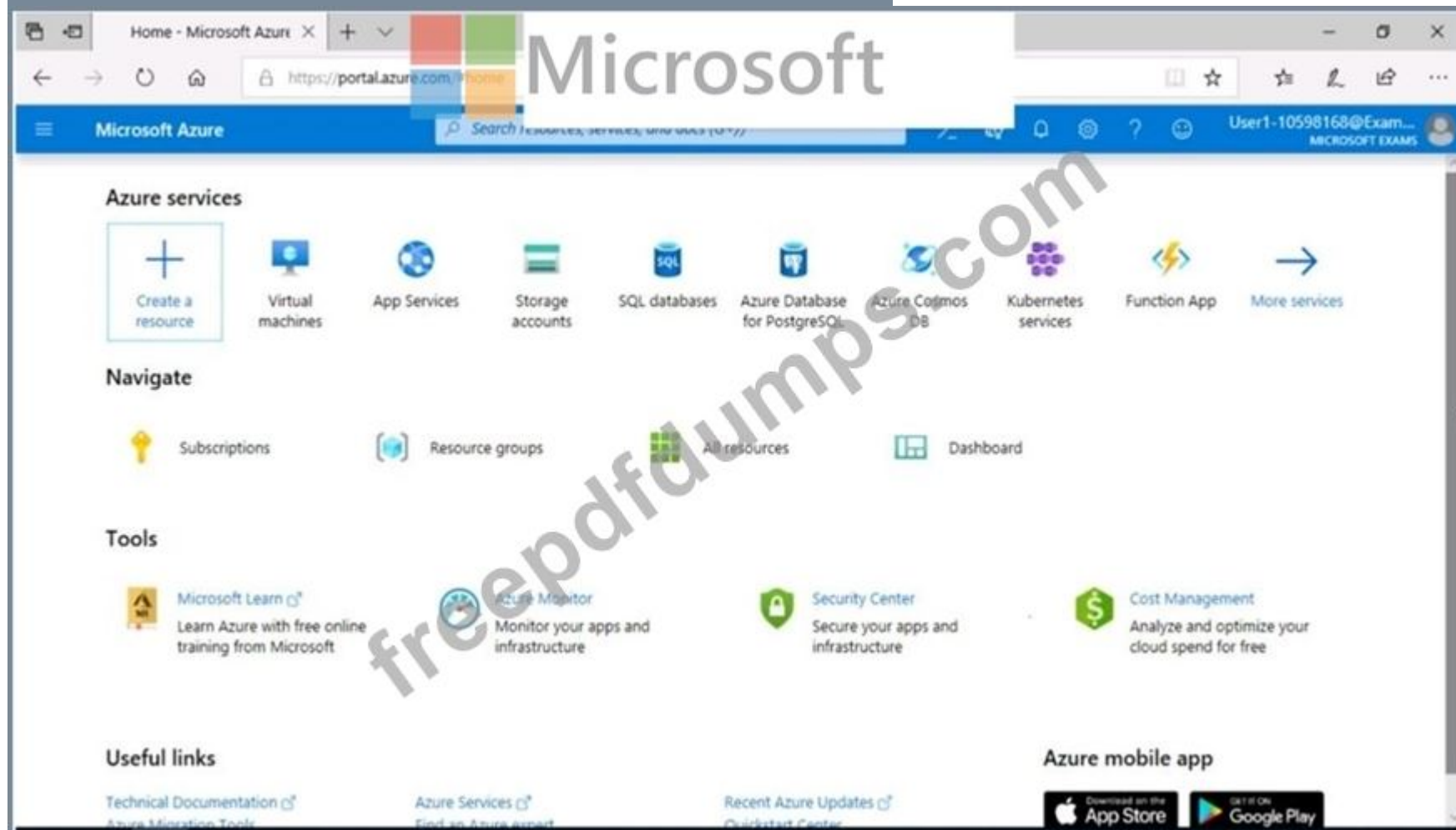
To enter your password, place your cursor in the Enter password box and click on the password below.

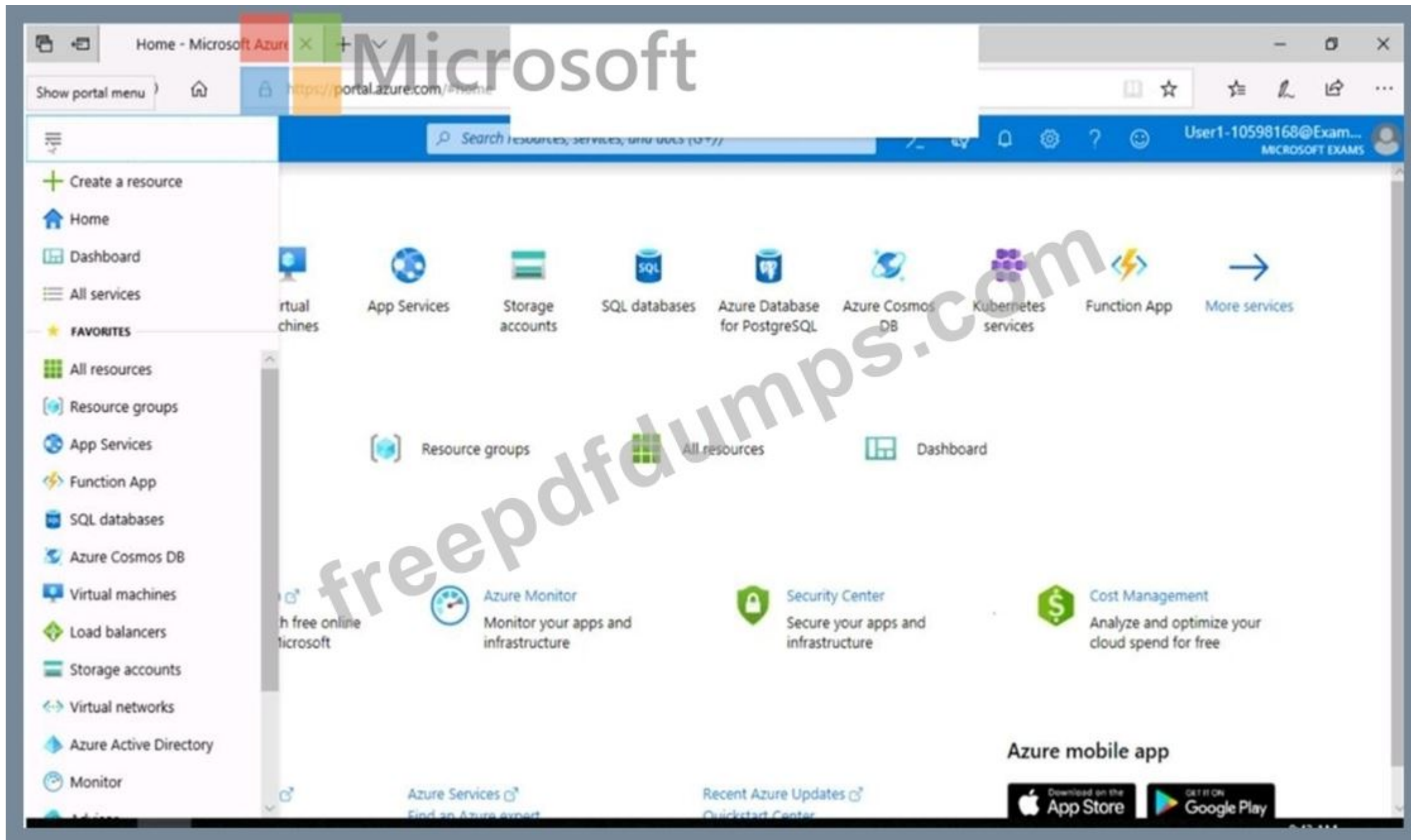
Azure Username: User1-10598168@ExamUsers.com

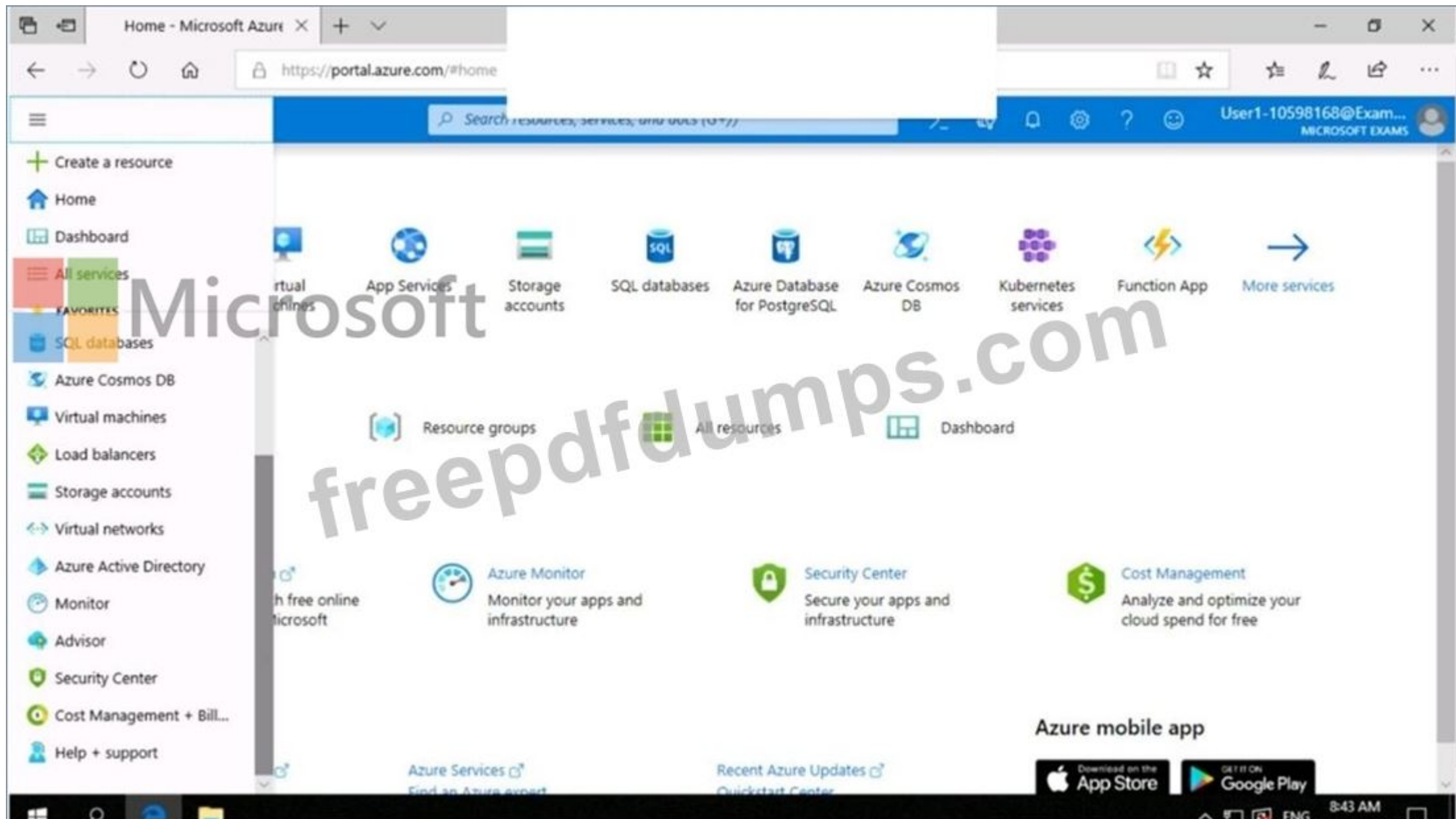
Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168







You need to ensure that the rg1lod10598168n1 Azure Storage account is encrypted by using a key stored in the KeyVault10598168 Azure key vault.

To complete this task, sign in to the Azure portal.

Answer:

See the explanation below.

Explanation

Step 1: To enable customer-managed keys in the Azure portal, follow these steps:

1. Navigate to your storage account rg1lod10598168n1
2. On the Settings blade for the storage account, click Encryption. Select the Use your own key option, as shown in the following figure.

Save Discard

Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

By default, data is encrypted using Microsoft Managed Keys for Azure Blobs, Tables, Files and Queues. You may choose to bring your own key for encryption for Azure Blobs and Files. Encryption for Tables and Queues will always use Microsoft Managed Keys.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process.

[Learn more](#)

Your storage account is currently encrypted with Microsoft managed key by default. You can choose to use your own key.

☐ Use your own key

Step 2: Specify a key from a key vault

To specify a key from a key vault, first make sure that you have a key vault that contains a key. To specify a key from a key vault, follow these steps:

4. Choose the Select from Key Vault option.
5. Choose the key vault KeyVault10598168 containing the key you want to use.
6. Choose the key from the key vault.

Save Discard

Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

By default, data is encrypted using Microsoft Managed Keys for Azure Blobs, Tables, Files and Queues. You may choose to bring your own key for encryption for Azure Blobs and Files. Encryption for Tables and Queues will always use Microsoft Managed Keys.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process.

[Learn more](#)

Your storage account is currently encrypted with Microsoft managed key by default. You can choose to use your own key.

☒ Use your own key

Encryption key

☐ Enter key URI

☒ Select from Key Vault

* Key Vault
<key-vault>

* Encryption key
<key>

 <storage-account> will be granted access to the selected key vault. Both soft delete and purge protection will be enabled on the key vault and cannot be disabled. [Learn more](#)

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-encryption-keys-portal>

NEW QUESTION: 73

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:

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

Reference:

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

NEW QUESTION: 74

You need to ensure that the Azure AD application registration and consent configurations meet the identity and access requirements.

What should you use in the Azure portal? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

To configure the registration settings:

Azure AD – User settings

Azure AD – App registrations settings

Enterprise Applications – User settings

To configure the consent settings:

Azure AD – User settings

Azure AD – App registrations settings

Enterprise Applications – User settings

Answer:

To configure the registration settings:

Azure AD – User settings

Azure AD – App registrations settings

Enterprise Applications – User settings

To configure the consent settings:

Azure AD – User settings

Azure AD – App registrations settings

Enterprise Applications – User settings

Reference:
<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent>

NEW QUESTION: 75

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
2
3
4

Network security rules: ▼

1
2
3
4

Microsoft

Answer:

NSGs: ▼

1
2
3
4

Network security rules: ▼

1
2
3
4

Microsoft

Explanation:

NSGs: 2

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: 76

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

Name	Type	Region	Resource group
Sa1	Azure Storage account	East US	RG1
VM1	Azure virtual machine	East US	RG2
KV1	Azure key vault	East US 2	RG1
SQL1	Azure SQL database	East US 2	RG2

You need to ensure that you can provide VM1 with secure access to a database on SQL1 by using a contained database user.

What should you do?

- A. Create a key in KV1.
- B. Enable a managed service identity on VM1.
- C. Configure a service endpoint on SQL1.
- D. Create a secret in KV1.

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 (517

Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 77

You have an Azure subscription named Sub 1 that is associated to an Azure Active Directory (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

Users who can onboard Azure AD Identity Protection:

User1 only
User1 and User2 only
User1, User 2, and User3 only
User1, User 2, User3, and User 4 only

Users who can remediate users and configure policies:

User1 and User2 only
User1 and User3 only
User1, User 2, and User3 only
User1, User 2, User3, and User 4

Answer:

Answer Area

Users who can onboard Azure AD Identity Protection:

- User1 only
- User1 and User2 only
- User1, User 2, and User3 only
- User1, User 2, User3, and User 4 only

Users who can remediate users and configure policies:

- User1 and User2 only
- User1 and User3 only
- User1, User 2, and User3 only
- User1, User 2, User3, and User 4

NEW QUESTION: 78

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

Name	Role
Admin1	Global administrator
Admin2	Group administrator
Admin3	User administrator

Contoso.com contains a group naming policy. The policy has a custom blocked word list rule that includes the word Contoso.

Which users can create a group named Contoso Sales in contoso.com? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Users who can create a security group named Contoso Sales:

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

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

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

Answer:

Users who can create a security group named Contoso Sales:

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

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

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

Reference:

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

NEW QUESTION: 79

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.



Microsoft

	▼
User1	
User2	
User3	
User4	

Tool:

	▼
Azure Account Center	
Azure Cloud Shell	
Azure PowerShell	
Azure Security Center	

Answer:

User:

	▼
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-azu>

NEW QUESTION: 80

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

NEW QUESTION: 81

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.

Microsoft
NSGs:

1
2
3
4

Network security rules:

1
2
3
4

Answer:

Microsoft
NSGs:

1
2
3
4

Network security rules:

1
2
3
4

Reference:

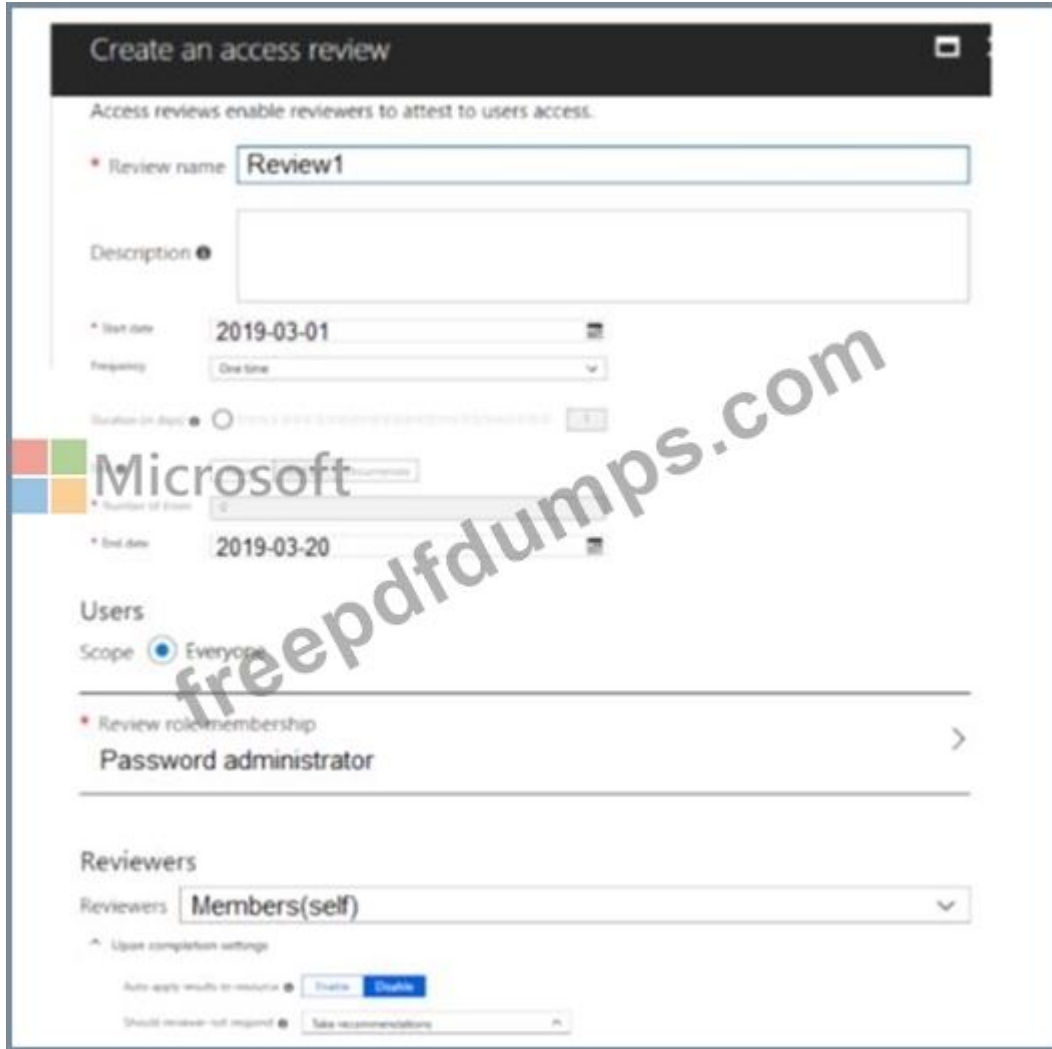
<https://docs.microsoft.com/en-us/azure/virtual-network/security-overview>

NEW QUESTION: 82

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 date

Number of times

Users

Scope ☒ Everyone

* Review role membership

Reviewers

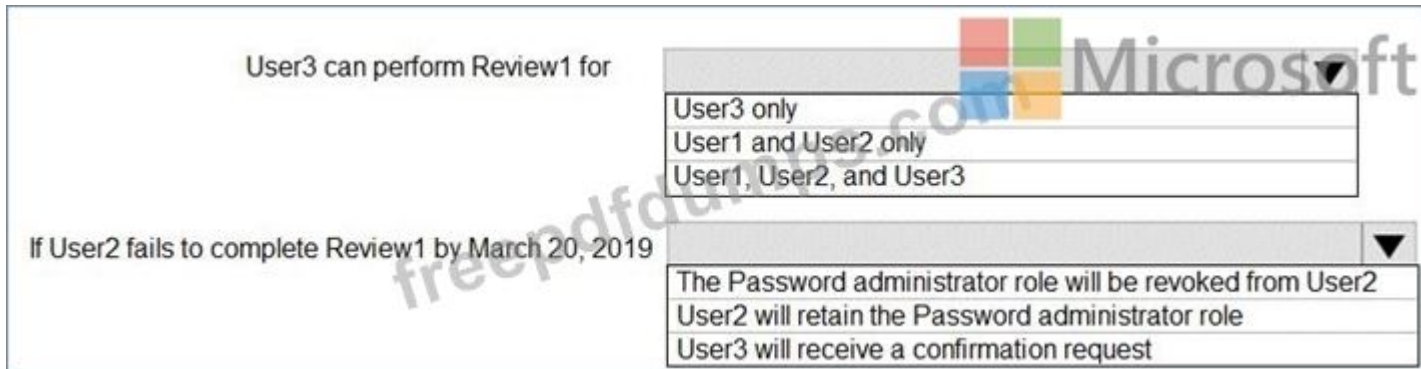
Reviewers

Auto apply results to reviewer ☒ Enabled

Should reviewer self respond ☒ Take recommendations

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

If User2 fails to complete Review1 by March 20, 2019

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

Reference:

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review>

NEW QUESTION: 83

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. ☒

☐

NEW QUESTION: 84

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: 85

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')]" : "[variable('var1')]"
      "AzureADApplicationID"
      "WorkspaceID"
      "WorkspaceName"
      "WorkspaceURL"
    },
    "protectedSettings" : {
      "[variable('var2')]" : "[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')]" : "[variable('var1')]"
    },
    "protectedSettings" : {
      "[variable('var2')]" : "[variable('var2')]"
    }
  }
}

```

▼

"AzureADApplicationID"

"WorkspaceID"

"WorkspaceName"

"WorkspaceURL"

▼

"AzureADApplicationSecret"

"StorageAccountKey"

"WorkspaceID"

"WorkspaceKey"



Reference:

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

NEW QUESTION: 86

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.

The screenshot shows two dropdown menus for configuring permissions for ContosoKey1. The first dropdown, labeled 'Delegate permissions for ContosoKey1:', has a list of options: 'User1 only', 'User1 and User2 only', 'User1 and User3 only', 'User1 and User4 only', 'User1, User2, and User3 only', and 'User1, User2, User3, and User4'. The second dropdown, labeled 'Configure network access to ContosoKey1:', has the same list of options. A large 'freepdfdumps.com' watermark is visible across the center of the image.

Answer:

This screenshot shows the same configuration interface as the previous one, but with the correct selections highlighted by red boxes. In the 'Delegate permissions for ContosoKey1:' dropdown, 'User1 and User3 only' is selected. In the 'Configure network access to ContosoKey1:' dropdown, 'User1 only' is selected. A large 'freepdfdumps.com' watermark is visible across the center of the image.

Reference:

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

NEW QUESTION: 87

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. Configure Azure Active Directory (Azure AD) Identity Protection.

B. From Microsoft Defender for Cloud, configure adaptive application controls.

C. Apply an Azure policy to RG1.

D. Apply a resource lock to RG1.

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

Explanation

Microsoft Defender for Cloud helps you prevent, detect, and respond to threats. Defender for Cloud gives you increased visibility into, and control over, the security of your Azure resources. It provides integrated security monitoring and policy management across your Azure subscriptions. It helps detect threats that might otherwise go unnoticed, and works with a broad ecosystem of security solutions.

Defender for Cloud helps you optimize and monitor the security of your virtual machines by:

* Providing security recommendations for the virtual machines. Example recommendations include: apply system updates, configure ACLs endpoints, enable antimalware, enable network security groups, and apply disk encryption.

* Monitoring the state of your virtual machines.

<https://learn.microsoft.com/en-us/azure/security/fundamentals/virtual-machines-overview>

NEW QUESTION: 88

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.	☒	☐

Topic 2, Litware, inc
Existing Environment
Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.
Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices.
Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.
The tenant contains the groups shown in the following table.

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

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

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

Azure Security Center is set to the Free tier.

Planned changes

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

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

Litware identifies the following identity and access requirements:

All San Francisco users and their devices must be members of Group1.

The members of Group2 must be assigned the Contributor role to Resource Group2 by using a permanent eligible assignment.

Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.

Platform Protection Requirements

Litware identifies the following platform protection requirements:

Microsoft Antimalware must be installed on the virtual machines in Resource Group1.

The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.

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

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.

A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.

Security Operations Requirements

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

NEW QUESTION: 89

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

- A. Azure Storage Explorer
- B. SQL query editor in Azure
- C. File Explorer in Windows
- D. Azure Security Center

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

Explanation

If you want to download the metrics for long-term storage or to analyze them locally, you must use a tool or write some code to read the tables. You must download the minute metrics for analysis. The tables do not appear if you list all the tables in your storage account, but you can access them directly by name. Many storage-browsing tools are aware of these tables and enable you to view them directly (see Azure Storage Client Tools for a list of available tools).

Microsoft provides several graphical user interface (GUI) tools for working with the data in your Azure Storage account. All of the tools outlined in the following table are free.

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

References:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-metrics?toc=%2fazure%2fstorage%2>

<https://docs.microsoft.com/en-us/azure/storage/common/storage-explorers>

NEW QUESTION: 90

You have an Azure subscription that contains the following Azure firewall:

- * Name: Fw1
- * Azure region: UK West
- * Private IP address: 10.1.3.4
- * Public IP address: 23.236.62.147

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

Name	Location	IP address space	Peered with
Vnet1	UK West	10.1.0.0/16	Vnet2
Vnet2	East US	10.2.0.0/16	Vnet1, Vnet3
Vnet3	West US	10.3.0.0/16	Vnet2,

The subscription contains the subnets shown in the following table.

Name	Virtual network	IP address range
Subnet1-1	Vnet1	10.1.1.0/24
Subnet1-2	Vnet1	10.1.2.0/24
AzureFirewallSubnet	Vnet1	10.1.3.0/24
Subnet2-1	Vnet2	10.2.1.0/24
Subnet3-1	Vnet3	10.3.1.0/24

The subscription contains the routes shown in the following table.

Name	Subnet	IP address prefix	Next hop type	Next hop IP address
Rt1	Subnet1-1	0.0.0.0/0	Virtual appliance	10.1.3.4
Rt2	Subnet1-2	10.1.1.0/24	Virtual appliance	10.1.3.4
Rt3	Subnet2-1	10.1.1.0/24	Virtual appliance	10.1.3.4
Rt4	Subnet3-1	10.2.1.0/24	Virtual appliance	10.1.3.4

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

Traffic from Subnet1-1 to Subnet 1-2 is routed through Fw1.

Yes No

☐ ☐

Traffic from Subnet2-1 to Subnet 1-1 is routed through Fw1.

☐ ☐

Traffic from Subnet3-1 to the internet is routed through Fw1.

☐ ☐

Answer:

Statements	Yes	No
Traffic from Subnet1-1 to Subnet 1-2 is routed through Fw1.	☒	☐
Traffic from Subnet2-1 to Subnet 1-1 is routed through Fw1.	☐	☒
Traffic from Subnet3-1 to the internet is routed through Fw1.	☒	☐

NEW QUESTION: 91

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

Microsoft

ASG1:

ASG2:

Answer:

Answer Area

Microsoft

ASG1:

VM2, VM3, and VM4 only

ASG2:

VM1, VM2, and VM4 only

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 (517 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 92

You have an Azure subscription that contains the alerts shown in the following exhibit.

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

cannot be changed
can be changed to Closed only
can be changed to New only
can be changed to New or Closed

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

cannot be changed
can be changed to Acknowledged only
can be changed to New only
can be changed to New or Acknowledged

Explanation

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

cannot be changed
can be changed to Closed only
can be changed to New only
can be changed to New or Closed

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

cannot be changed
can be changed to Acknowledged only
can be changed to New only
can be changed to New or Acknowledged

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

NEW QUESTION: 93

You have the role assignments shown in the following exhibit.

```
{
  {
    "RoleAssignmentId": "13ae6e22-b93a-412f-9dc5-fc82b1726bde",
    "Scope": "/subscriptions/0a1baf97-0be4-424a-92fa-873c5a45fbbc/resourceGroups/RG1",
    "DisplayName": "Admin1",
    "SignInName": "Admin1@contoso.com",
    "RoleDefinitionName": "Owner",
    "RoleDefinitionId": "/subscriptions/0a1baf97-0be4-424a-92fa-873c5a45fbbc/providers/
```

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: 94

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)

Explanation

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

NEW QUESTION: 95

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.

Microsoft

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: 96

What is the membership of Group1 and Group2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Group1:

No members
Only User2
Only User2 and User4
User1, User2, User3, and User4

Group2:

No members
Only User3
Only User1 and User3
User1, User2, User3, and User4

Answer:

Group1: ▼

- No members
- Only User2
- Only User2 and User4
- User1, User2, User3, and User4

Group2: ▼

- No members
- Only User3
- Only User1 and User3
- User1, User2, User3, and User4

Explanation:

Box 1: User1, User2, User3, User4

Contains "ON" is true for Montreal (User1), MONTREAL (User2), London (User 3), and Ontario (User4) as string and regex operations are not case sensitive.

Box 2: Only User3

Match "*on" is only true for London (User3).

Scenario:

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.

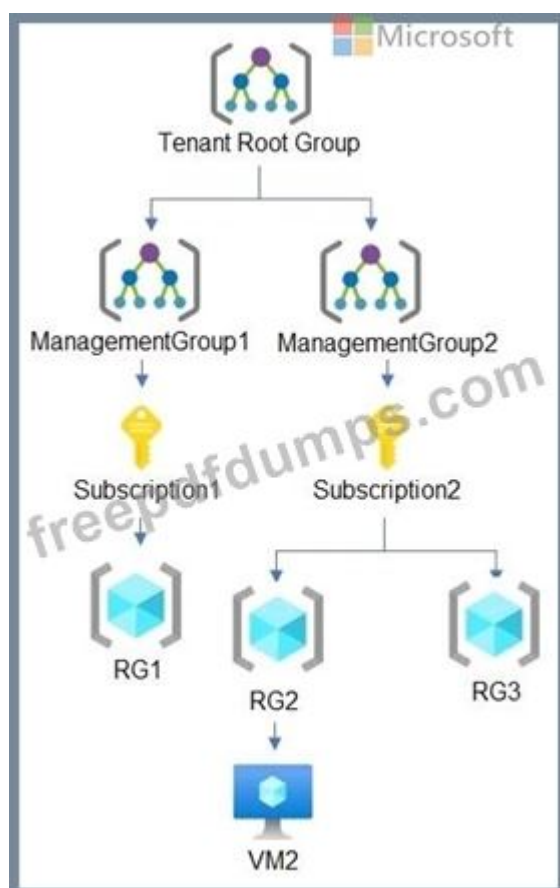
Name	Membership type	Dynamic membership rule
Group1	Dynamic user	user.city -contains "ON"
Group2	Dynamic user	user.city -match "*on"

References:

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

NEW QUESTION: 97

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.	☐	☒

NEW QUESTION: 98

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](#))

Explanation

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.

NEW QUESTION: 99

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		
+ 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.	☐	☒

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

NEW QUESTION: 100

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?

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

NEW QUESTION: 101

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.

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

Reference:

<https://docs.microsoft.com/en-us/azure/automation/automation-update-management>

NEW QUESTION: 102

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

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

User2 is the owner of Group2.

The user and group settings for App1 are configured as shown in the following exhibit.

Add user
 Edit
 Remove
 Update Credentials
 Columns
 Got feedback?

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

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

DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
Group1	Group	Default Access

You enable self-service application access for App1 as shown in the following exhibit.

Allow users to request access to this application?
Yes No

To which group should assigned users be added?

Select group

Group2

Require approval before granting access to this application?
Yes No

Who is allowed to approve access to this application?

Select approvers

1 users selected

To which role should users be assigned in this application?

*Select a role

Default Access

User3 is configured to approve access to Appl.

You need to identify the owners of Group2 and the users of Appl.

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

NOTE: Each correct selection is worth one point.

Group2 owners:

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

App1 users:

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

Answer:

Group2 owners:

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

App1 users:

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

Reference:

NEW QUESTION: 103

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

From VM1, you can successfully ping the private IP address of VM4.

☐

No

☐

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: 104

Which virtual networks in Sub1 can User2 modify and delete in their current state? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Virtual networks that User2 can modify:

- VNET4 only
- VNET4 and VNET1 only
- VNET4, VNET3, and VNET1 only
- VNET4, VNET3, VNET2, and VNET1

Virtual networks that User2 can delete:

- VNET4 only
- VNET4 and VNET1 only
- VNET4, VNET3, and VNET1 only
- VNET4, VNET3, VNET2, and VNET1

Answer:

Virtual networks that User2 can modify:

VNET4 only
VNET4 and VNET1 only
VNET4, VNET3, and VNET1 only
VNET4, VNET3, VNET2, and VNET1

Virtual networks that User2 can delete:

VNET4 only
VNET4 and VNET1 only
VNET4, VNET3, and VNET1 only
VNET4, VNET3, VNET2, and VNET1

Explanation

Virtual networks that User2 can modify:

VNET4 only
VNET4 and VNET1 only
VNET4, VNET3, and VNET1 only
VNET4, VNET3, VNET2, and VNET1

Virtual networks that User2 can delete:

VNET4 only
VNET4 and VNET1 only
VNET4, VNET3, and VNET1 only
VNET4, VNET3, VNET2, and VNET1

Box 1: VNET4 and VNET1 only

RG1 has only Delete lock, while there are no locks on RG4.

RG2 and RG3 both have Read-only locks.

Box 2: VNET4 only

There are no locks on RG4, while the other resource groups have either Delete or Read-only locks.

Note: As an administrator, you may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. You can set the lock level to CanNotDelete or ReadOnly. In the portal, the locks are called Delete and Read-only respectively.

* CanNotDelete means authorized users can still read and modify a resource, but they can't delete the resource.

* ReadOnly means authorized users can read a resource, but they can't delete or update the resource.

Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

Scenario:

User2 is a Security administrator.

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

References:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources>

NEW QUESTION: 105

You need to prevent administrators from performing accidental changes to the Homepage app service plan.

To complete this task, sign in to the Azure portal.

See the explanation below.

Answer:

Explanation

You need to configure a 'lock' for the app service plan. A read-only lock ensures that no one can make changes to the app service plan without first deleting the lock.

* In the Azure portal, type App Service Plans App Service Plans from the search results then select Homepage. Alternatively, browse to App Service Plans in the left navigation pane.

* In the properties of the app service plan, click on

* Click the Add button to add a new lock.

* Enter a name in the Lock name field. It doesn't matter what name you provide for the exam.

* For the Lock type, select Read-only.

* Click OK to save the changes.

NEW QUESTION: 106

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: ([SHOW ANSWER](#))

Explanation

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>

Topic 1, 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	networkSecurityGroups	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.

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 (517 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 107

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: ☒ Enable ☐ Disable

Should reviewer not respond: ☐ Take recommendations ☐

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

If User2 fails to complete Review1 by March 20, 2019

Microsoft

Answer:

User3 can perform Review1 for

If User2 fails to complete Review1 by March 20, 2019

Explanation:

User3 can perform Review1 for

If User2 fails to complete Review1 by March 20, 2019

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-se>

NEW QUESTION: 108

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

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

Answer Area

OU2:

Tool

User1:

Tool

Answer:

Tools

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

Answer Area

OU2:

Azure AD Connect

User1:

The Azure portal

NEW QUESTION: 109

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.)

```

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet
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 State
-----
Allow /subscriptions/a90c8c8f-d8bc-4112-abfb-dac4906573dd/resourceGroups/RG1/providers/Microsoft.Network/virtualNetworks/VNET1/subnets/Subnet1 Succeeded

PS C:\> _

```

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: 110

You have an Azure subscription that contains the following Azure firewall:

* Name: Fw1

* Azure region: UK West

* Private IP address: 10.1.3.4

* Public IP address: 23.236.62.147

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

Name	Location	IP address space	Peered with
Vnet1	UK West	10.1.0.0/16	Vnet2
Vnet2	East US	10.2.0.0/16	Vnet1, Vnet3
Vnet3	West US	10.3.0.0/16	Vnet2,

The subscription contains the subnets shown in the following table.

Name	Virtual network	IP address range
Subnet1-1	Vnet1	10.1.1.0/24
Subnet1-2	Vnet1	10.1.2.0/24
AzureFirewallSubnet	Vnet1	10.1.3.0/24
Subnet2-1	Vnet2	10.2.1.0/24
Subnet3-1	Vnet3	10.3.1.0/24

The subscription contains the routes shown in the following table.

Name	Subnet	IP address prefix	Next hop type	Next hop IP address
Rt1	Subnet1-1	0.0.0.0/0	Virtual appliance	10.1.3.4
Rt2	Subnet1-2	10.1.1.0/24	Virtual appliance	10.1.3.4
Rt3	Subnet2-1	10.1.1.0/24	Virtual appliance	10.1.3.4
Rt4	Subnet3-1	10.2.1.0/24	Virtual appliance	10.1.3.4

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
Traffic from Subnet1-1 to Subnet 1-2 is routed through Fw1.	☐	☐
Traffic from Subnet2-1 to Subnet 1-1 is routed through Fw1.	☐	☐
Traffic from Subnet3-1 to the internet is routed through Fw1.	☐	☐

Answer:

Answer Area

Statements	Yes	No
Traffic from Subnet1-1 to Subnet 1-2 is routed through Fw1.	☒	☐
Traffic from Subnet2-1 to Subnet 1-1 is routed through Fw1.	☐	☒
Traffic from Subnet3-1 to the internet is routed through Fw1.	☒	☐

Explanation:

Answer Area

Statements	Yes	No
Traffic from Subnet1-1 to Subnet 1-2 is routed through Fw1.	☒	☐
Traffic from Subnet2-1 to Subnet 1-1 is routed through Fw1.	☐	☒
Traffic from Subnet3-1 to the internet is routed through Fw1.	☒	☐

NEW QUESTION: 111

You have an Azure subscription that contains the following resources:

- * A virtual network named VNET1 that contains two subnets named Subnet1 and Subnet2.
- * A virtual machine named VM1 that has only a private IP address and connects to Subnet1.

You need to ensure that Remote Desktop connections can be established to VM1 from the internet.

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

Configure a network security group (NSG).

Create a network rule collection.

Create a NAT rule collection.

Create a new subnet.

Deploy Azure Application Gateway.

Deploy Azure Firewall.

Answer Area

Answer:
Explanation

Create a new subnet.

Deploy Azure Firewall.

Create a NAT rule collection.

NEW QUESTION: 112

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table. Contoso.com contains a group naming policy. The policy has a custom blocked word list rule that includes the word Contoso. Which users can create a group named Contoso Sales in contoso.com? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Users who can create a security group named Contoso Sales:

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

Microsoft

Answer:

Users who can create a security group named Contoso Sales:

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

Reference:

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

NEW QUESTION: 113

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

Name	Region	Description
HubVNet	East US	HubVNet is a virtual network connected to the on-premises network by using a site-to-site VPN that has BGP route propagation enabled. HubVNet contains a subnet named HubVNetSubnet0.
SpokeVNet	East US	SpokeVNet is a virtual network connected to HubVNet by using VNet peering. SpokeVNet contains a subnet named SpokeVNetSubnet0.

The Azure virtual machines on SpokeVNetSubnet0 can communicate with the computers on the on-premises network.

You plan to deploy an Azure firewall to HubVNet.

You create the following two routing tables:

* RT1: Includes a user-defined route that points to the private IP address of the Azure firewall as a next hop address

* RT2: Disables BGP route propagation and defines the private IP address of the Azure firewall as the default gateway You need to ensure that traffic between SpokeVNetSubnet0 and the on-premises network flows through the Azure firewall.

To which subnet should you associate each route table? To answer, drag the appropriate subnets to the correct route tables. Each subnet 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.

Subnets

Azure FirewallSubnet

GatewaySubnet

HubVNetSubnet0

Answer Area

RT1:

RT2:

Subnets

Azure FirewallSubnet

GatewaySubnet

HubVNetSubnet0

Answer Area

RT1: GatewaySubnet

RT2: HubVNetSubnet0

Topic 1, Litware, inc

Case Study

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

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question on this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next sections of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question on this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

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

Existing Environment

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

Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices.

Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.

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

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

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

Azure Security Center is set to the Free tier.

Planned changes

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

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

Litware identifies the following identity and access requirements:

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

Platform Protection Requirements

Litware identifies the following platform protection requirements:

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

Security Operations Requirements

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

NEW QUESTION: 114

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.	☒	☐

NEW QUESTION: 115

You need to deploy Microsoft Antimalware to meet the platform protection requirements.

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

NOTE: Each correct selection is worth one point.

Create a custom policy definition that has effect set to:

Append

Deny

DeployIfNotExists

Create a policy assignment and modify:

The Create a Managed Identify setting

The exclusion settings

The scope

Answer:

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

Create a custom policy definition that has effect set to:

Append
Deny
DeployIfNotExists

Create a policy assignment and modify:

The Create a Managed Identify setting
The exclusion settings
The scope

Scenario: Microsoft Antimalware must be installed on the virtual machines in RG1.

RG1 is a resource group that contains Vnet1, VM0, and VM1.

Box 1: DeployIfNotExists

DeployIfNotExists executes a template deployment when the condition is met.

Azure policy definition Antimalware

Reference:

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

NEW QUESTION: 116

You create a new Azure subscription.

You need to ensure that you can create custom alert rules in Azure Security Center.

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

NOTE: Each correct selection is worth one point.

- A. Onboard Azure Active Directory (Azure AD) Identity Protection.
- B. Create an Azure Storage account.
- C. Implement Azure Advisor recommendations.
- D. Create an Azure Log Analytics workspace.
- E. Upgrade the pricing tier of Security Center to Standard.

Answer: D,E (LEAVE A REPLY)

Explanation

D: You need write permission in the workspace that you select to store your custom alert.

References:

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

NEW QUESTION: 117

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.

NOTE: Each correct selection is worth one point.

Answer Area

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:

Answer Area

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: 118

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:

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: 119

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: 120

You have an Azure subscription.
You plan to create a workflow automation in Azure Security Center that will automatically remediate a security vulnerability.
What should you create first?

- A. a managed identity
- B. an alert rule
- C. an Azure function app
- D. an Azure logic app
- E. an automation account

Answer: E (LEAVE A REPLY)

NEW QUESTION: 121

You have an Azure subscription that has a managed identity named identity and is linked to an Azure Active Directory (Azure AD) tenant. The tenant contains the resources shown in the following table.

Which resources can be added to AU1 and AU2? To answer, select the appropriate options in the answer area.

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

Which resources can be added to AU1 and AU2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



AU1:
AU2 only
Group2 only
Identity1 only
AU2 and Group2 only
Group2 and Identity1 only

AU2:
Identity1 only
AU1 and Identity1 only
Group1 and Group2 only
AU1, Group2 and Identity1 only
Group1, Group2 and User1 only

Answer:

Answer Area



freepdfdumps.com

AU1:
AU2 only
Group2 only
Identity1 only
AU2 and Group2 only
Group2 and Identity1 only

AU2:
Identity1 only
AU1 and Identity1 only
Group1 and Group2 only
AU1, Group2 and Identity1 only
Group1, Group2 and User1 only

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 (517 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 122

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	Yes	No
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: 123

You have three Azure subscriptions and a user named User1.

You need to provide User1 with the ability to manage and view costs for the resources across all three subscriptions. The solution must use the principle of least privilege.

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.

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Actions

- Create a management group.
- Add the three subscriptions to the management group.
- Assign User1 the Global administrator role.
- Assign User1 the Owner role for the management group.
- Assign User1 the Cost Management Contributor role for the management group.

Answer:

Actions

Create a management group.	Assign User1 the Cost Management Contributor role for the management group.
Add the three subscriptions to the management group.	
Assign User1 the Global administrator role.	Assign User1 the Global administrator role.
Assign User1 the Owner role for the management group.	
Assign User1 the Cost Management Contributor role for the management group.	Add the three subscriptions to the management group.

Explanation:

Actions

Create a management group.
Assign User1 the Owner role for the management group.
Assign User1 the Cost Management Contributor role for the management group.

Answer Area

1	Assign User1 the Cost Management Reader role for the management group.
2	Assign User1 the Global administrator role.
3	Add the three subscriptions to the management group.

NEW QUESTION: 124

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:

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

Platforms:

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

Answer:

Operating systems:

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

Platforms:

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

NEW QUESTION: 125

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

Name	Pattern	Case sensitivity
Condition1	White	On
Condition2	Black	Off

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

Name	Applies to	Use label	Set the default label
Global	<i>Not applicable</i>	None	None
Policy1	User1	Label1	None
Policy2	User1	Label2	None

You need to identify how Azure Information Protection will label files.

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

NOTE: Each correct selection is worth one point.

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

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

Answer:

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

No label
Label1 only
Label2 only
Label1 and Label2

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

No label
Label1 only
Label2 only
Label1 and Label2

Reference:

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

NEW QUESTION: 126

You have the Azure key vaults shown in the following table.

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

KV1 stores a secret named Secret1 and a key for a managed storage account named Key1.

You back up Secret1 and Key1.

To which key vaults can you restore each backup? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

You can restore the Secret1 backup to:

▼

KV1 only

KV1 and KV2 only

KV1, KV2 and KV3 only

KV1, KV2 and KV4 only

KV1, KV2, KV3, KV4, and KV5

You can restore the Key1 backup to:

▼

KV1 only

KV1 and KV2 only

KV1, KV2 and KV3 only

KV1, KV2 and KV4 only

KV1, KV2, KV3, KV4, and KV5

Answer:

You can restore the Secret1 backup to:

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

You can restore the Key1 backup to:

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

NEW QUESTION: 127

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

Name	Member of	Mobile phone	Multi-factor authentication (MFA) status
User1	Group1	123 555 7890	Disabled
User2	Group1, Group2	None	Enabled
User3	Group1	123 555 7891	Required

You create and enforce an Azure AD Identity Protection user risk policy that has the following settings:

- * Assignment: Include Group1, Exclude Group2
- * Conditions: Sign-in risk of Medium and above
- * Access: Allow access, Require password change

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 User1 signs in from an unfamiliar location, he must change his password.	☐	☐
If User2 signs in from an anonymous IP address, she must change her password.	☐	☐
If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password.	☐	☐

Answer:

Statements	Yes	No
If User1 signs in from an unfamiliar location, he must change his password.	☒	☐
If User2 signs in from an anonymous IP address, she must change her password.	☒	☐
If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password.	☐	☒

Explanation:

Statements	Yes	No
If User1 signs in from an unfamiliar location, he must change his password.	☒	☐
If User2 signs in from an anonymous IP address, she must change her password.	☒	☐
If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password.	☐	☒

Box 1: Yes

User1 is member of Group1. Sign in from unfamiliar location is risk level Medium.

Box 2: Yes

User2 is member of Group1. Sign in from anonymous IP address is risk level Medium.

Box 3: No

Sign-ins from IP addresses with suspicious activity is low.

Note:

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

Azure AD Identity protection can detect six types of suspicious sign-in activities:

- * Users with leaked credentials
- * Sign-ins from anonymous IP addresses
- * Impossible travel to atypical locations
- * Sign-ins from infected devices
- * Sign-ins from IP addresses with suspicious activity
- * Sign-ins from unfamiliar locations

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

References:

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

NEW QUESTION: 128

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

NEW QUESTION: 129

SIMULATION

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: User1-10598168@ExamUsers.com

Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168

https://login.microsoftonline.com/

This site uses cookies for analytics, personalized content and ads. By

Microsoft Azure

Microsoft

Sign in

to continue to Microsoft Azure

Email, phone, or Skype

No account? [Create one!](#)

Can't access your account?

Next

Sign in with GitHub

Terms of use

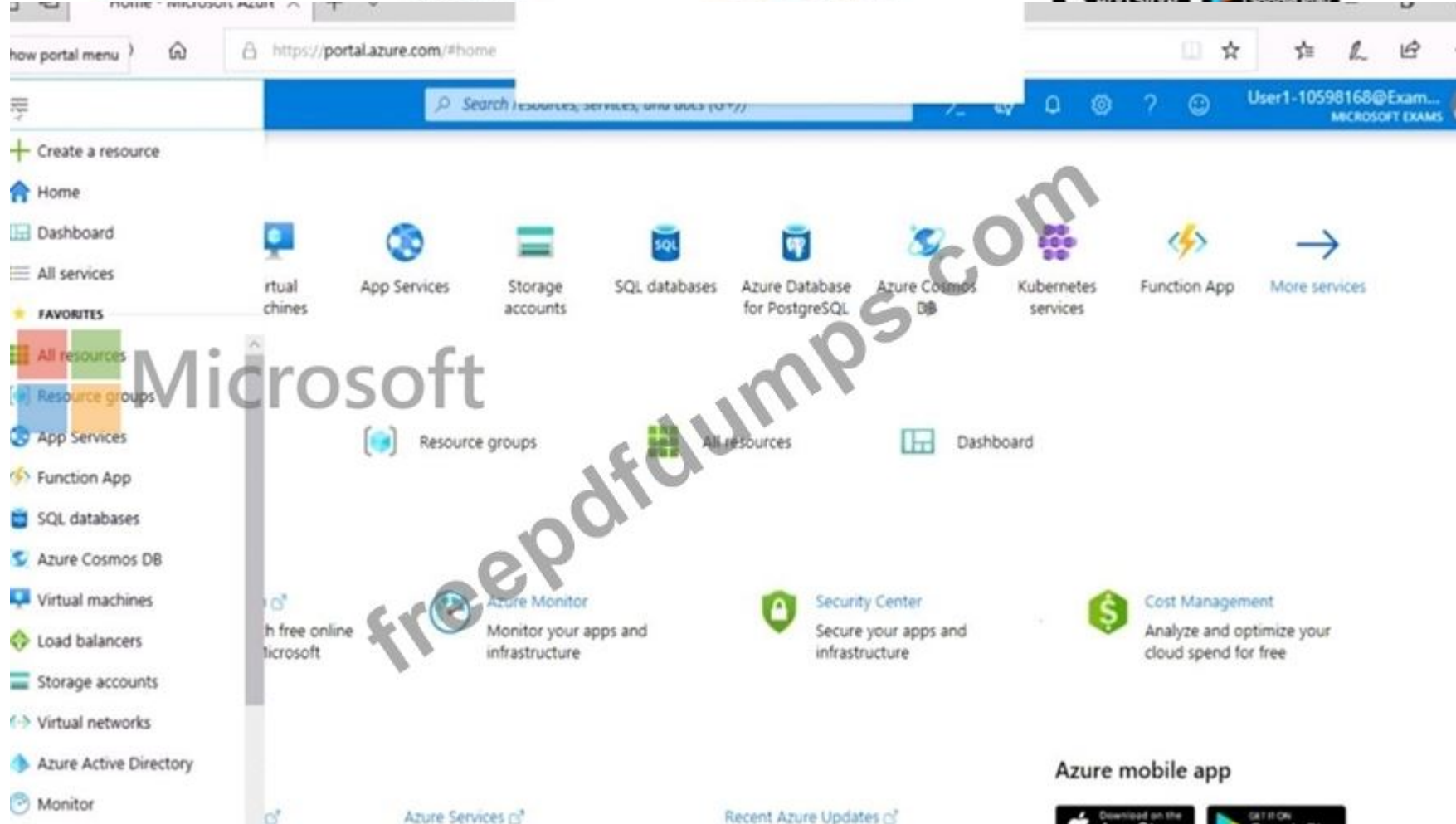
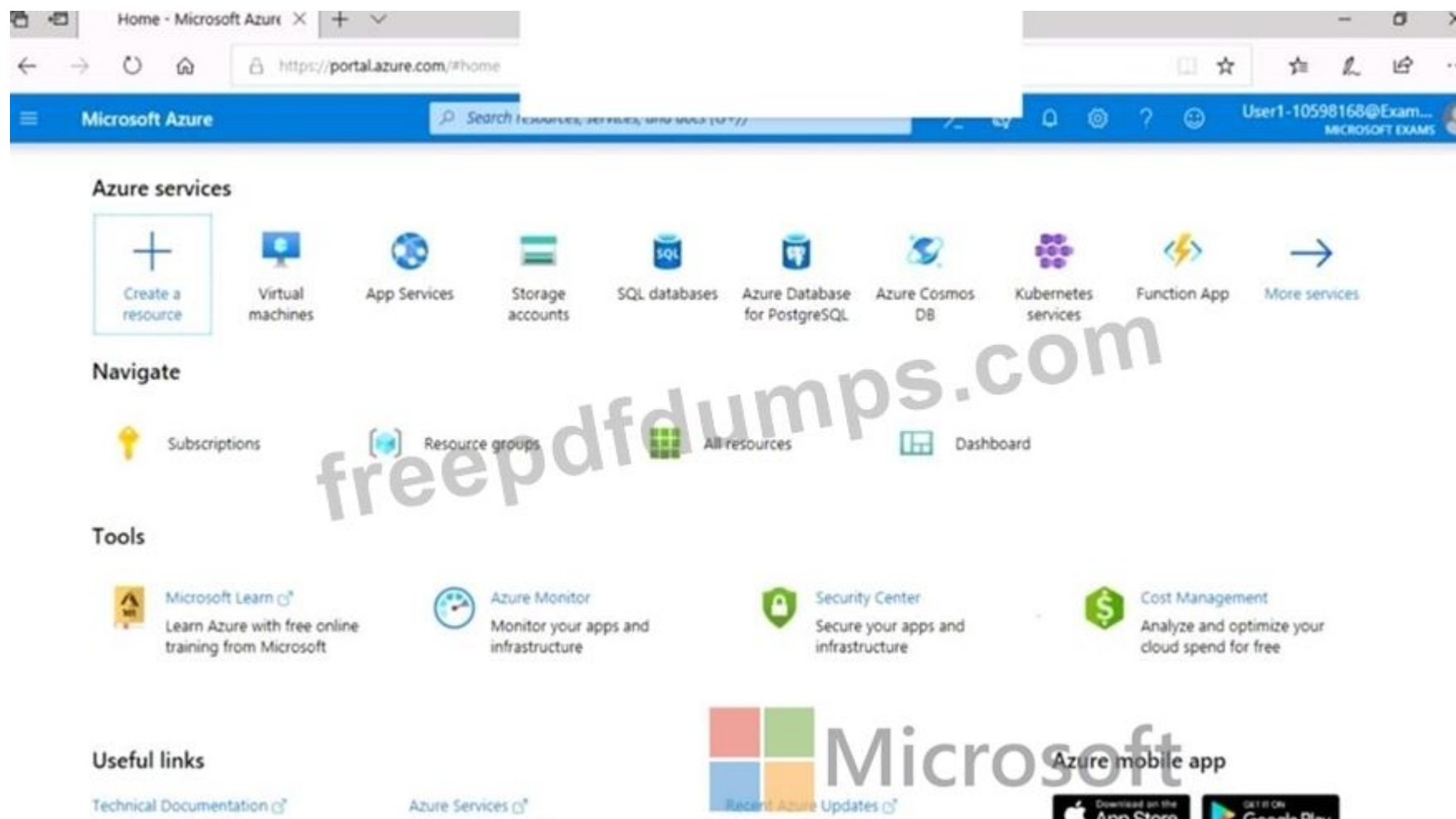
Privacy & cookies

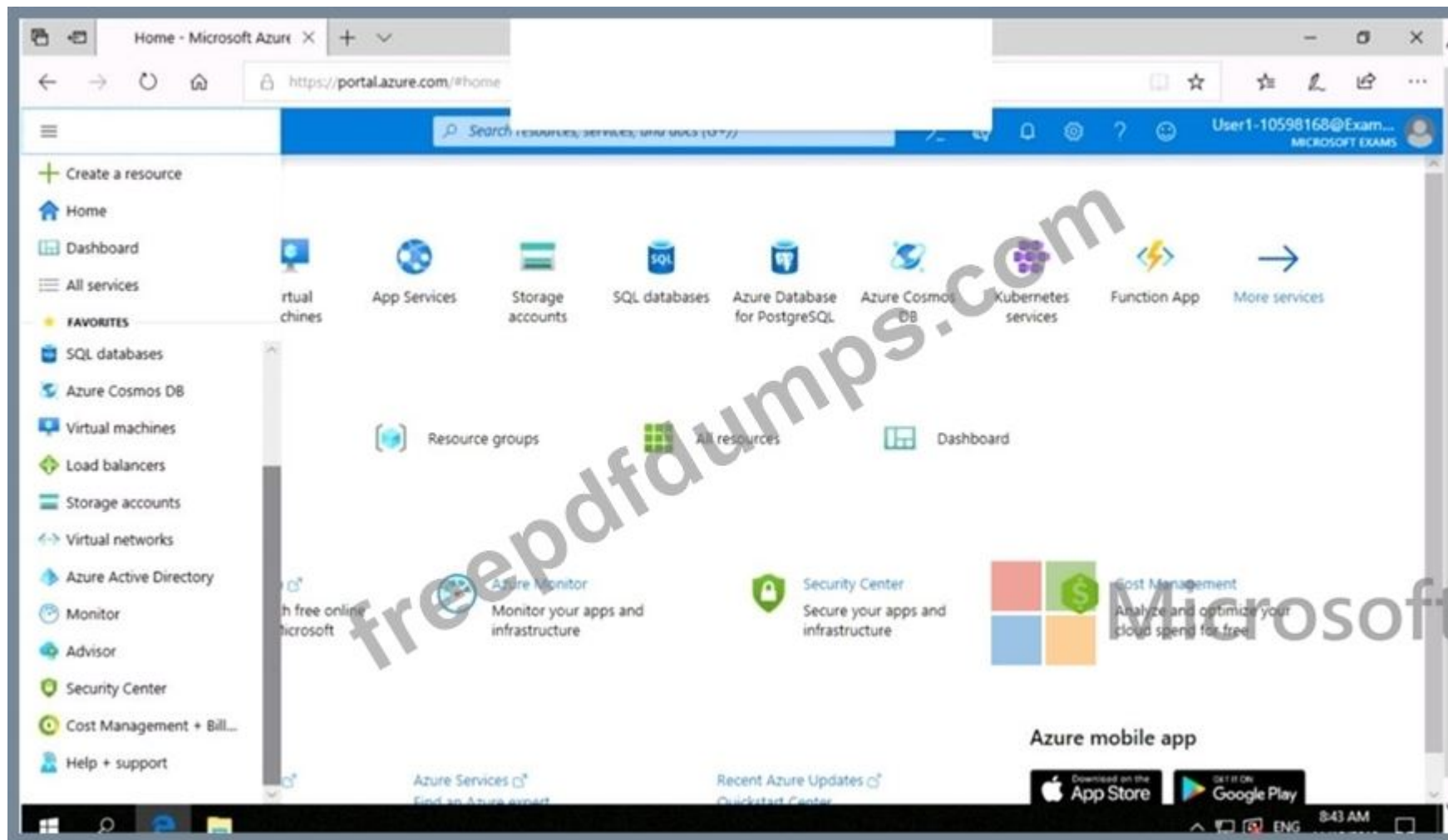
...

ENG

8:39 AM

11/15/2019





You need to configure Azure to allow RDP connections from the Internet to a virtual machine named VM1. The solution must minimize the attack surface of VM1. To complete this task, sign in to the Azure portal.

A. To enable the RDP port in an NSG, follow these steps:

- * Sign in to the Azure portal.
- * In Virtual Machines, select VM1
- * In Settings, select Networking.
- * In Inbound port rules, check whether the port for RDP is set correctly. The following is an example of the configuration:

Priority: 300

Name: Port_3389

Port(Destination): 3389

Protocol: TCP

Source: Any

Destinations: Any

Action: Allow

B. To enable the RDP port in an NSG, follow these steps:

- * Sign in to the Azure portal.
- * In Virtual Machines, select VM1
- * In Settings, select Networking.
- * In Inbound port rules, check whether the port for RDP is set correctly. The following is an example of the configuration:

Priority: 300

Name: Port_3889
Port(Destination): 3388
Protocol: TCP
Source: Any
Destinations: Any
Action: Allow

Answer: ([SHOW ANSWER](#))

Reference:
<https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-nsg-problem>

NEW QUESTION: 130

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:

Download images:

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: 131

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

- 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:

Create an incident:

Initiate a script to configure the firewall rule:

Component

Component

Component

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



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: 132

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: (SHOW ANSWER)

You can use Azure Automation State Configuration to manage Azure VMs (both Classic and Resource Manager), on-premises VMs, Linux machines, AWS VMs, and on-premises physical machines.

Note: Azure Automation State Configuration provides a DSC pull server similar to the Windows Feature DSCService so that target nodes automatically receive configurations, conform to the desired state, and report back on their compliance. The built-in pull server in Azure Automation eliminates the need to set up and maintain your own pull server. Azure Automation can target virtual or physical Windows or Linux machines, in the cloud or on-premises.

Reference:

<https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started>

NEW QUESTION: 133

You need to deploy Microsoft Antimalware to meet the platform protection requirements.

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

NOTE: Each correct selection is worth one point.

Create a custom policy definition that has effect set to:

▼

Append

Deny

DeployIfNotExists

Create a policy assignment and modify:

▼

The Create a Managed Identify setting

The exclusion settings

The scope

Answer:

Create a custom policy definition that has effect set to:

▼

Append

Deny

DeployIfNotExists

Create a policy assignment and modify:

▼

The Create a Managed Identify setting

The exclusion settings

The scope

NEW QUESTION: 134

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:  Microsoft

- 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

NEW QUESTION: 135

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	Yes	No
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.	☒	☐

NEW QUESTION: 136

You are evaluating the security of VM1, VM2, and VM3 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 the Internet, you can connect to the web server on VM1 by using HTTP.	☐	☐
From the Internet, you can connect to the web server on VM2 by using HTTP.	☐	☐
From the Internet, you can connect to the web server on VM3 by using HTTP.	☐	☐

Answer:

Answer Area

Statements	Yes	No
From the Internet, you can connect to the web server on VM1 by using HTTP.	☒	☐
From the Internet, you can connect to the web server on VM2 by using HTTP.	☐	☒
From the Internet, you can connect to the web server on VM3 by using HTTP.	☒	☐

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 (517 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 137

A user named Debbie has the Azure app installed on her mobile device.

You need to ensure that debbie@contoso.com is alerted when a resource lock is deleted.

To complete this task, sign in to the Azure portal.

You need to configure an alert rule in Azure Monitor.

Type Monitor into the search box and select Monitor from the search results.

Click on Alerts.

Click on +New Alert Rule.

In the Scope section, click on the Select resource link.

In the Filter by resource type box, type locks and select Management locks (locks) from the filtered results.

Select the subscription then click the Done button.

In the Condition section, click on the Select condition link.

Select the Delete management locks condition then click the Done button.

In the Action group section, click on the Select action group link.

Click the Create action group button to create a new action group.

Give the group a name such as Debbie Mobile App (it doesn't matter what name you enter for the exam) then click the Next: Notifications > button.

In the Notification type box, select the Email/SMS message/Push/Voice option.

In the Email/SMS message/Push/Voice window, tick the Azure app Push Notifications checkbox and enter debbie@contoso.com in the Azure account email field.

Click the OK button to close the window.

A. Click the Create alert rule button to create the alert rule.

B. Back in the Create alert rule window, in the Alert rule details section, enter a name such as Management lock deletion in the Alert rule name field.

C. Click the Review & Create button then click the Create button to create the action group.

D. Enter a name such as Debbie Mobile App in the notification name box.

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

NEW QUESTION: 138

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. Off

B. Report only

C. On

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

NEW QUESTION: 139

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.)

Role settings

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 approvers
No 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.	☒	☐

References:

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

NEW QUESTION: 140

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: Component
A data connector for the firewall software	Create an incident: Component
A playbook	Initiate a script to configure the firewall rule: Component
A rule	
A Security Events connector	
A workbook	

Answer:

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

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: 141

You need to configure an access review. The review will be assigned to a new collection of reviews and reviewed by resource owners.

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

Create an access review program.

Set Reviewers to Selected users.

Create an access review audit.

Create an access review control.

Set Reviewers to Group owners.

Set Reviewers to Members.



Answer:

Actions

Create an access review program.

Set Reviewers to Selected users.

Create an access review audit.

Create an access review control.

Set Reviewers to Group owners.

Set Reviewers to Members.



Answer Area

Create an access review program.

Create an access review control.

Set Reviewers to Group owners.



Explanation

Answer Area

Create an access review program.

Create an access review control.

Set Reviewers to Group owners.

Step 1: Create an access review program

Step 2: Create an access review control

Step 3: Set Reviewers to Group owners

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.



References:

<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: 142

You have an Azure subscription that contains the following resources:

- * A virtual network named VNET1 that contains two subnets named Subnet1 and Subnet2.
- * A virtual machine named VM1 that has only a private IP address and connects to Subnet1.

You need to ensure that Remote Desktop connections can be established to VM1 from the internet.

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

Configure a network security group (NSG).

Create a network rule collection.

Create a NAT rule collection.

Create a new subnet.

Deploy Azure Application Gateway.

Deploy Azure Firewall.

Answer Area

Answer:

Actions

Configure a network security group (NSG).

Create a network rule collection.

Create a NAT rule collection.

Create a new subnet.

Deploy Azure Application Gateway.

Deploy Azure Firewall.

Answer Area

Create a new subnet.

Deploy Azure Firewall.

Create a NAT rule collection.

NEW QUESTION: 143

You need to deploy Microsoft Antimalware to meet the platform protection requirements.

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

NOTE: Each correct selection is worth one point.

Create a custom policy definition that has effect set to:

Append

Deny

DeployIfNotExists

Create a policy assignment and modify:

The Create a Managed Identify setting

The exclusion settings

The scope

Answer:

Create a custom policy definition that has effect set to:

Create a policy assignment and modify:

Explanation

Create a custom policy definition that has effect set to:

Create a policy assignment and modify:

Scenario: Microsoft Antimalware must be installed on the virtual machines in RG1.

RG1 is a resource group that contains Vnet1, VM0, and VM1.

Box 1: DeployIfNotExists

DeployIfNotExists executes a template deployment when the condition is met.

Azure policy definition Antimalware

Reference:

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

NEW QUESTION: 144

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. Create an Azure Sentinel workspace.

- B. Create an Azure Advanced Threat Protection (ATP) instance.
- C. Add the SQL Health Check solution to Azure Monitor.
- D. Enable Advanced Data Security.

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

NEW QUESTION: 145

You have an Azure subscription that contains a resource group named RG1. RG1 contains a virtual machine named VM1 that uses Azure Active Directory (Azure AD) authentication.

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

The permissions for Role2 are shown in the following JSON code.

```
"permissions": [  
  {  
    "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	Role1, 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.

Answer Area

Statements	Yes	No
User1 can delete VM1.	☐	☐
User2 can delete VM1.	☐	☐
User3 can sign in to VM1 by using Azure AD credentials.	☐	☐

Answer:
Answer Area

Statements	Yes	No
User1 can delete VM1.	☐	☒
User2 can delete VM1.	☒	☐
User3 can sign in to VM1 by using Azure AD credentials.	☒	☐

NEW QUESTION: 146

You have an Azure subscription that contains the alerts shown in the following exhibit.

All Alerts

+ New alert rule | Edit columns | Manage alert rules | View classic alerts | Refresh | Change state

Don't see a subscription? [Open Directory + Subscription settings](#)

* Subscription: Azure Pass - Sponsorship | Resource group: Type to start filtering ... | Resource type: 0 selected | Resource: Type to start filtering ... | Time range: Past hour

Monitor service: 15 selected | Monitor condition: 2 selected | Severity: Sev 4 | Alert state: 3 selected | Smart group id: Smart group id

All Alerts | Alerts By Smart Group (Preview)

Search by name (case-insensitive)

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

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.

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

cannot be changed
 can be changed to Closed only
 can be changed to New only
 can be changed to New or Closed

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

cannot be changed
 can be changed to Acknowledged only
 can be changed to New only
 can be changed to New or Acknowledged

Answer:

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

cannot be changed
 can be changed to Closed only
 can be changed to New only
 can be changed to New or Closed

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

cannot be changed
 can be changed to Acknowledged only
 can be changed to New only
 can be changed to New or Acknowledged

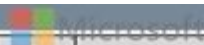
Explanation:

References:

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

NEW QUESTION: 147

Your company has an Azure subscription named Subscription1. Subscription1 is associated with the Azure Active Directory tenant that includes 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: 

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

Reference:

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

NEW QUESTION: 148

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.

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

Reference:

<https://docs.microsoft.com/en-us/azure/automation/automation-update-management>

NEW QUESTION: 149

You have an Azure subscription that contains a virtual machine named VM1.

You create an Azure key vault that has the following configurations:

Name: Vault5

Region: West US

Resource group: RG1

You need to use Vault5 to enable Azure Disk Encryption on VM1. The solution must support backing up VM1 by using Azure Backup.

Which key vault settings should you configure?

A. Access policies

- B. Secrets
 - C. Keys
 - D. Locks
- Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 150

From Azure Security Center, you need to deploy SecPol1.
What should you do first?

- A. Enable Azure Defender.
- B. Create an Azure Management group.
- C. Create an initiative.
- D. Configure continuous export.

Answer: B (LEAVE A REPLY)

Reference:
<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/security-center/custom-security-policies.md>
<https://zimmergren.net/create-custom-security-center-recommendation-with-azure-policy/>

NEW QUESTION: 151

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": [],
  "notDataActions": []
],
"permissions": [
  {
    "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.

Answer Area



Statements

Yes

No

User1 can delete VM1.

☐
☐

User2 can delete VM1.

☐
☐

User3 can delete VM1.

☐
☐

Answer:

Answer Area

Statements

Yes

No

User1 can delete VM1.

☐
☒

User2 can delete VM1.

☐
☒

User3 can delete VM1.

☒
☐


Microsoft

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 (517 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 152

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

Configure secrets for the Azure key vault.

Create an Azure key vault.

Run Set-AzureRmStorageAccount.

Configure access policies for the Azure key vault.

Run Set-AzureRmVmDiskEncryptionExtension.

Answer Area

Answer:

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:

References:

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

NEW QUESTION: 153

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

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

You create the groups shown in the following table.

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

Which resources can you add to Group5 and Group6? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Group5: ▼

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

Group6: ▼

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

Answer:

Group5:

▼

User1 only

User1 and Group1 only

User1, Group1, and Managed1 only

User1, Group1, Managed1, and App1

Group6:

▼

User1 only

User1 and Group1 only

User1, Group1, and Managed1 only

User1, Group1, Managed1, and App1

NEW QUESTION: 154
You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

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

You create an Azure role by using the following JSON file.

```

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

```

You assign Role1 to User1 for 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.

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

Answer:

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

Reference:

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

NEW QUESTION: 155

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: 156

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.

NOTE: Each correct selection is worth one point.

Answer Area

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:

Answer Area

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: 157

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant and a user named User1.

The App registrations settings for the tenant are configured as shown in the following exhibit.

App registrations

Users can register applications

Yes

No

You plan to deploy an app named App1.
You need to ensure that User1 can register App1 in Azure AD. The solution must use the principle of least privilege.
Which role should you assign to User1?
A. App Configuration Data Owner for the subscription
B. Managed Application Contributor for the subscription
C. Cloud application administrator in Azure AD
D. Application developer in Azure AD.
Answer: D (LEAVE A REPLY)
Reference:
<https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task>

NEW QUESTION: 158

You implement the planned changes for ASG1 and ASG2.
In which NSGs can you use ASG1. and the network interfaces of which virtual machines can you assign to ASG2?

Answer Area



freepdfdumps.com

NSGs:

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

Virtual machines:

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

Answer:

Answer Area



freepdfdumps.com

NSGs:

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

Virtual machines:

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

NEW QUESTION: 159

You have an Azure subscription named Sub 1 that is associated to an Azure Active Directory (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

Users who can onboard Azure AD Identity Protection:

User1 only

User1 and User2 only

User1, User 2, and User3 only

User1, User 2, User3, and User 4 only

Users who can remediate users and configure policies:

User1 and User2 only

User1 and User3 only

User1, User 2, and User3 only

User1, User 2, User3, and User 4

Answer:
Answer Area

Users who can onboard Azure AD Identity Protection:

User1 only

User1 and User2 only

User1, User 2, and User3 only

User1, User 2, User3, and User 4 only

Users who can remediate users and configure policies:

User1 and User2 only

User1 and User3 only

User1, User 2, and User3 only

User1, User 2, User3, and User 4

NEW QUESTION: 160

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.)

Role settings

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 approvers

No 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:

References:

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

NEW QUESTION: 161

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 1

You need to configure Azure to allow RDP connections from the Internet to a virtual machine named VM1.

The solution must minimize the attack surface of VM1.

Answer:

Check below steps in explanation for Task.

Explanation

To configure Azure to allow RDP connections from the Internet to a virtual machine named VM1, you can follow the steps below:

Create a new inbound security rule in the network security group (NSG) that is associated with the virtual network subnet that contains VM1. The rule should allow RDP traffic from the Internet to the virtual network subnet. You can use the Azure portal, Azure PowerShell, or Azure CLI to create the rule.

Configure the network security group (NSG) to associate it with the virtual network subnet that contains VM1.

Configure the virtual machine to allow RDP traffic. You can use the Azure portal, Azure PowerShell, or Azure CLI to configure the virtual machine.

To minimize the attack surface of VM1, you can use the following best practices:

Use a strong password for the local administrator account on the virtual machine.

Use Network Security Groups (NSGs) to restrict traffic to only the necessary ports and protocols.

Use Azure Security Center to monitor and protect your virtual machines.

NEW QUESTION: 162

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

Microsoft

ASG1:

ASG2:

Answer:

Answer as below.

Answer Area

Microsoft

ASG1: VM2, VM3, and VM4 only

ASG2: VM1, VM2, and VM4 only

NEW QUESTION: 163

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

NEW QUESTION: 164

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has an Active Directory forest with a single domain, named weylandindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.

You have been tasked with integrating Active Directory and the Azure AD tenant. You intend to deploy Azure AD Connect.

Your strategy for the integration must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.

Solution: You recommend the use of pass-through authentication and seamless SSO with password hash synchronization.

Does the solution meet the goal?

A. Yes

B. No

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

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>

NEW QUESTION: 165

You have an Azure subscription.

You need to create and deploy an Azure policy that meets the following requirements:

When a new virtual machine is deployed, automatically install a custom security extension.

Trigger an autogenerated remediation task for non-compliant virtual machines to install the extension.

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

NOTE: Each correct selection is worth one point.

Definition effect:  ▼

- Append
- DeployIfNotExists
- EnforceOPAConstraint
- EnforceRegoPolicy
- Modify

Assignment remediation task: ▼

- A managed identity that has the Contributor role
- A managed identity that has the User Access Administrator role
- A service principal that has the Contributor role
- A service principal that has the User Access Administrator role

Answer:

Definition effect: ▼

- Append
- DeployIfNotExists
- EnforceOPAConstraint
- EnforceRegoPolicy
- Modify

Assignment remediation task: ▼

- A managed identity that has the Contributor role
- A managed identity that has the User Access Administrator role
- A service principal that has the Contributor role
- A service principal that has the User Access Administrator role

Explanation

Definition effect:  ▼

- Append
- DeployIfNotExists
- EnforceOPAConstraint
- EnforceRegoPolicy
- Modify

Assignment remediation task: ▼

- A managed identity that has the Contributor role
- A managed identity that has the User Access Administrator role
- A service principal that has the Contributor role
- A service principal that has the User Access Administrator role

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources>

NEW QUESTION: 166

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.

Name	Resource group	TDE
SQL2	RG2	Disabled
SQL3	RG1	Disabled

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
SQL1 will have TDE enabled automatically.	☐	☐
The deployment of SQL2 will fail.	☐	☐
SQL3 will be deployed and marked as noncompliant.	☐	☐

Answer:

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

Reference:

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

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 (517 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 167

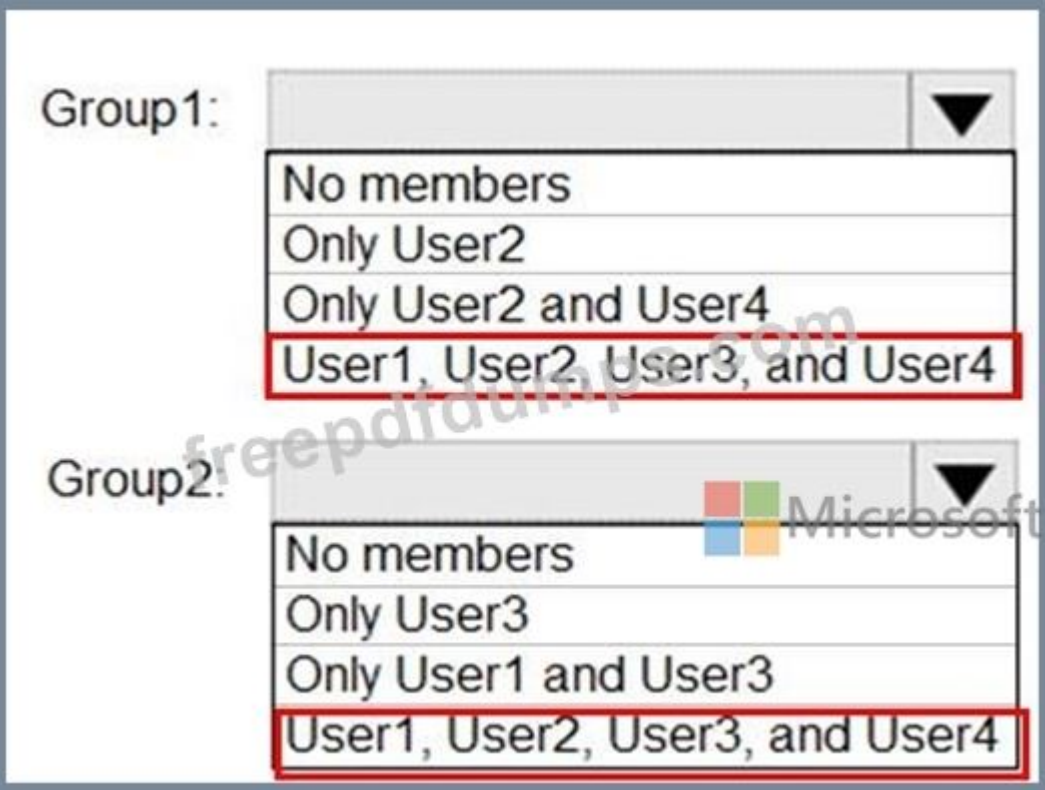
What is the membership of Group1 and Group2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Group1:

Group2:

Answer:



Reference:

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

Topic 2, Litware, inc

Existing Environment

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

Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices.

Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.

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

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

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

Azure Security Center is set to the Free tier.

Planned changes

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

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

Litware identifies the following identity and access requirements:

All San Francisco users and their devices must be members of Group1.

The members of Group2 must be assigned the Contributor role to Resource Group2 by using a permanent eligible assignment.

Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.

Platform Protection Requirements

Litware identifies the following platform protection requirements:

Microsoft Antimalware must be installed on the virtual machines in Resource Group1.

The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.

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

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.

A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.

Security Operations Requirements

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

NEW QUESTION: 168

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.	☐	☒

NEW QUESTION: 169

You have an Azure subscription that contains the alerts shown in the following exhibit.

All Alerts

+ New alert rule Edit columns Manage alert rules View classic alerts Refresh Change state

Don't see a subscription? [Open Directory + Subscription settings](#)

* Subscription: Azure Pass - Sponsorship Resource group: Type to start filtering ... Resource type: 0 selected Resource: Type to start filtering ... Time range: Past hour

Monitor service: 15 selected Monitor condition: 2 selected Severity: Sev 4 Alert state: 3 selected Smart group id: Smart group id

All Alerts Alerts By Smart Group (Preview)

Search by name (case-insensitive)

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

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.

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

cannot be changed
can be changed to Closed only
can be changed to New only
can be changed to New or Closed

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

cannot be changed
can be changed to Acknowledged only
can be changed to New only
can be changed to New or Acknowledged

Answer:

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

▼

- cannot be changed
- can be changed to Closed only
- can be changed to New only
- can be changed to New or Closed

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

▼

- cannot be changed
- can be changed to Acknowledged only
- can be changed to New only
- can be changed to New or Acknowledged

Reference:

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

NEW QUESTION: 170

You have an Azure subscription that contains the following resources:

A virtual network named VNET1 that contains two subnets named Subnet1 and Subnet2.

A virtual machine named VM1 that has only a private IP address and connects to Subnet1.

You need to ensure that Remote Desktop connections can be established to VM1 from the internet.

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 a network security group (NSG).	
Create a network rule collection.	
Create a NAT rule collection.	
Create a new subnet.	
Deploy Azure Application Gateway.	
Deploy Azure Firewall.	

Answer:



Actions

- Configure a network security group (NSG).
- Create a network rule collection.
- Create a NAT rule collection.
- Create a new subnet.
- Deploy Azure Application Gateway.
- Deploy Azure Firewall.

Answer Area

- Create a new subnet.
- Deploy Azure Firewall.
- Create a NAT rule collection.



NEW QUESTION: 171

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

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

The tenant contains the named locations shown in the following table.

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

You create the conditional access policies for a cloud app named App1 as shown in the following table.

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

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 can access App1 from an IP address of 154.12.18.10.	☐	☐
User2 can access App1 from an IP address of 193.77.10.15.	☐	☐
User2 can access App1 from an IP address of 154.12.18.34.	☐	☐

Answer:

Answer Area

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

Explanation

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

NEW QUESTION: 172

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	AllowAzureLoadBalanc...	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:

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: 173

You have two Azure virtual machines in the East US2 region as shown in the following table.

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

You deploy and configure an Azure Key vault.

You need to ensure that you can enable Azure Disk Encryption on VM1 and VM2.

What should you modify on each virtual machine? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

VM1:

The operating system version

The tier

The type

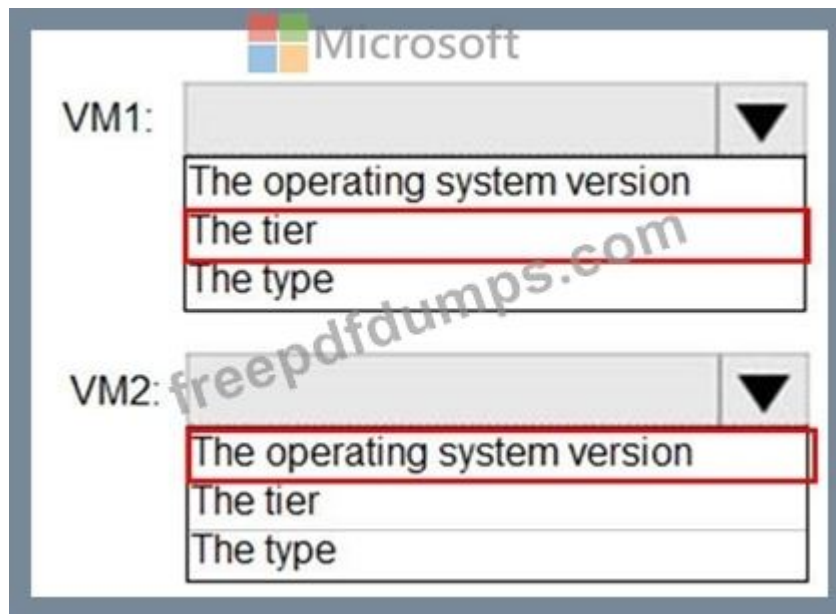
VM2:

The operating system version

The tier

The type

Answer:



Reference:

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

NEW QUESTION: 174

You have an Azure subscription that contains an Azure web app named Appl.

You plan to configure a Conditional Access policy for Appl. The solution must meet the following requirements:

- * Only allow access to App1 from Windows devices.
- * Only allow devices that are marked as compliant to access Appl.

Which Conditional Access policy settings should you configure? To answer, drag the appropriate settings to the correct requirements. Each setting 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:



NEW QUESTION: 175

You need to meet the technical requirements for VNetwork1.

What should you do first?

- A.** Create a new subnet on VNetwork1.
- B.** Remove the NSGs from Subnet11 and Subnet13.
- C.** Associate an NSG to Subnet12.
- D.** Configure DDoS protection for VNetwork1.

<https://www.fast2test.com/AZ-500-practice-test.html> 36

Valid Fast2test AZ-500 Exam PDF Dumps - New AZ-500 Real Exam Questions

Answer: A (LEAVE A REPLY)

From scenario: Deploy Azure Firewall to VNetwork1 in Sub2.

Azure firewall needs a dedicated subnet named AzureFirewallSubnet.

References:

<https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal>

<https://www.fast2test.com/AZ-500-practice-test.html> 37

Valid Fast2test AZ-500 Exam PDF Dumps - New AZ-500 Real Exam Questions

Implement platform protection

Question Set 3

NEW QUESTION: 176

You have an Azure subscription that contains a user named Admin1 and a resource group named RG1.

In Azure Monitor, you create the alert rules shown in the following table.

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

Admin1 performs the following actions on RG1:

- * Adds a virtual network named VNET1
- * Adds a Delete lock named Lock1

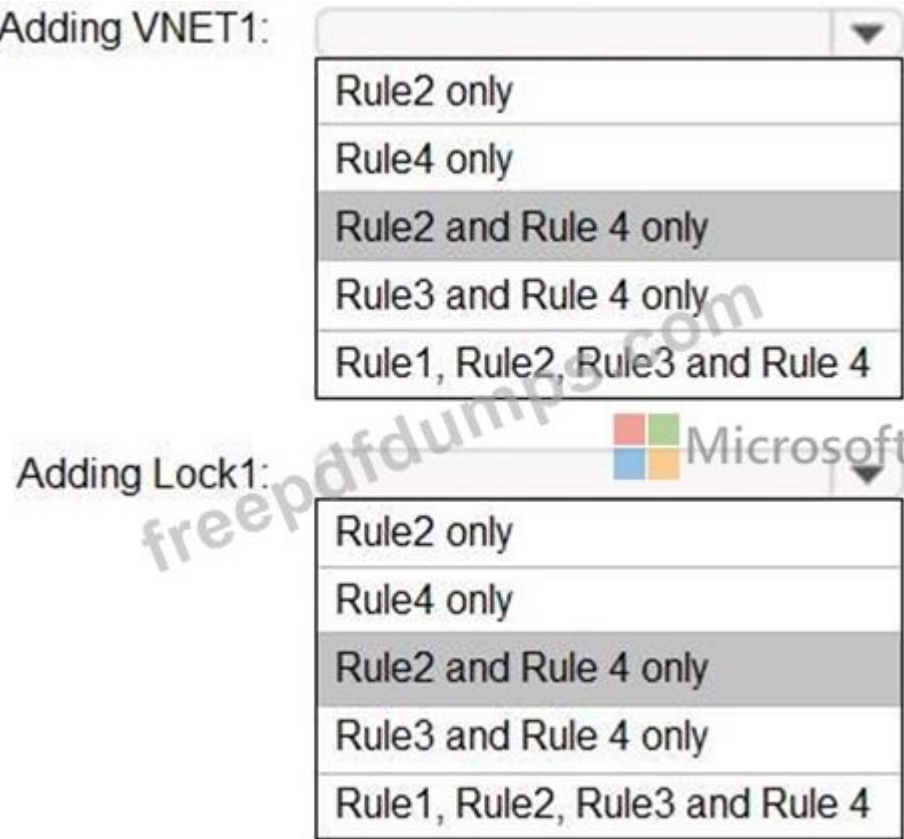
Which rules will trigger an alert as a result of the actions of Admin1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation



NEW QUESTION: 177

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.)

Role settings

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 approvers

No 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.	☒	☐

Reference:

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

NEW QUESTION: 178

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

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

User1 is a member of Group1. Group1 and User2 are assigned the Key Vault Contributor role for Vault1.

On January 1, 2019, you create a secret in Vault1. The secret is configured as shown in the exhibit. (Click the Exhibit tab.)

Create a secret

Upload options

Manual

* Name ⓘ

Password1

* Value

• • • • • • • •

Content type (optional)

Set activation date? ☒

Activation Date

2019-03-01 12:00:00 AM

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

Set expiration Date? ⓘ ☒

Expiration Date

2020-03-01 12:00:00 AM

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

Enabled? ☒ Yes ☐ No



User2 is assigned an access policy to Vault1. The policy has the following configurations:

Key Management Operations: Get, List, and Restore

Cryptographic Operations: Decrypt and Unwrap Key

Secret Management Operations: Get, List, and Restore

Group1 is assigned an access to Vault1. The policy has the following configurations:

Key Management Operations: Get and Recover

Secret Management Operations: List, Backup, and Recover

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

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

Answer:

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

NEW QUESTION: 179

You need to configure an access review. The review will be assigned to a new collection of reviews and reviewed by resource owners.

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

Create an access review program.

Set Reviewers to Selected users.

Create an access review audit.

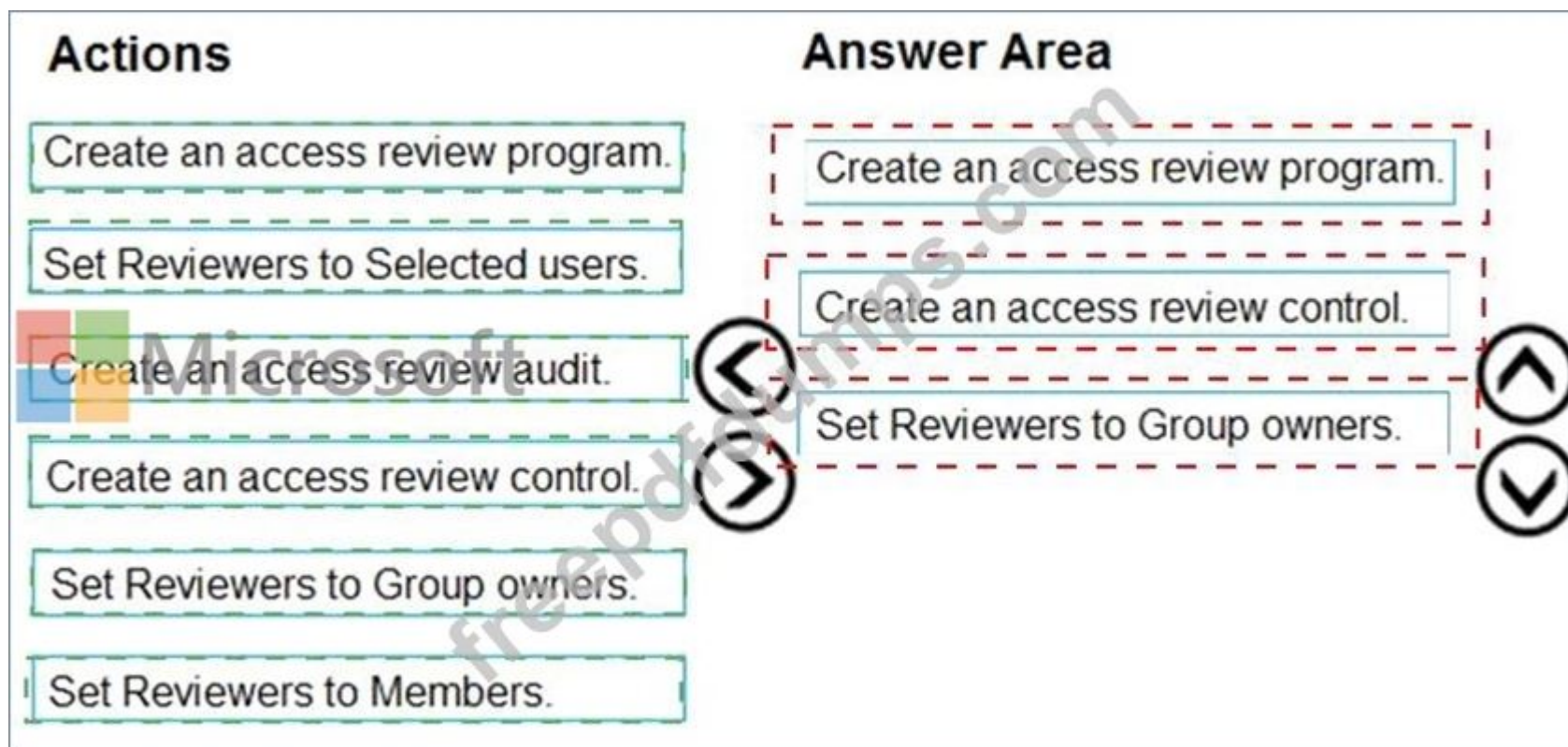
Create an access review control.

Set Reviewers to Group owners.

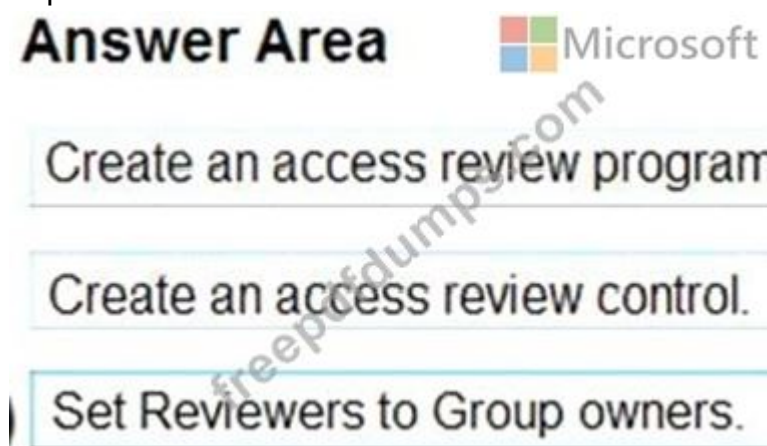
Set Reviewers to Members.



Answer:



Explanation:



Step 1: Create an access review program

Step 2: Create an access review control

Step 3: Set Reviewers to Group owners

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.



References:

<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: 180

You have the Azure key vaults shown in the following table.

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

KV1 stores a secret named Secret1 and a key for a managed storage account named Key1.

You back up Secret1 and Key1.

To which key vaults can you restore each backup? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

You can restore the Secret1 backup to:

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

You can restore the Key1 backup to:

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

Answer:

You can restore the Secret1 backup to:

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

You can restore the Key1 backup to:

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

Explanation:

You can restore the Secret1 backup to:

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

You can restore the Key1 backup to:

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

The backups can only be restored to key vaults in the same subscription and same geography. You can restore to a different region in the same geography.

<https://docs.microsoft.com/en-us/azure/key-vault/general/backup?tabs=azure-cli>

NEW QUESTION: 181

Which virtual networks in Sub1 can User2 modify and delete in their current state? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Virtual networks that User2 can modify:

	▼
VNET4 only	
VNET4 and VNET1 only	
VNET4, VNET3, and VNET1 only	
VNET4, VNET3, VNET2, and VNET1	



Virtual networks that User2 can delete:

	▼
VNET4 only	
VNET4 and VNET1 only	
VNET4, VNET3, and VNET1 only	
VNET4, VNET3, VNET2, and VNET1	

Answer:

Virtual networks that User2 can modify:

	▼
VNET4 only	
VNET4 and VNET1 only	
VNET4, VNET3, and VNET1 only	
VNET4, VNET3, VNET2, and VNET1	

Virtual networks that User2 can delete:

	▼
VNET4 only	
VNET4 and VNET1 only	
VNET4, VNET3, and VNET1 only	
VNET4, VNET3, VNET2, and VNET1	

Explanation:

Virtual networks that User2 can modify:

Virtual networks that User2 can delete:

Box 1: VNET4 and VNET1 only

RG1 has only Delete lock, while there are no locks on RG4.

RG2 and RG3 both have Read-only locks.

Box 2: VNET4 only

There are no locks on RG4, while the other resource groups have either Delete or Read-only locks.

Note: As an administrator, you may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. You can set the lock level to CanNotDelete or ReadOnly. In the portal, the locks are called Delete and Read-only respectively.

CanNotDelete means authorized users can still read and modify a resource, but they can't delete the resource.

ReadOnly means authorized users can read a resource, but they can't delete or update the resource.

Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

Scenario:

User2 is a Security administrator.

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	RG4	Read-only

References:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources

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 (517 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 182

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

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

In the Azure portal, you plan to create new custom roles by cloning existing roles. The new roles will be configured as shown in the following table.

Name	Type
Role3	Azure AD
Role4	Azure subscription

Which roles can you clone to create each new role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Role3:

Microsoft

Role1 only

Built-in Azure AD roles only

Role1 and built-in Azure AD roles only

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

Role4:

Role2 only

Built-in Azure AD roles only

Role2 and built-in Azure subscription roles only

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

Answer:

Role3:  Microsoft

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

Role4:

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

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/custom-create>

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

NEW QUESTION: 183

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 (AzureAD).

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 the On-premises data gateway to the on-premises network.

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.

References:

<https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network>

NEW QUESTION: 184

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

- A. the Security & Compliance admin center
- B. SQL query editor in Azure
- C. File Explorer in Windows
- D. AzCopy

Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 185

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

2

3

4

Network security rules:

▼

1

2

3

4

Answer:

Microsoft

NSGs:

1

2

3

4

Network security rules:

1

2

3

4

Explanation

Microsoft

NSGs:

1

2

3

4

Network security rules:

1

2

3

4

NSGs: 2
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: 186

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: 187

Which virtual networks in Sub1 can User2 modify and delete in their current state? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

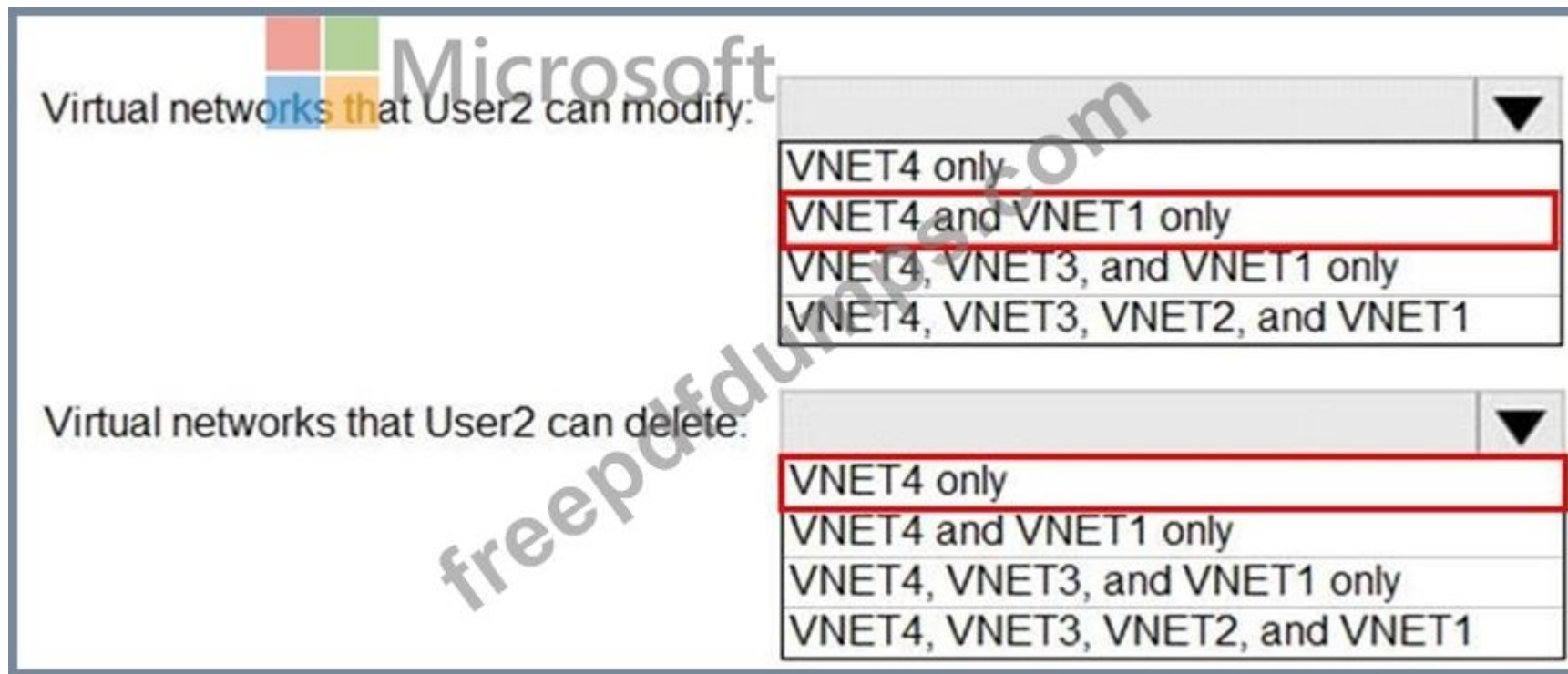
Virtual networks that User2 can modify:

- ☒ VNET4 only
- ☒ VNET4 and VNET1 only
- ☒ VNET4, VNET3, and VNET1 only
- ☒ VNET4, VNET3, VNET2, and VNET1

Virtual networks that User2 can delete:

- ☒ VNET4 only
- ☒ VNET4 and VNET1 only
- ☒ VNET4, VNET3, and VNET1 only
- ☒ VNET4, VNET3, VNET2, and VNET1

Answer:



Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources>

NEW QUESTION: 188

You have an Azure SQL Database server named SQL1.

You turn on Advanced Threat Protection for SQL1 to detect all threat detection types.

Which action will Advanced Threat Protection detect as a threat?

- A. A user updates more than 50 percent of the records in a table.
- B. A user attempts to sign in as SELECT * FROM table1.
- C. A user is added to the db_owner database role.
- D. A user deletes more than 100 records from the same table.

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

Advanced Threat Protection can detect potential SQL injections: This alert is triggered when an active exploit happens against an identified application vulnerability to SQL injection. This means the attacker is trying to inject malicious SQL statements using the vulnerable application code or stored procedures.

References:

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection-overview>

NEW QUESTION: 189

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

VNet1: 

1
2
3
5
10

VNet2: 

1
2
3
6
15

Answer:

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



Microsoft

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 to a new device from the Seattle office on June 7, the user will be prompted for MFA.	☐	☐

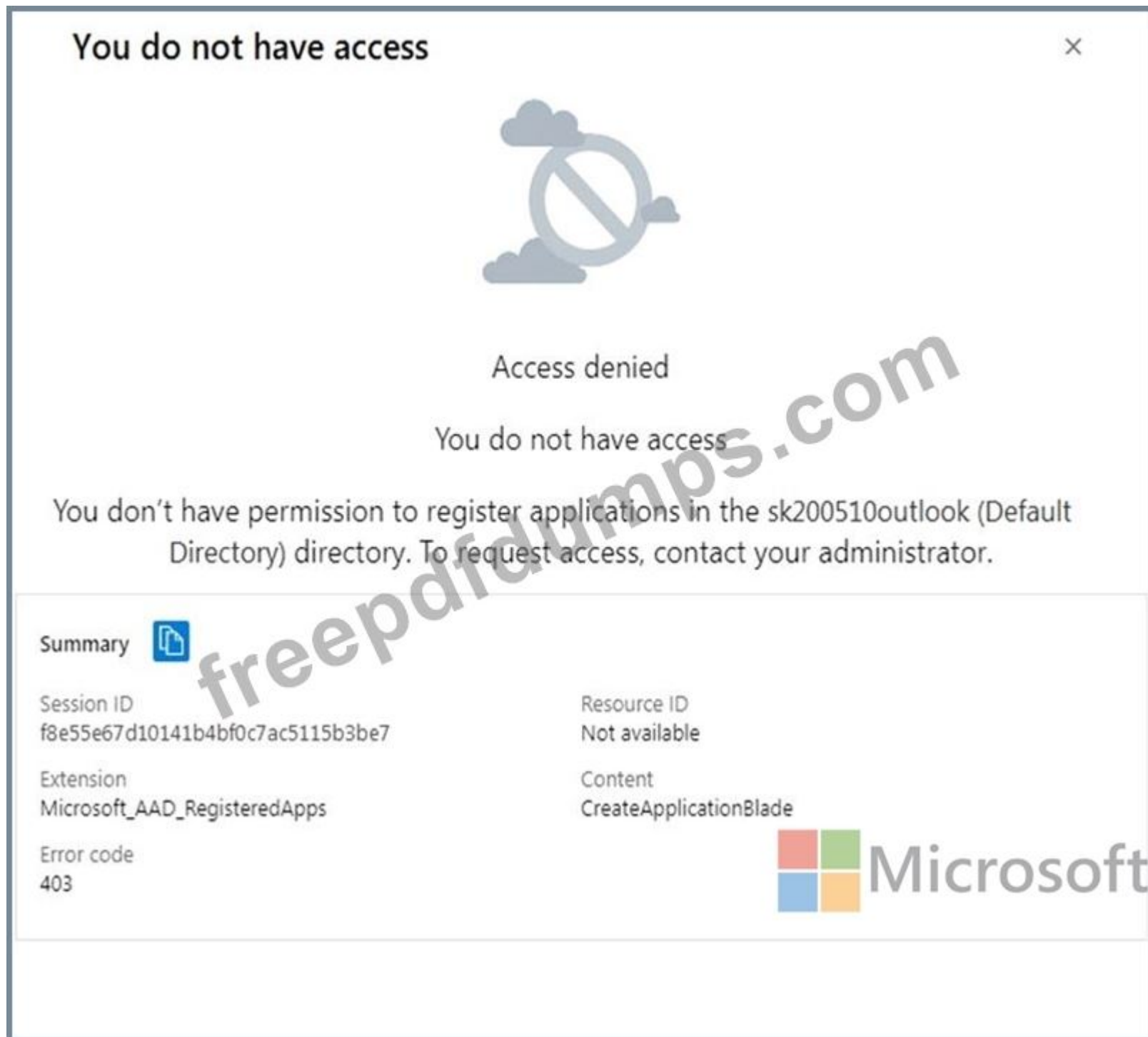
Answer:

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 to a new device from the Seattle office on June 7, the user will be prompted for MFA.	☒	☐

NEW QUESTION: 191

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 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: 192

You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016.

You need to implement a policy to ensure that each virtual machine has a custom antimalware virtual machine extension installed.

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

NOTE: Each correct selection is worth one point.

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

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

Answer:

```

{
  "if" : {
    "allOf" : [
      {
        "field" : "type",
        "equals" : "Microsoft.Compute/virtualMachines"
      },
      {
        "field" : "Microsoft.Compute/imageSKU",
        "equals" : "2016-Datacenter",
      }
    ],
    "then" : {
      "effect" : "
    },
    "details" : {
      "type" : "Microsoft.GuestConfiguration/guestConfigurationAssignments",
      "roleDefinitionsIds" : [
        "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
      ],
      "name" : "customExtension",
      "deployment" : {
        "properties" : {
          "mode": "incremental",
          "parameters" : {
            "
          },
          "
        },
        "
      },
      "
    },
    "
  },
  "
}

```



Reference:

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

NEW QUESTION: 193

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

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: 194

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')]" : "[variable('var1')]",
      "AzureADApplicationID" : "[variable('var1')]",
      "WorkspaceID" : "[variable('var1')]",
      "WorkspaceName" : "[variable('var1')]",
      "WorkspaceURL" : "[variable('var1')]"
    },
    "protectedSettings" : {
      "[variable('var2')]" : "[variable('var2')]",
      "AzureADApplicationSecret" : "[variable('var2')]",
      "StorageAccountKey" : "[variable('var2')]",
      "WorkspaceID" : "[variable('var2')]",
      "WorkspaceKey" : "[variable('var2')]"
    }
  }
}

```



Answer:

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-w>

NEW QUESTION: 195

You have an Azure Active Directory (Azure AD) tenant that contains a user named Admin1. Admin1 is assigned the Application developer role.

You purchase a cloud app named App1 and register App1 in Azure AD.

Admin1 reports that the option to enable token encryption for App1 is unavailable.

You need to ensure that Admin1 can enable token encryption for App1 in the Azure portal.

What should you do?

- A. Upload a certificate for App1.
- B. Modify the API permissions of App1.
- C. Add App1 as an enterprise application.
- D. Assign Admin1 the Cloud application administrator role.

Answer: C (LEAVE A REPLY)

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

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

Reference:

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

NEW QUESTION: 196

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.

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:

Group2 owners:	Microsoft ▼ User2 only User3 only User1 and User2 only User2 and User3 only User1, User2, and User3
App1 users:	▼ Group1 members only Group2 members only Group1 and Group2 members only Group1 and Group2 members and User1 only Group1 and Group2 members, User1, and User3 only

Explanation

No,

Yes,

Yes

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 (517 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 197

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

Reference:

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

NEW QUESTION: 198

You have an Azure subscription that contains a resource group named RG1. RG1 contains a virtual machine named VM1 that uses Azure Active Directory (Azure AD) authentication.

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

The permissions for Role2 are shown in the following JSON code.

```
"permissions": [
  {
    "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	Role1, 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 sign in to VM1 by using Azure AD credentials.	☐	☐

Answer:

Answer Area

Statements	Yes	No
User1 can delete VM1.	☐	☒
User2 can delete VM1.	☒	☐
User3 can sign in to VM1 by using Azure AD credentials.	☒	☐

NEW QUESTION: 199

You need to configure network connectivity between a virtual network named VNET1 and a virtual network named VNET2. The solution must ensure that virtual machines connected to VNET1 can communicate with virtual machines connected to VNET2.

To complete this task, sign in to the Azure portal and modify the Azure resources.

Answer:

See the explanation below.

Explanation

You need to configure VNet Peering between the two networks. The questions states, "The solution must ensure that virtual machines connected to VNET1 can communicate with virtual machines connected to VNET2". It doesn't say the VMs on VNET2 should be able to communicate with VMs on VNET1. Therefore, we need to configure the peering to allow just the one-way communication.

1. In the Azure portal, type Virtual Networks Virtual Networks from the search results then select VNET1. Alternatively, browse to in the left navigation pane.
 2. In the properties of VNET1, click on
 3. In the Peerings blade, click Add
 4. In the Name of the peering from VNET1 to remote virtual network box, enter a name such as VNET1-VNET2 (this is the name that the peering will be displayed as in VNET1)
 5. In the Virtual Network box, select
 6. In the Name of the peering from remote virtual network to VNET1 box, enter a name such as VNET2-VNET1 (this is the name that the peering will be displayed as in VNET2).
- There is an option Allow virtual network access from VNET to remote virtual network. This should be left as Enabled.
7. For the option Allow virtual network access from remote network to VNET1, click the slider button to Disabled.
 8. Click the OK button to save the changes.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering>

NEW QUESTION: 200

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: (SHOW ANSWER)

Explanation

References:

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

NEW QUESTION: 201

You have the Azure resource shown in the following table.

Name	Type	Parent
Management1	Management group	Tenant Root Group
Subscription1	Subscription	Management1
RG1	Resource group	Subscription1
RG2	Resource group	Subscription1
VM1	Virtual machine	RG1
VM2	Virtual machine	RG2

You need to meet the following requirements:

- * Internet-facing virtual machines must be protected by using network security groups (NSGs).
- * All the virtual machines must have disk encryption enabled.

What is the minimum number of security that you should create in Azure Security Center?

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

Answer: D (LEAVE A REPLY)

NEW QUESTION: 202

You implement the planned changes for ASG1 and ASG2.

In which NSGs can you use ASG1. and the network interfaces of which virtual machines can you assign to ASG2?

Answer Area

NSGs:

NSG2 only

NSG2 and NSG4 only

NSG2, NSG3, and NSG4

Virtual machines:

VM3 only

VM2 and VM4 only

VM1, VM2, and VM4 only

VM2, VM3, and VM4 only

VM1, VM2, VM3, and VM4

Answer:

Answer Area

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

Virtual machines:

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

NEW QUESTION: 203

You have an Azure subscription that contains a resource group named RG1 and the identities shown in the following table.

User1	User	Not applicable
Group1	Microsoft 365 group	Yes
Group2	Security group	No
Group3	Security group	Yes
Group4	Security group	Yes

You assign Group4 the Contributor role for RG1.

Which identities can you add to Group4 as members?

- A. User1, Group2, and Group3 only
- B. User1, Group1, Group2, and Group3
- C. User1 and Group3 only
- D. User1, Group1, and Group3 only
- E. User1 only

Answer: (SHOW ANSWER)

NEW QUESTION: 204

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

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

Azure AD Privileged Identity Management (PIM) is enabled for the tenant.

In PIM, the Password Administrator role has the following settings:

- * Maximum activation duration (hours): 2
- * Send email notifying admins of activation: Disable
- * Require incident/request ticket number during activation: Disable
- * Require Azure Multi-Factor Authentication for activation: Enable

* Require approval to activate this role: Enable

* Selected approver: Group1

You assign users the Password Administrator role as shown in the following table.

Name	Assignment type
User1	Active
User2	Eligible
user3	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
When User1 signs in, the user is assigned the Password Administrator role automatically.	☐	☐
User2 can request to activate the Password Administrator role.	☐	☐
If User3 wants to activate the Password Administrator role, the user can approve their own request.	☐	☐

Answer:

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

Explanation

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

Box 1: Yes

Active assignments don't require the member to perform any action to use the role. Members assigned as active have the privileges assigned to the role at all times.

Box 2: No

MFA is disabled for User2 and the setting Require Azure Multi-Factor Authentication for activation is enabled.

Note: Eligible assignments require the member of the role to perform an action to use the role. Actions might include performing a multi-factor authentication (MFA) check, providing a business justification, or requesting approval from designated approvers.

Box 3: Yes

User3 is Group1, which is a Selected Approver Group

Reference:

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

NEW QUESTION: 205

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 the Tenant Root Group management group.

<https://www.fast2test.com/AZ-500-practice-test.html> 74

Valid Fast2test AZ-500 Exam PDF Dumps - New AZ-500 Real Exam Questions

Does this meet the goal?

A. Yes

B. No

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

Explanation/Reference:

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

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

NEW QUESTION: 206

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. Add a user-assigned managed identity to WebApp1.

B. Add an app setting to the WebApp1 configuration.

C. Enable system-assigned managed identity for the WebApp1.

D. Configure the TLS/SSL binding for WebApp1.

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

Reference:

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

NEW QUESTION: 207

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.

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:

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

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.	☐	☐

NEW QUESTION: 208

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

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

User1 is a member of Group1. Group1 and User2 are assigned the Key Vault Contributor role for Vault1.

On January 1, 2019, you create a secret in Vault1. The secret is configured as shown in the exhibit. (Click the Exhibit tab.)

Create a secret

Upload options

Manual

* Name ⓘ

Password1

* Value

• • • • •

Content type (optional)

Set activation date? ☒

Activation Date

2019-03-01 12:00:00 AM

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

Set expiration Date? ⓘ ☒

Expiration Date

2020-03-01 12:00:00 AM

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

Enabled? ☒ Yes ☐ No



User2 is assigned an access policy to Vault1. The policy has the following configurations:

Key Management Operations: Get, List, and Restore

Cryptographic Operations: Decrypt and Unwrap Key

Secret Management Operations: Get, List, and Restore

Group1 is assigned an access to Vault1. The policy has the following configurations:

Key Management Operations: Get and Recover

Secret Management Operations: List, Backup, and Recover

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

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

Answer:

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

NEW QUESTION: 209

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
2
3
4

Network security rules:

1
2
3
4

Answer:

NSGs:

1
2
3
4

Network security rules:

1
2
3
4

Explanation

NSGs: 1

Network security rules: 3

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

References:

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

NEW QUESTION: 210

Which virtual networks in Sub1 can User2 modify and delete in their current state? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Virtual networks that User2 can modify:

 Microsoft ▼

VNET4 only
VNET4 and VNET1 only
VNET4, VNET3, and VNET1 only
VNET4, VNET3, VNET2, and VNET1

Virtual networks that User2 can delete:

▼

VNET4 only
VNET4 and VNET1 only
VNET4, VNET3, and VNET1 only
VNET4, VNET3, VNET2, and VNET1

Answer:

Virtual networks that User2 can modify:

VNET4 only
VNET4 and VNET1 only
VNET4, VNET3, and VNET1 only
VNET4, VNET3, VNET2, and VNET1

Virtual networks that User2 can delete:

VNET4 only
VNET4 and VNET1 only
VNET4, VNET3, and VNET1 only
VNET4, VNET3, VNET2, and VNET1

Explanation

Virtual networks that User2 can modify:

VNET4 only

VNET4 and VNET1 only

VNET4, VNET3, and VNET1 only

VNET4, VNET3, VNET2, and VNET1

Virtual networks that User2 can delete:

VNET4 only

VNET4 and VNET1 only

VNET4, VNET3, and VNET1 only

VNET4, VNET3, VNET2, and VNET1

Box 1: VNET4 and VNET1 only

RG1 has only Delete lock, while there are no locks on RG4.

RG2 and RG3 both have Read-only locks.

Box 2: VNET4 only

There are no locks on RG4, while the other resource groups have either Delete or Read-only locks.

Note: As an administrator, you may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. You can set the lock level to CanNotDelete or ReadOnly. In the portal, the locks are called Delete and Read-only respectively.

* CanNotDelete means authorized users can still read and modify a resource, but they can't delete the resource.

* ReadOnly means authorized users can read a resource, but they can't delete or update the resource.

Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

Scenario:

User2 is a Security administrator.

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.

References:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources>

NEW QUESTION: 211

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant and a user named User1.

The App registrations settings for the tenant are configured as shown in the following exhibit.



You plan to deploy an app named App1.

You need to ensure that User1 can register App1 in Azure AD. The solution must use the principle of least privilege.

Which role should you assign to User1?

- A. App Configuration Data Owner for the subscription
- B. Managed Application Contributor for the subscription
- C. Cloud application administrator in Azure AD
- D. Application developer in Azure AD.

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

Reference:

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

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 (517

Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 212

You are implementing conditional access policies.

You must evaluate the existing Azure Active Directory (Azure AD) risk events and risk levels to configure and implement the policies.

You need to identify the risk level of the following risk events:

Users with leaked credentials

Impossible travel to atypical locations

Sign ins from IP addresses with suspicious activity

Which level should you identify for each risk event? To answer, drag the appropriate levels to the correct risk events. Each level 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.

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

Answer:

Levels Answer Area

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

NEW QUESTION: 213

You have three Azure subscriptions and a user named User1.

You need to provide User1 with the ability to manage and view costs for the resources across all three subscriptions. The solution must use the principle of least privilege.

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.

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Actions

Create a management group.
Add the three subscriptions to the management group.
Assign User1 the Global administrator role.
Assign User1 the Owner role for the management group.
Assign User1 the Cost Management Contributor role for the management group.

Answer:

Answer Area

Assign User1 the Cost Management Reader,,,,,
Assign User1 the Global administrator role.
Add the three subscriptions to the management group.

1 - Assign User1 the Cost Management Reader,,,,,

2 - Assign User1 the Global administrator role.

3 - Add the three subscriptions to the management group.

NEW QUESTION: 214

You have an Azure subscription that contains several Azure SQL databases and an Azure Sentinel workspace.

You need to create a saved query in the workspace to find events reported by Advanced Threat Protection for Azure SQL Database.

What should you do?

- A. From Azure CLI run the Get-AzOperationalInsightsworkspace cmdlet.
- B. From the Azure Sentinel workspace, create a Kusto Query Language query.
- C. From the Azure SQL Database query editor, create a Transact-SQL query.
- D. From Microsoft SQL Server Management Studio (SSMS), create a Transact-SQL query.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 215

You have an Azure Active Directory (Azure AD) tenant named contoso1812.onmicrosoft.com that contains the users shown in the following table.

Name	Username	Type
User1	User1@contoso1812.onmicrosoft.com	Member
User2	User2@contoso1812.onmicrosoft.com	Member
User3	User3@contoso1812.onmicrosoft.com	Member
User4	User4@outlook.com	Guest

You create an Azure Information Protection label named Label1. The Protection settings for Label1 are configured as shown in the exhibit. (Click the Exhibit tab.)

Protection

Contoso1812 - Azure Information Protection

Protections settings ⓘ

Azure (cloud key) HYOK (AD RMS)

Select the protection action type ⓘ

- ☒ Set permissions
- ☐ Set user-defined permissions (Preview)

USERS	PERMISSIONS
AuthenticatedUsers	Viewer
User1@contoso1812.onmicrosoft.com	Co-Author
User2@contoso1812.onmicrosoft.com	Reviewer

[+Add permissions](#)



Label1 is applied to a file named File1.

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 print File1.

☐☐

User3 can read File1.

☐☐

User4 can print File1.

☐☐

Answer:

Statements

Yes

No

User1 can print File1.

☒☐

User3 can read File1.

☒☐

User4 can print File1.

☐☒

Explanation:

Statements	Yes	No
User1 can print File1.	☒	☐
User3 can read File1.	☐	☐
User4 can print File1.	☐	☒

NEW QUESTION: 216

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. an app registration
- B. a custom role-based access control (RBAQ role
- C. an Azure AD Application Proxy
- D. an external identity

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

NEW QUESTION: 217

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

Name	Type	Attached to	NSG
NSG1	Network security group (NSG)	VM5	<i>Not applicable</i>
NSG2	Network security group (NSG)	Subnet1	<i>Not applicable</i>
Subnet1	Subnet	<i>Not applicable</i>	<i>Not applicable</i>
VM5	Virtual machine	Subnet1	NSG1

An IP address of 10.1.0.4 is assigned to VM5. VM5 does not have a public IP address.

VM5 has just in time (JIT) VM access configured as shown in the following exhibit.

JIT VM access configuration

VM5

+ Add

Save

Discard

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

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

You enable JIT VM access for VM5.

NSG1 has the inbound rules shown in the following exhibit.

Priority	Name	Port	Protocol	Source	Destination	Action
00	SecurityCenter-JITRule-...	3389	Any	Any	10.1.0.4	Allow
000	SecurityCenter-JITRule_341...	3389	Any	Any	10.1.0.4	Deny
001	RDP	3389	TCP	Any	Any	Allow
15000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
15001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	Allow
15500	DenyAllInBound	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
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	☐	☐
Remote Desktop access to VM5 is blocked.	☐	☐
An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.	☐	☐

Answer:

Statements	Yes	No
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	☒	☐
Remote Desktop access to VM5 is blocked.	☒	☐
An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.	☐	☒

NEW QUESTION: 218

DRAG DROP

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 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.

Select and Place:

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



NEW QUESTION: 219

You have an Azure subscription.

You plan to create a workflow automation in Azure Security Center that will automatically remediate a security vulnerability.

What should you create first?

- A. a managed identity
- B. an automation account
- C. an Azure function app
- D. an alert rule
- E. an Azure logic app

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

Reference:

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

NEW QUESTION: 220

You create a new Azure subscription.

You need to ensure that you can create custom alert rules in Azure Security Center.

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

NOTE: Each correct selection is worth one point.

- A. Onboard Azure Active Directory (Azure AD) Identity Protection.
- B. Create an Azure Storage account.
- C. Implement Azure Advisor recommendations.
- D. Create an Azure Log Analytics workspace.
- E. Upgrade the pricing tier of Security Center to Standard.

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

Section: [none]

Explanation:

D: You need write permission in the workspace that you select to store your custom alert.

References:

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

NEW QUESTION: 221

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

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

Azure AD Privileged Identity Management (PIM) is enabled for the tenant.

In PIM, the Password Administrator role has the following settings:

- * Maximum activation duration (hours): 2
- * Send email notifying admins of activation: Disable
- * Require incident/request ticket number during activation: Disable
- * Require Azure Multi-Factor Authentication for activation: Enable
- * Require approval to activate this role: Enable
- * Selected approver: Group1

You assign users the Password Administrator role as shown in the following table.

Name	Assignment type
User1	Active
User2	Eligible
user3	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
When User1 signs in, the user is assigned the Password Administrator role automatically.	☐	☐
User2 can request to activate the Password Administrator role.	☐	☐
If User3 wants to activate the Password Administrator role, the user can approve their own request.	☐	☐

Answer:

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

Explanation

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

Box 1: Yes

Active assignments don't require the member to perform any action to use the role. Members assigned as active have the privileges assigned to the role at all times.

Box 2: No

MFA is disabled for User2 and the setting Require Azure Multi-Factor Authentication for activation is enabled.

Note: Eligible assignments require the member of the role to perform an action to use the role. Actions might include performing a multi-factor authentication (MFA) check, providing a business justification, or requesting approval from designated approvers.

Box 3: Yes

User3 is Group1, which is a Selected Approver Group

Reference:

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

NEW QUESTION: 222

You are evaluating the security of VM1, VM2, and VM3 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



Microsoft

Statements

Yes

No

From the Internet, you can connect to the web server on VM1 by using HTTP.

☐☐

From the Internet, you can connect to the web server on VM2 by using HTTP.

☐☐

From the Internet, you can connect to the web server on VM3 by using HTTP.

☐☐

Answer:

Statements

Yes

No

Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.

☐☒

Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription.

☐☒

Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.

☐☒

Explanation

Yes

No

From the Internet, you can connect to the web server on VM1 by using HTTP.

☒☐

From the Internet, you can connect to the web server on VM2 by using HTTP.

☐☒

From the Internet, you can connect to the web server on VM3 by using HTTP.

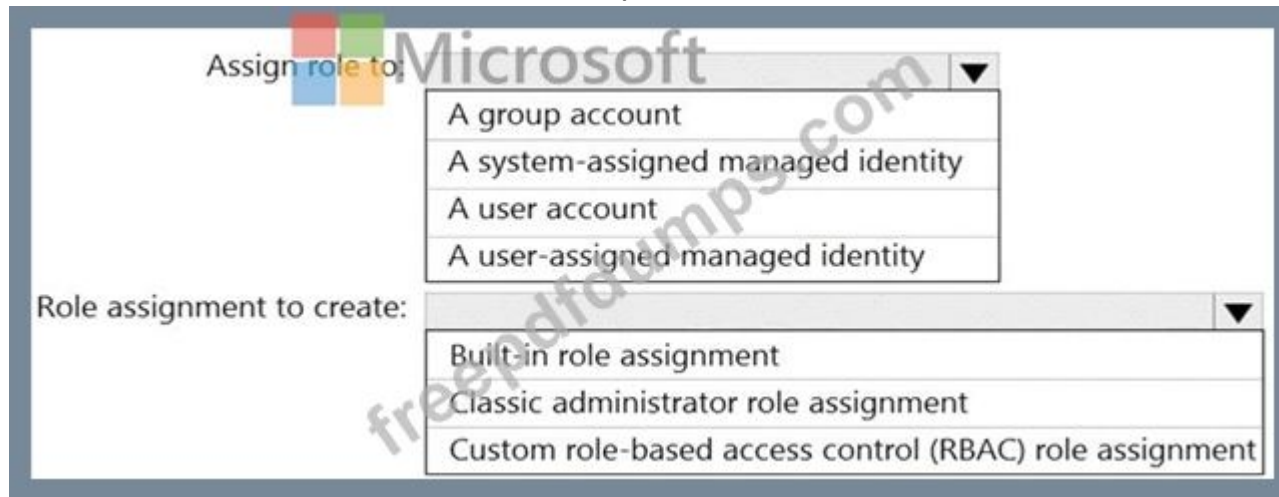
☒☐

NEW QUESTION: 223

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.



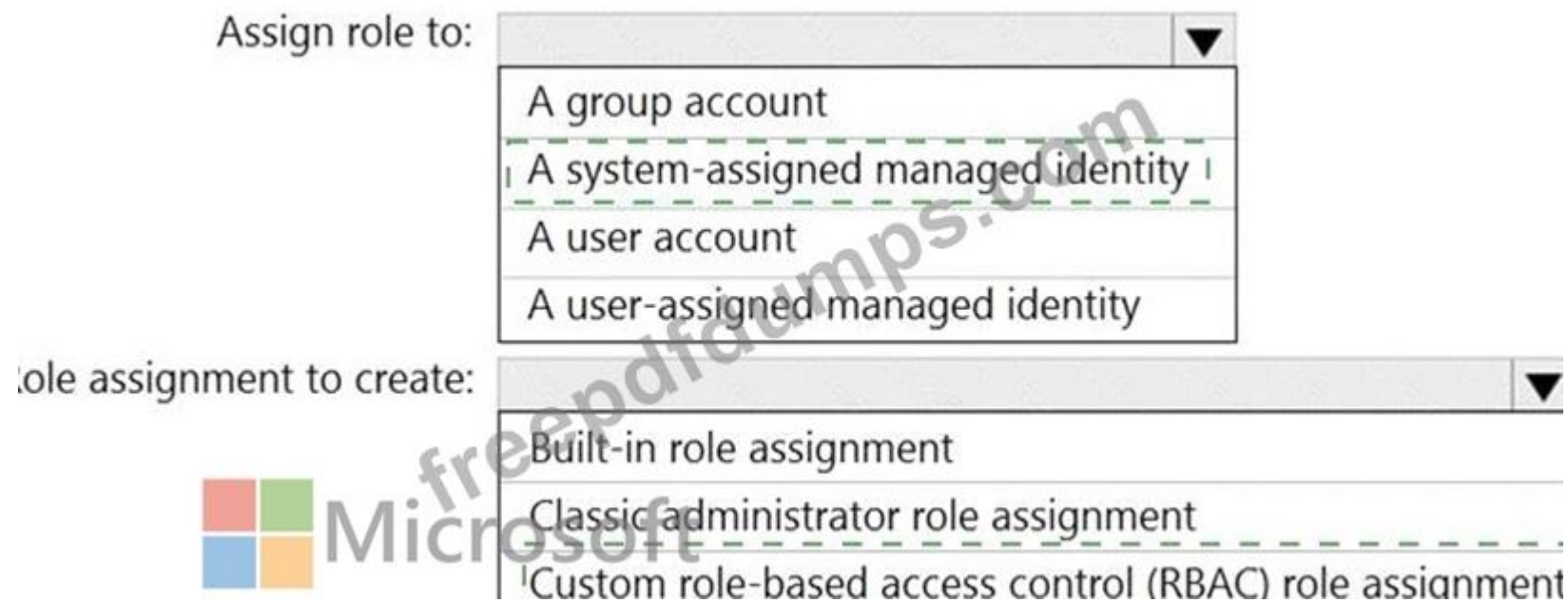
Assign role to:

- 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:

ole assignment to create:

Microsoft

freepdfmups.com

A group account

A system-assigned managed identity

A user account

A user-assigned managed identity

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>

NEW QUESTION: 224

You have a Azure subscription.

You enable Azure Active Directory (Azure AD) Privileged identify (PIM).

Your company's security policy for administrator accounts has the following conditions:

- * The accounts must use multi-factor authentication (MFA).
- * The account must use 20-character complex passwords.
- * The passwords must be changed every 180 days.
- * The account must be managed by using PIM.

You receive alerts about administrator who have not changed their password during the last 90 days.

You need to minimize the number of generated alerts.

Which PIM alert should you modify?

- A. Roles don't require multi-factor authentication for activation.
- B. Administrator aren't using their privileged roles
- C. Roles are being assigned outside of Privileged identity Management
- D. Potential stale accounts in a privileged role.

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

Reference:

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

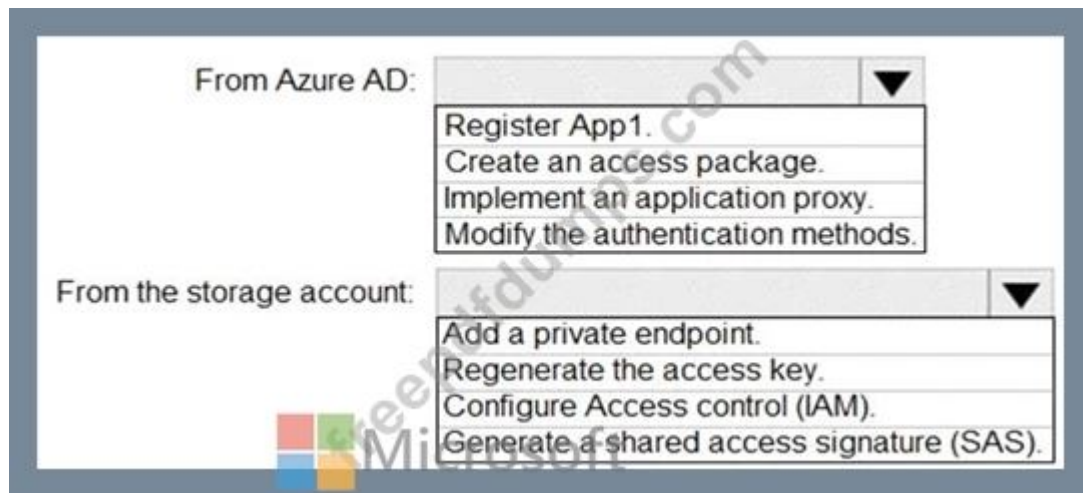
NEW QUESTION: 225

You have an Azure Storage account that contains a blob container named container1 and a client application named App1.

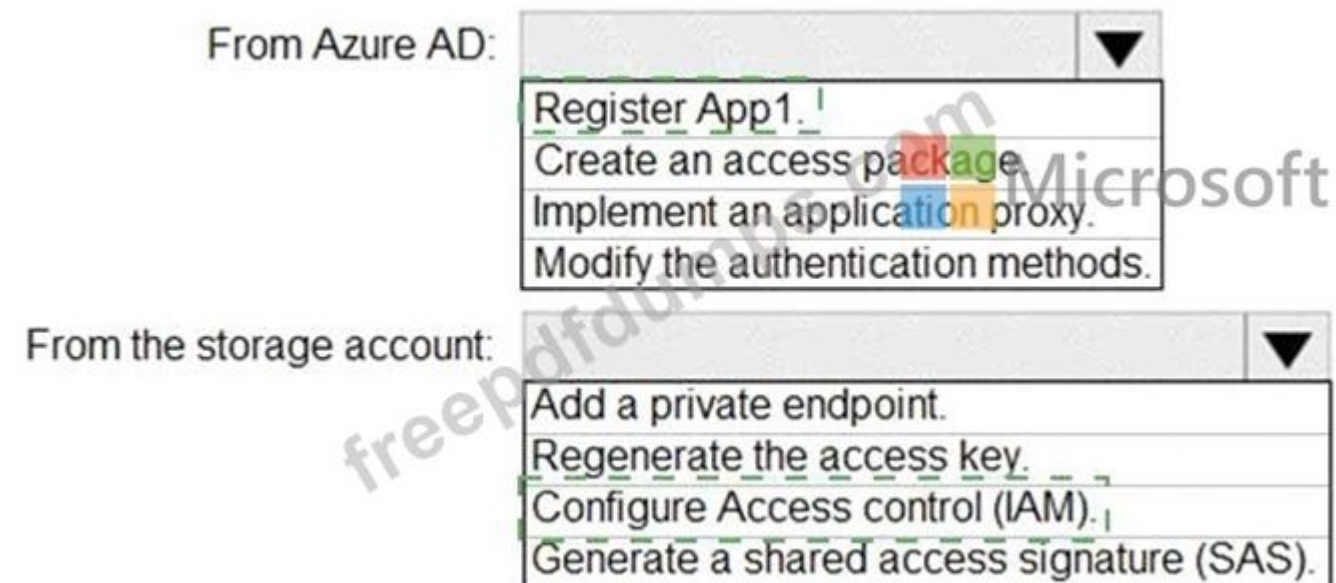
You need to enable App1 access to container1 by using Azure Active Directory (Azure AD) authentication.

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

NOTE: Each correct selection is worth one point.



Answer:



Explanation:



Reference:

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

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/storage/common/storage-auth-aad-rbac-portal.>

NEW QUESTION: 226

You need to ensure that the Azure AD application registration and consent configurations meet the identity and access requirements.

What should you use in the Azure portal? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

To configure the registration settings:

	▼
Azure AD – User settings	
Azure AD – App registrations settings	
Enterprise Applications – User settings	

To configure the consent settings:

	▼
Azure AD – User settings	
Azure AD – App registrations settings	
Enterprise Applications – User settings	

Answer:

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

Explanation

To configure the registration settings:

	▼
Azure AD – User settings	
Azure AD – App registrations settings	
Enterprise Applications – User settings	

To configure the consent settings:

	▼
Azure AD – User settings	
Azure AD – App registrations settings	
Enterprise Applications – User settings	

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent>

Topic 2, ContosoPlease wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall

test time.

When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.

Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all Please note that once you submit your work by clicking the Next button within a lab.

Task 1:

You need to configure Azure to allow RDP connections from the Internet to a virtual machine named VM1.

The solution must minimize the attack surface of VM1.

To complete this task, sign in to the Azure portal.

Task 2:

You need to add the network interface of a virtual machine named VM1 to an application security group named ASG1.

To complete this task, sign in to the Azure portal.

Task 3:

You need to perform a full malware scan every Sunday at 02:00 on a virtual machine named VM1 by using Microsoft Antimalware for Virtual Machines.

Task 4:

The developers at your company plan to create a web app named App10317806 and to publish the app to <https://www.contoso.com>.

You need to perform the following tasks:

- * Ensure that App10317806 is registered to Azure Active Directory (Azure AD).

- * Generate a password for App10317806.

Task 5:

You need to prevent administrative users from accidentally deleting a virtual network named VNET1. The administrative users must be allowed to modify the settings of VNET1.

Task 6:

You need to ensure that a user named user210317806 can manage the properties of the virtual machines in the RG1lod10317806 resource group. The solution must use the principle of least privilege.

Task 7:

You need to ensure that only devices connected to a 131.107.0.0/16 subnet can access data in the railod10317806 Azure Storage account, Task 8:

You need to email an alert to a user named admin1@contoso.com if the average CPU usage of a virtual machine named VM1 is greater than 70 percent for a period of 15 minutes.

Task 9:

You need to collect all the audit failure data from the security log of a virtual machine named VM1 to an Azure Storage account.

To complete this task, sign in to the Azure portal.

This task might take several minutes to complete. You can perform other tasks while the task completes.

Task 10:

You need to prevent HTTP connections to the rg1lod10317806n1 Azure Storage account.

Task 11:

You need to ensure that the rg1lod10317806n1 Azure Storage account is encrypted by using a key stored in the KeyVault10317806 Azure key vault.

Task 12:

You need to create a new Azure Active Directory (Azure AD) directory named 10317806.onmicrosoft.com.

The new directory must contain a user named user10317806.onmicrosoft.com who is configured to sign in by using Azure Multi-Factor Authentication (MFA).

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	Section	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	networkSecurityGroups	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.

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 (517 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 227

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

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

You create an Azure role by using the following JSON file.

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

You assign Role1 to User1 for 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.

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

Answer:

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

Reference:

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

NEW QUESTION: 228

You suspect that users are attempting to sign in to resources to which they have no access.

You need to create an Azure Log Analytics query to identify failed user sign-in attempts from the last three days. The results must only show users who had more than five failed sign-in attempts.

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

NOTE: Each correct selection is worth one point.

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

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

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

Answer:

```

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

```

	▼
ActivityID	
DataType	
EventID	
QuantityUnit	

==4625

```

Summarize failed_login_attempts=

```

	▼
Count(),	
Countif(),	
Makeset(),	
Split(),	

```

latest_failed_login=arg_max(TimeGenerated by Account
where failed_login_attempts > 5

```

Explanation

```

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

```

	▼
ActivityID	
DataType	
EventID	
QuantityUnit	

==4625

```

| Summarize failed_login_attempts=

```

	▼
Count(),	
Countif(),	
Makeset(),	
Split(),	

```

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

```

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

```

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

```

References:

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

NEW QUESTION: 229

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

Answer:

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

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

2 - Select the query result.

3 - Add a bookmark and map an entity.

Reference:

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

NEW QUESTION: 230

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

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

Which users can enable Azure AD Privileged Identity Management (PIM)?

- A. User2 and User3 only
- B. User1 and User2 only
- C. User2 only
- D. User1 only

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

Reference:

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

NEW QUESTION: 231

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

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

You plan to deploy the virtual machines shown in the following table.

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

You need to assign managed identities to the virtual machines. The solution must meet the following requirements:

Assign each virtual machine the required roles.

Use the principle of least privilege.

What is the minimum number of managed identities required?

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

Answer: ([SHOW ANSWER](#))

Explanation

We have two different sets of required permissions. VM1 and VM2 have the same permission requirements.

VM3 and VM4 have the same permission requirements.

A user-assigned managed identity can be assigned to one or many resources. By using user-assigned managed identities, we can create just two managed identities: one with the permission requirements for VM1 and VM2 and the other with the permission requirements for VM3 and VM4.

Reference:

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

NEW QUESTION: 232

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.

The screenshot shows the configuration page for an application named 'App1' in the Microsoft My Apps portal. The page has a top bar with 'Save', 'Discard', 'Delete', and 'Got feedback' buttons. The configuration fields are as follows:

- Enabled for users to sign-in?**: Radio buttons for 'Yes' (selected) and 'No'.
- Name**: Text input field containing 'App1'.
- Homepage URL**: Empty text input field.
- Logo**: A blue square logo with the letters 'AP' in white. Below it is a 'Select a file' button with a folder icon.
- Application ID**: Text input field containing '75082794-3617-4347-ac6d-88cfd564072'.
- Object ID**: Text input field containing '4926ab6c-ef57-4c9f-a028-f6d635cde655'.
- User assignment required?**: Radio buttons for 'Yes' and 'No' (selected).
- Visible to users**: Radio buttons for 'Yes' (selected) and 'No'.
- Notes**: A large empty text area.

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: 233

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

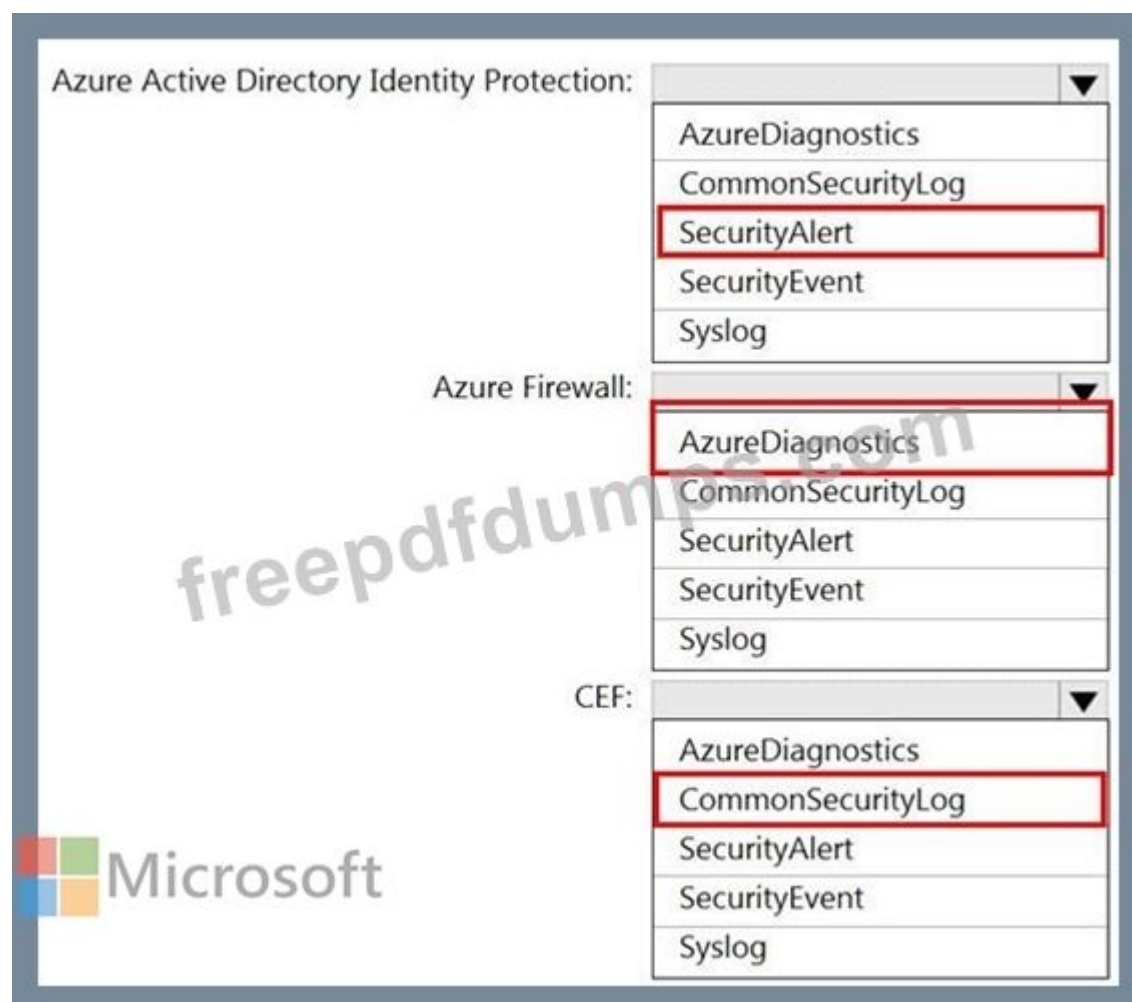
Azure Firewall: ▼

AzureDiagnostics
CommonSecurityLog
SecurityAlert
SecurityEvent
Syslog

CEF: ▼

AzureDiagnostics
CommonSecurityLog
SecurityAlert
SecurityEvent
Syslog

Answer:



NEW QUESTION: 234

You have an Azure subscription that has a managed identity named identity and is linked to an Azure Active Directory (Azure AD) tenant. The tenant contains the resources shown in the following table.

Which resources can be added to AU1 and AU2? To answer, select the appropriate options in the answer area.

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

Which resources can be added to AU1 and AU2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:



NEW QUESTION: 235

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](#))

Explanation

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, ContosoPlease wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.

Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all Please note that once you submit your work by clicking the Next button within a lab.

Task 1:

You need to configure Azure to allow RDP connections from the Internet to a virtual machine named VM1.

The solution must minimize the attack surface of VM1.

To complete this task, sign in to the Azure portal.

Task 2:

You need to add the network interface of a virtual machine named VM1 to an application security group named ASG1.

To complete this task, sign in to the Azure portal.

Task 3:

You need to perform a full malware scan every Sunday at 02:00 on a virtual machine named VM1 by using Microsoft Antimalware for Virtual Machines.

Task 4:

The developers at your company plan to create a web app named App10317806 and to publish the app to <https://www.contoso.com>.

You need to perform the following tasks:

- * Ensure that App10317806 is registered to Azure Active Directory (Azure AD).

- * Generate a password for App10317806.

Task 5:

You need to prevent administrative users from accidentally deleting a virtual network named VNET1. The administrative users must be allowed to modify the settings of VNET1.

Task 6:

You need to ensure that a user named user210317806 can manage the properties of the virtual machines in the RG1lod10317806 resource group. The solution must use the principle of least privilege.

Task 7:

You need to ensure that only devices connected to a 131.107.0.0/16 subnet can access data in the railod10317806 Azure Storage account, Task 8:

You need to email an alert to a user named admin1@contoso.com if the average CPU usage of a virtual machine named VM1 is greater than 70 percent for a period of 15 minutes.

Task 9:

You need to collect all the audit failure data from the security log of a virtual machine named VM1 to an Azure Storage account.

To complete this task, sign in to the Azure portal.

This task might take several minutes to complete. You can perform other tasks while the task completes.

Task 10:

You need to prevent HTTP connections to the rg1lod10317806n1 Azure Storage account.

Task 11:

You need to ensure that the rg1lod10317806n1 Azure Storage account is encrypted by using a key stored in the KeyVault10317806 Azure key vault.

Task 12:

You need to create a new Azure Active Directory (Azure AD) directory named 10317806.onmicrosoft.com.

The new directory must contain a user named user10317806.onmicrosoft.com who is configured to sign in by using Azure Multi-Factor Authentication (MFA).

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	networkSecurityGroups	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: 236

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 Virtual Network Manager
- B. Azure Front Door
- C. Azure Network Function Manager
- D. Azure Firewall Manager

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 237

SIMULATION

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.

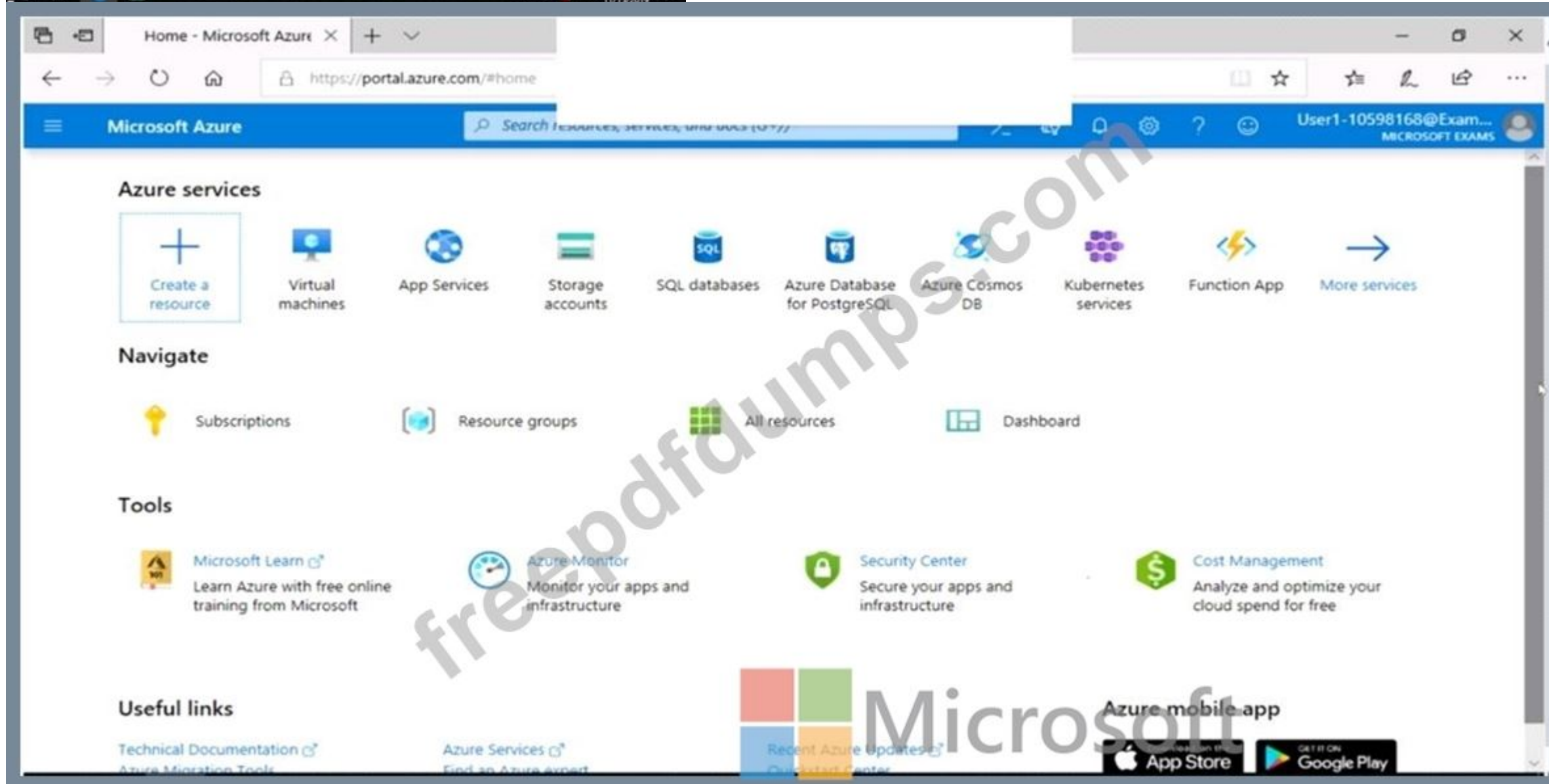
To enter your password, place your cursor in the Enter password box and click on the password below.

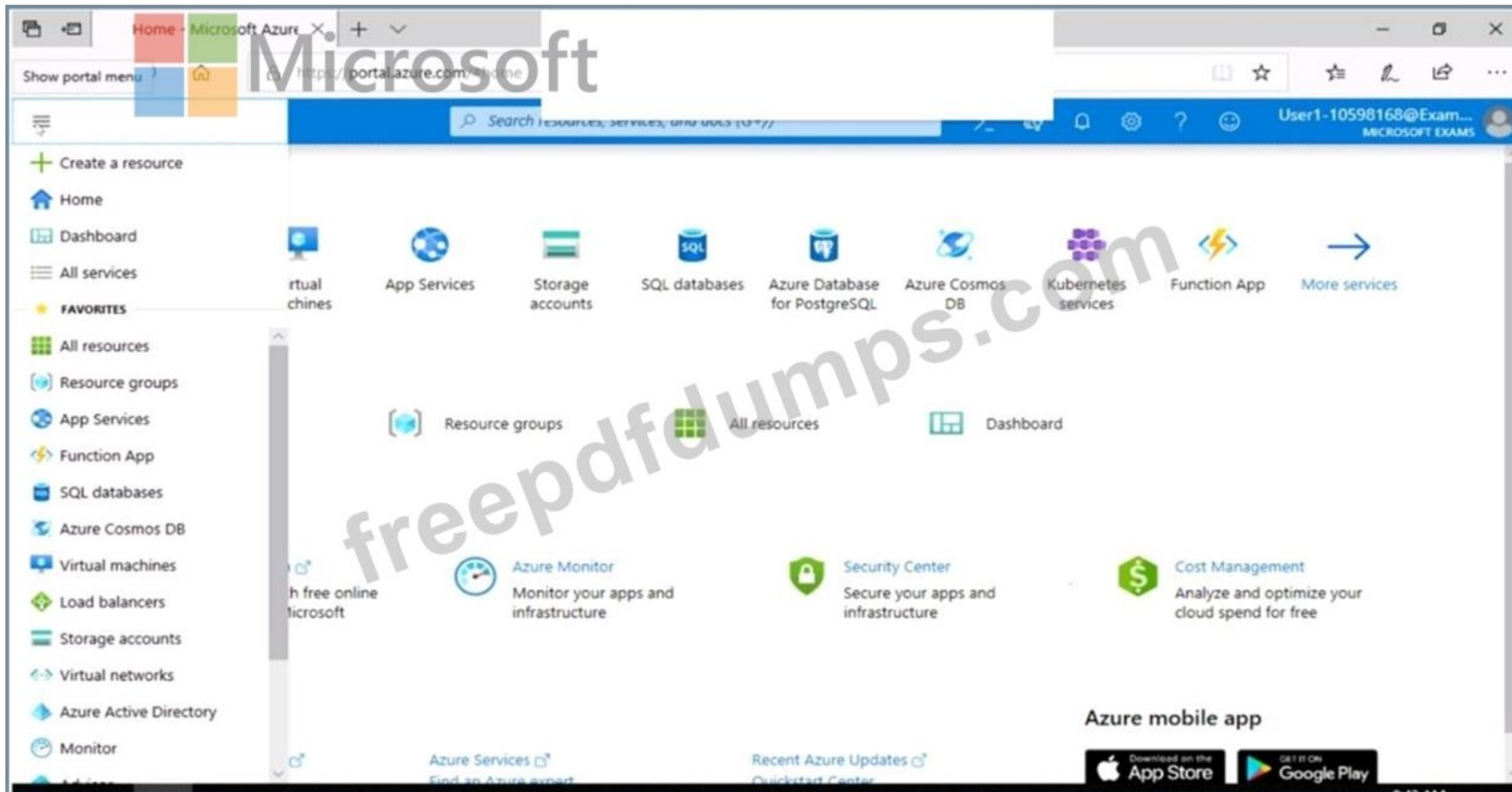
Azure Username: User1-10598168@ExamUsers.com

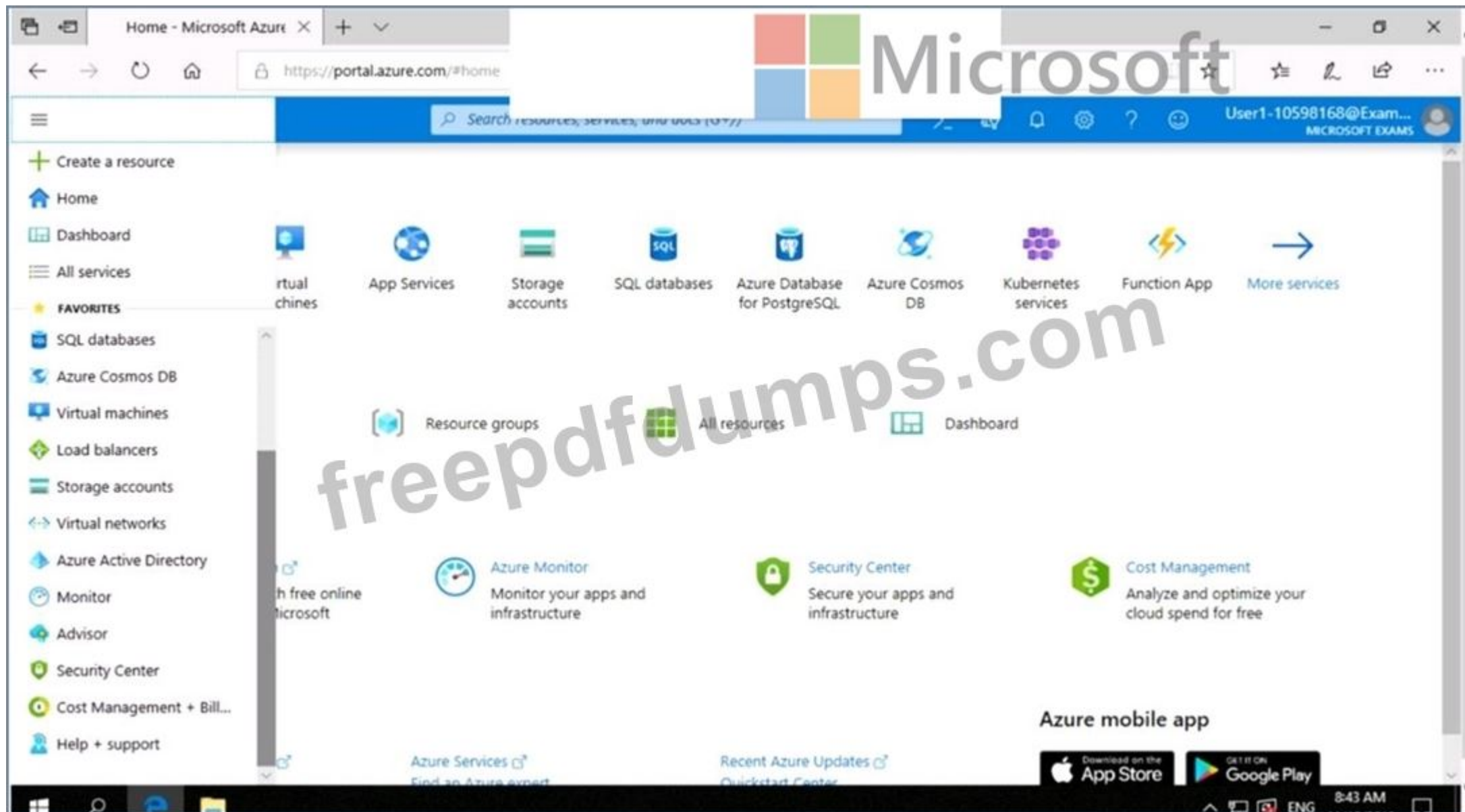
Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168







You need to add the network interface of a virtual machine named VM1 to an application security group named ASG1.

To complete this task, sign in to the Azure portal.

A. *In the Search resources, services, and docs box at the top of the portal, begin typing the name of a virtual machine, VM1 that has a network interface that you want to add to, or remove from, an application security group.

* When the name of your VM appears in the search results, select it.

* Under SETTINGS, select Networking.

B. *In the Search resources, services, and docs box at the top of the portal, begin typing the name of a virtual machine, VM1 that has a network interface that you want to add to, or remove from, an application security group.

* When the name of your VM appears in the search results, select it.

* Under SETTINGS, select Networking. Select Configure the application security groups, select the application security groups that you want to add the network interface to, or unselect the application security groups that you want to remove the network interface from, and then select Save.

Answer: B (LEAVE A REPLY)

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface>

NEW QUESTION: 238

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 Defender for Cloud

B. Azure Active Directory (Azure AD) Identity Protection

C. Microsoft Defender for Identity

D. Microsoft Sentinel

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

NEW QUESTION: 239

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

You need to use 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 Active Directory (Azure AD) user

D. an Azure Active Directory (Azure AD) group

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

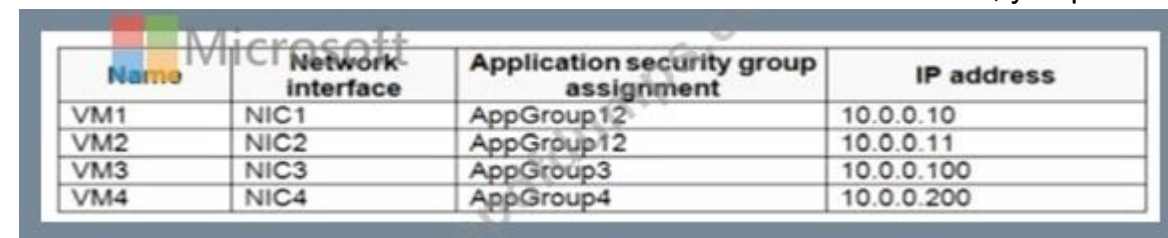
Reference:

<https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal>

NEW QUESTION: 240

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

2

3

4

Network security rules:

▼

1

2

3

4

 Microsoft

Answer:

NSGs:

▼

1

2

3

4

Network security rules:

▼

1

2

3

4

 Microsoft

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

NEW QUESTION: 241

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

Microsoft

ASG1:

ASG2:

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

Answer Area

Microsoft

ASG1:

VM2, VM3, and VM4 only

ASG2:

VM1, VM2, and VM4 only

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 (517 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 242

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 ContososKey1.
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.

Delegate permissions for ContosoKey1:

Configure network access to ContosoKey1:

Answer:

Delegate permissions for ContosoKey1:

Configure network access to ContosoKey1:

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

NEW QUESTION: 243

You 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.	☒	☐

NEW QUESTION: 244

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.

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

References:

<https://docs.microsoft.com/en-us/azure/automation/automation-update-management>

NEW QUESTION: 245

You plan to use Azure Sentinel to create an analytic rule that will detect suspicious threats and automate responses.

Which components are required for the rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Detect suspicious threats:

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

Automate responses:

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

Answer:

Detect suspicious threats:

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

Automate responses:

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

Reference:

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

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

NEW QUESTION: 246

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": [],
    "notDataActions": []
  }
]
}

```

The permissions are assigned to the following role definition:

```

"permissions": [
  {
    "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.

Answer Area

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

Answer:

Answer Area

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

NEW QUESTION: 247

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.	☒	☐

NEW QUESTION: 248

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.

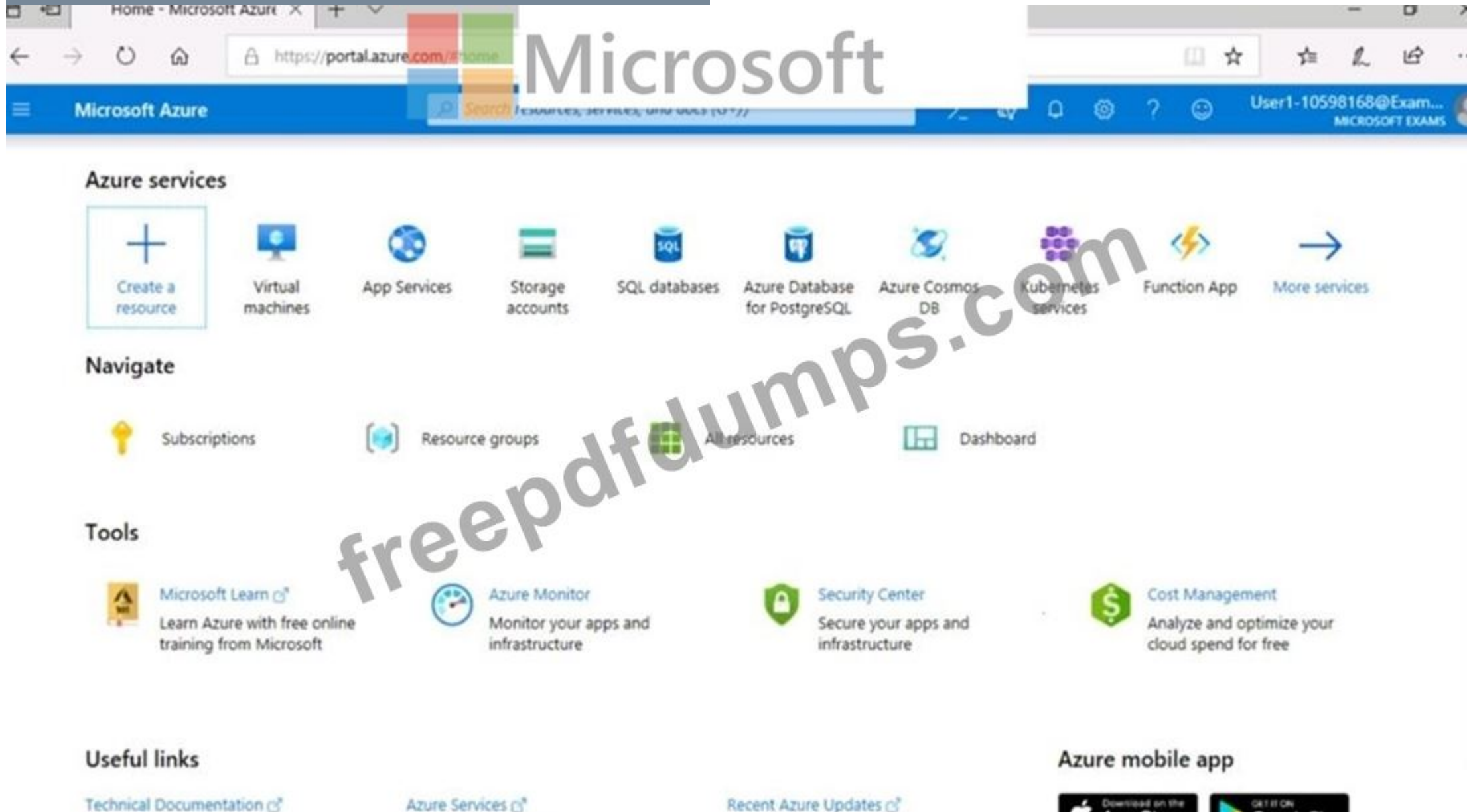
To enter your password, place your cursor in the Enter password box and click on the password below.

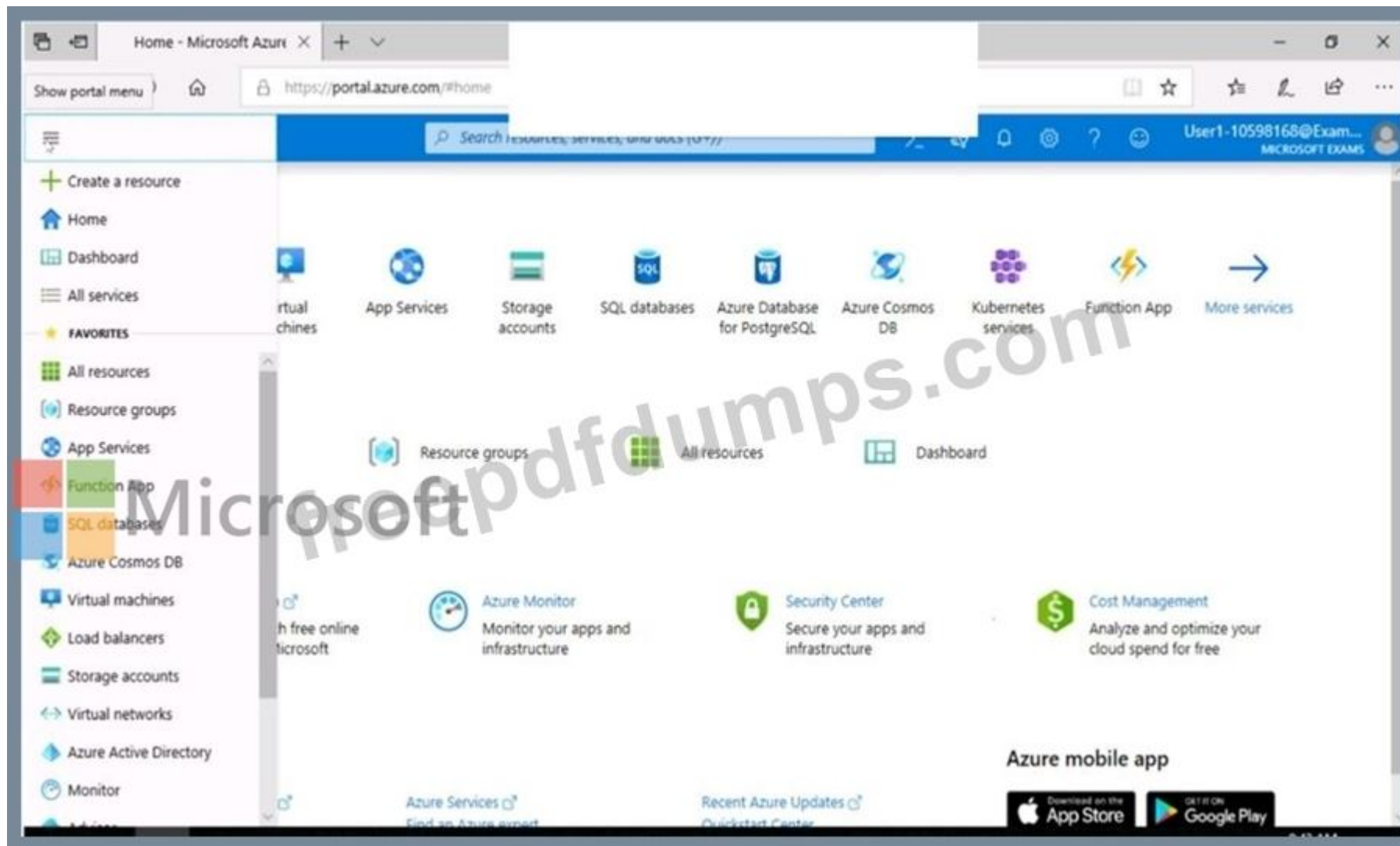
Azure Username: User1-10598168@ExamUsers.com

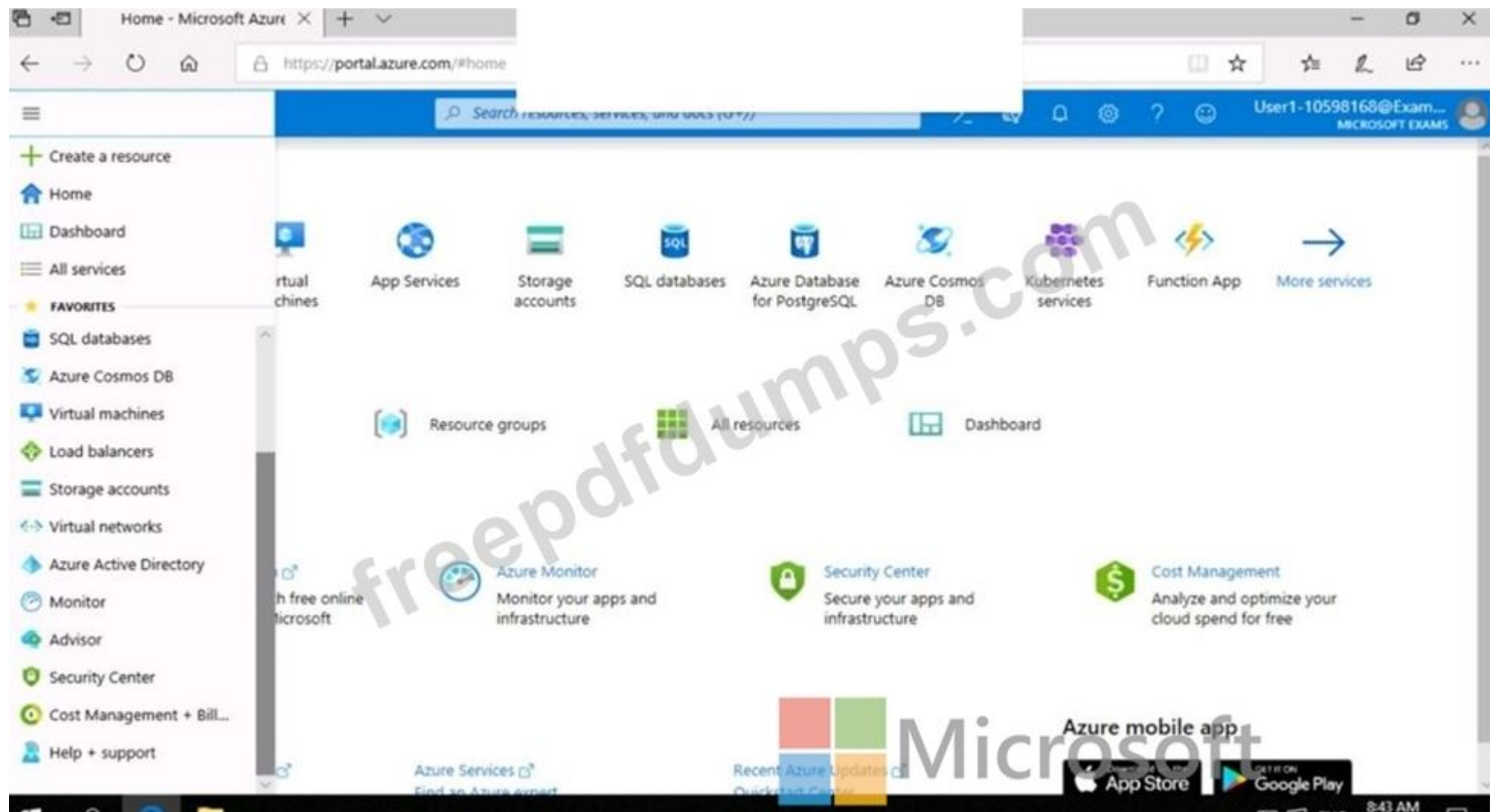
Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168







You need to email an alert to a user named admin1@contoso.com if the average CPU usage of a virtual machine named VM1 is greater than 70 percent for a period of 15 minutes. To complete this task, sign in to the Azure portal.

Answer:

See the explanation below.

Explanation

Create an alert rule on a metric with the Azure portal

1. In the portal, locate the resource, here VM1, you are interested in monitoring and select it.
2. Select Alerts (Classic) under the MONITORING section. The text and icon may vary slightly for different resources.
3. Select the Add metric alert (classic) button and fill in the fields as per below, and click OK.

Metric: CPU Percentage

Condition: Greater than

Period: Over last 15 minutes

Notify via: email

Additional administrator email(s): admin1@contoso.com

Condition  Microsoft

Greater than

* Threshold

60

Period

Over the last 5 minutes

Notify via

Email owners, contributors, and readers

☒

Additional administrator email(s)

admin@contoso.com

Webhook

http://www.contoso.com/dowork?param

Reference:

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-insights-alerts-portal>

NEW QUESTION: 249

You have an Azure subscription that has a managed identity named identity and is linked to an Azure Active Directory (Azure AD) tenant. The tenant contains the resources shown in the following table.

Which resources can be added to AU1 and AU2? To answer, select the appropriate options in the answer area.

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

Which resources can be added to AU1 and AU2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

AU1:

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

AU2:

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

Answer:

Answer Area

creepdfdumps.com

AU1:

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

AU2:

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

Microsoft

NEW QUESTION: 250

You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016.

You need to implement a policy to ensure that each virtual machine has a custom antimalware virtual machine extension installed.

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

NOTE: Each correct selection is worth one point.



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

```

Answer:


```

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

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

```

Reference:

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

NEW QUESTION: 251

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

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

You create the Azure Storage accounts shown in the following table.

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

You need to configure auditing for SQL1.

Which storage accounts and Log Analytics workspaces can you use as the audit log destination? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



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

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

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

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

Answer:

Actions

Create a new workspace.

Apply the scope configuration to the solution.

Create a scope configuration.

Create a computer group.

Create a data source.

Answer Area

Create a computer group.

Create a scope configuration.

Apply the scope configuration to the solution.

Explanation

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

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

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

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

NEW QUESTION: 252

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:

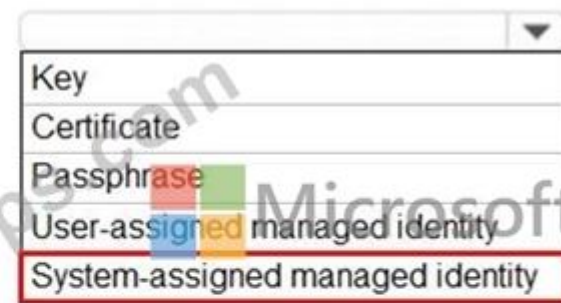
Key
Certificate
Passphrase
User-assigned managed identity
System-assigned managed identity

Configure a Key Vault reference for App1 from the:

Extensions blade
General settings tab
TLS/SSL settings blade
Application settings tab

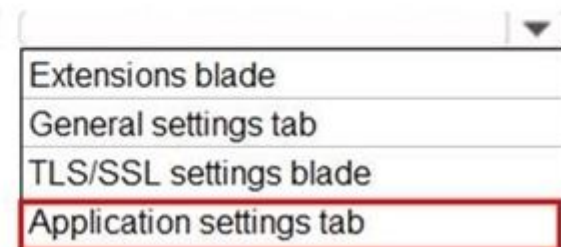
Answer:

Configure App1 to authenticate by using a:



A dropdown menu showing authentication options. The options are: Key, Certificate, Passphrase, User-assigned managed identity, and System-assigned managed identity. The 'System-assigned managed identity' option is highlighted with a red border.

Configure a Key Vault reference for App1 from the:



A dropdown menu showing Key Vault reference options. The options are: Extensions blade, General settings tab, TLS/SSL settings blade, and Application settings tab. The 'Application settings tab' option is highlighted with a red border.

Reference:

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

NEW QUESTION: 253

You have an Azure Active Directory (Azure AD) tenant that contains two users named User1 and User2 and a registered app named App1.

You create an app-specific role named Role1.

You need to assign Role1 to User1 and enable User2 to request access to App1.

Which two settings should you modify? To answer select the appropriate settings in the answer area NOTE: Each correct selection is worth one point.



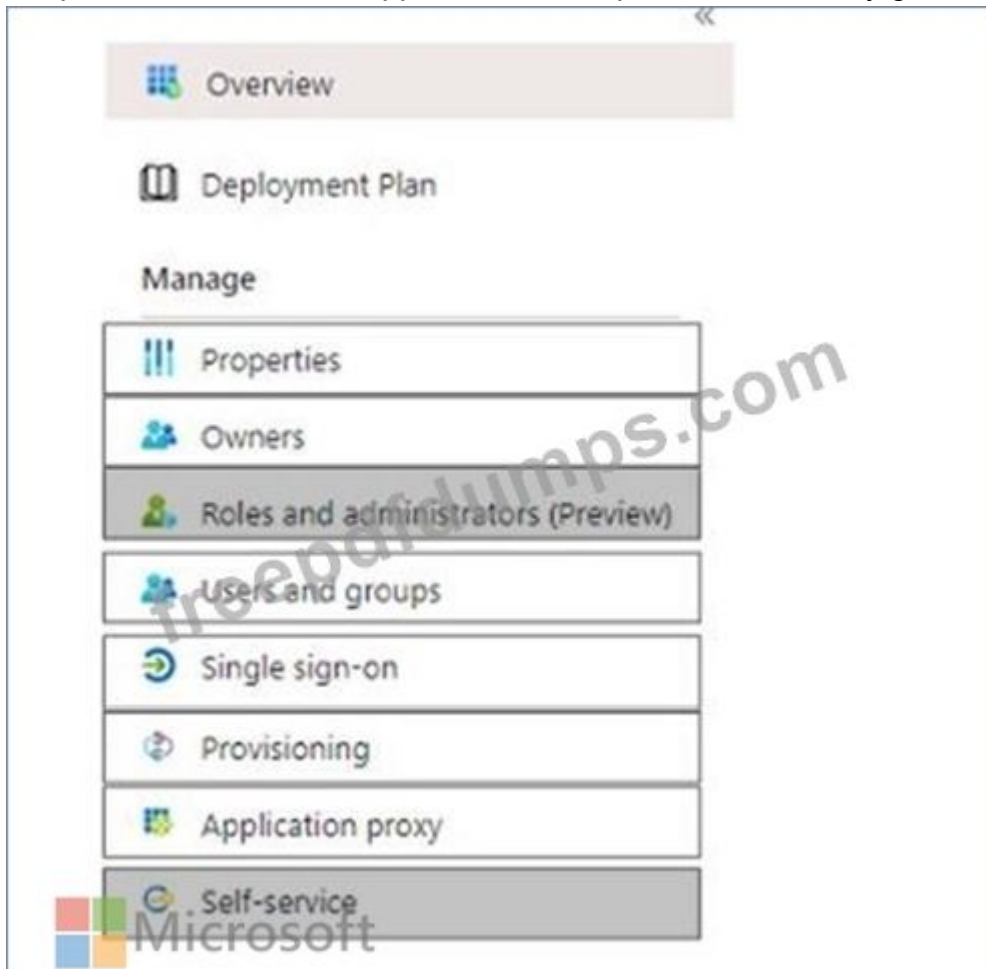
A screenshot of the Azure AD settings page. The page is divided into sections: Owners, Roles and administrators (Preview), Users and groups, Single sign-on, Provisioning, Application proxy, Self-service, Security, Conditional Access, Permissions, Token encryption, Activity, Sign-ins, and Usage & insights. The 'Application proxy' and 'Self-service' settings are highlighted with green checkmarks.

Answer:



Explanation

Graphical user interface, application Description automatically generated



NEW QUESTION: 254

You have an Azure subscription that contains an Azure Sentinel workspace.

Azure Sentinel is configured to ingest logs from several Azure workloads. A third-party service management platform is used to manage incidents. You need to identify which Azure Sentinel components to configure to meet the following requirements:

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

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

Which component should you identify for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

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

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

The image shows two identical dropdown menus. Each menu has a header with the Microsoft logo and a list of options: Analytics, Data connectors, Playbooks, and Workbooks. The first dropdown menu is currently open, showing the list of options.

Answer:

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

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

The image shows the same two dropdown menus as above. In the first dropdown menu, the 'Analytics' option is highlighted with a red box. In the second dropdown menu, the 'Playbooks' option is highlighted with a red box.

Reference:

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

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

NEW QUESTION: 255

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](#))

Explanation

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: 256

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

Name	Resource group
VM1	RG1
VM2	RG2
VM3	RG1
VM4	RG2

You need to ensure that the virtual machines in RG1 have the Remote Desktop port closed until an authorized user requests access.

What should you configure?

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

B. an application security group

C. Azure Active Directory (Azure AD) conditional access

D. just in time (JIT) VM access

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

Explanation

Just-in-time (JIT) virtual machine (VM) access can be used to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.

Note: When just-in-time is enabled, Security Center locks down inbound traffic to your Azure VMs by creating an NSG rule. You select the ports on the VM to which inbound traffic will be locked down.

These ports are controlled by the just-in-time solution.

When a user requests access to a VM, Security Center checks that the user has Role-Based Access Control (RBAC) permissions that permit them to successfully request access to a VM. If the request is approved, Security Center automatically configures the Network Security Groups (NSGs) and Azure Firewall to allow inbound traffic to the selected ports and requested source IP addresses or ranges, for the amount of time that was specified. After the time has expired, Security Center restores the NSGs to their previous states. Those connections that are already established are not being interrupted, however.

Reference:

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

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 (517 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 257

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:	Microsoft ▼ Cannot be accessed Can be accessed from the Azure portal only Can be accessed from inside container1 only Can be accessed from inside container1 and the Azure portal
Variable2:	▼ 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:

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

Variable2:

	▼
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: 258

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:

	▼
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	

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: 259

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:

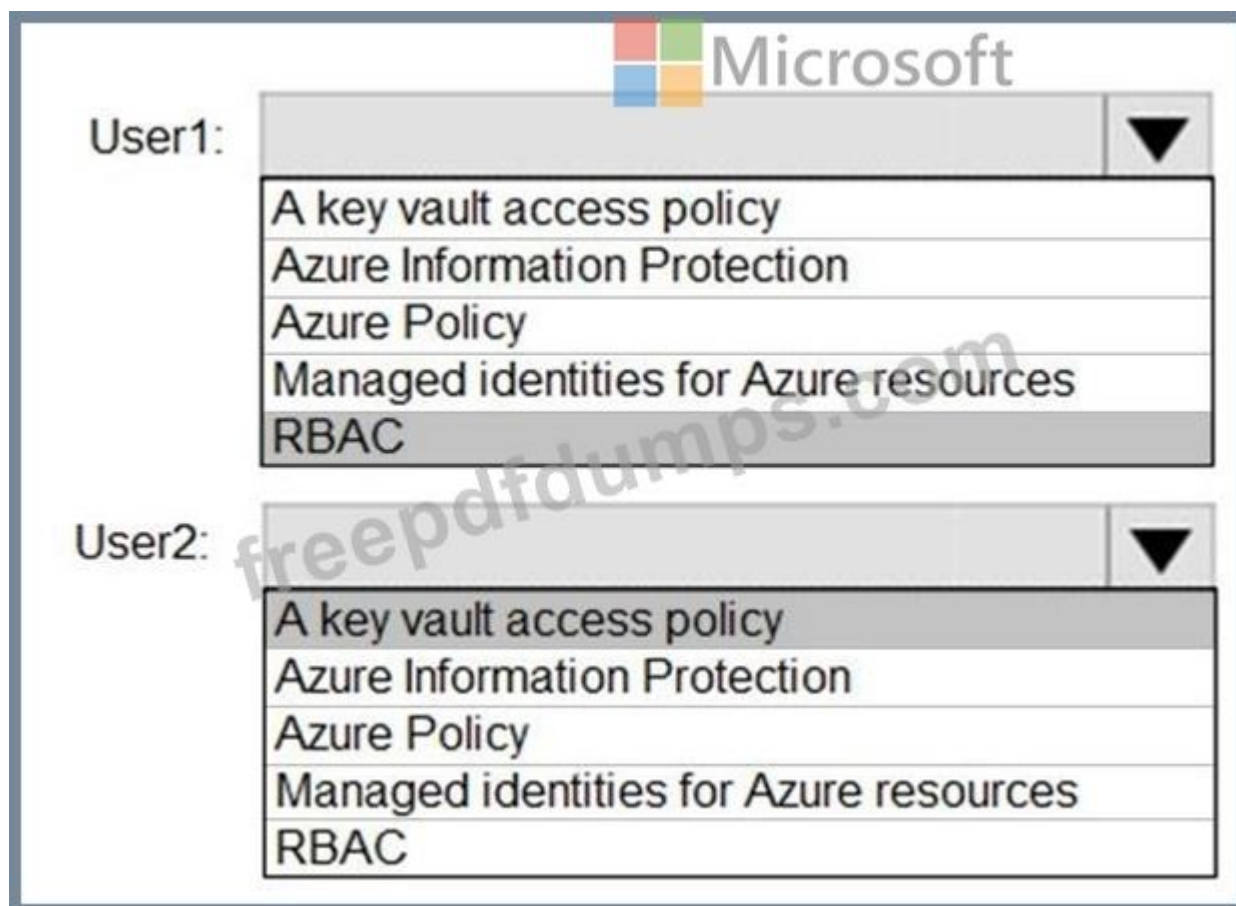
User1: ▼

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: 260

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

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

You create an Azure role by using the following JSON file.

```

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

```

You assign Role1 to User1 for 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.

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

Answer:

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

Reference:

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

NEW QUESTION: 261

You need to ensure that User2 can implement PIM.

What should you do first?

- A. Assign User2 the Global administrator role.
- B. Configure authentication methods for contoso.com.
- C. Configure the identity secure score for contoso.com.
- D. Enable multi-factor authentication (MFA) for User2.

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

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

1. Sign in to the Azure portal as a Global Administrator of your directory.

You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com), to enable PIM for a directory.

Scenario: Technical requirements include: Enable Azure AD Privileged Identity Management (PIM) for contoso.com References:

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-started> Manage identity and access Question Set 3

Manage identity and access

Testlet 1

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

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question on this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next sections of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question on this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

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

Existing Environment

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

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

The tenant contains the groups shown in the following table.

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

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

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

Azure Security Center is set to the Free tier.

Planned changes

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

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

Identity and Access Requirements

Litware identifies the following identity and access requirements:

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

Platform Protection Requirements

Litware identifies the following platform protection requirements:

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

Security Operations Requirements

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

Data and Application Requirements

Litware identifies the following data and applications requirements:

- * The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.
- * WebApp1 must enforce mutual authentication.

General Requirements

Litware identifies the following general requirements:

- * Whenever possible, administrative effort must be minimized.
- * Whenever possible, use of automation must be minimized.

NEW QUESTION: 262

You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016.

You need to implement a policy to ensure that each virtual machine has a custom antimalware virtual machine extension installed.

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

NOTE: Each correct selection is worth one point.



Microsoft

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

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

Answer:

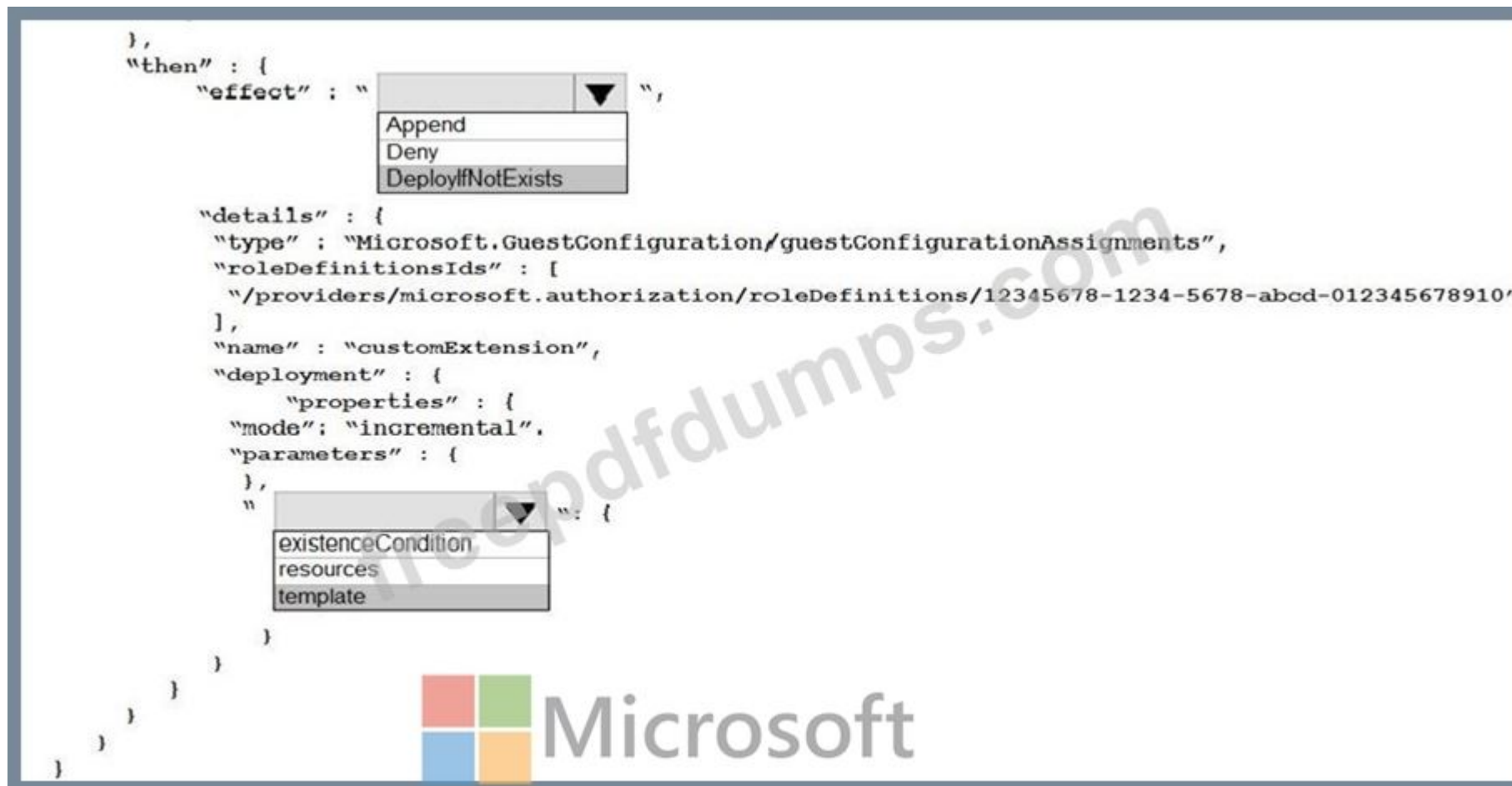
```

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

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

```

Explanation



Box 1: DeployIfNotExists

DeployIfNotExists executes a template deployment when the condition is met.

Box 2: Template

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

Deployment [required]

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

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

NEW QUESTION: 263

You plan to use Azure Sentinel to create an analytic rule that will detect suspicious threats and automate responses.

Which components are required for the rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Microsoft

Detect suspicious threats:

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

Automate responses:

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

Answer:

Microsoft

Detect suspicious threats:

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

Automate responses:

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

Reference:

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

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

NEW QUESTION: 264

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.)

```

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

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:

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: 265

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.

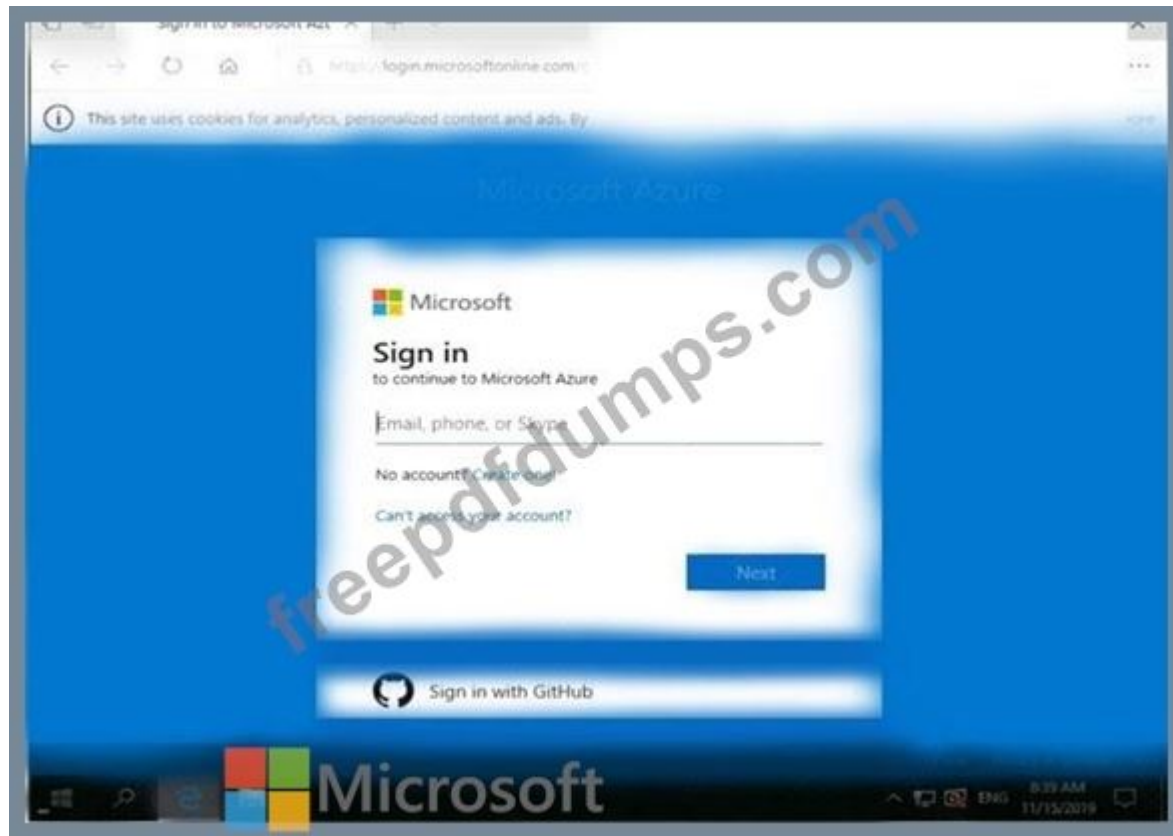
To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User1-10598168@ExamUsers.com

Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168



Home - Microsoft Azure x

https://portal.azure.com/home

Microsoft

Microsoft Azure

Search resources, services, and docs (0/77)

User1-10598168@Exam... MICROSOFT EXAMS

Azure services

Create a resource

Virtual machines

App Services

Storage accounts

SQL databases

Azure Database for PostgreSQL

Azure Cosmos DB

Kubernetes services

Function App

More services

Navigate

Subscriptions

Resource groups

All resources

Dashboard

Tools

Microsoft Learn
Learn Azure with free online training from Microsoft

Azure Monitor
Monitor your apps and infrastructure

Security Center
Secure your apps and infrastructure

Cost Management
Analyze and optimize your cloud spend for free

Useful links

Technical Documentation

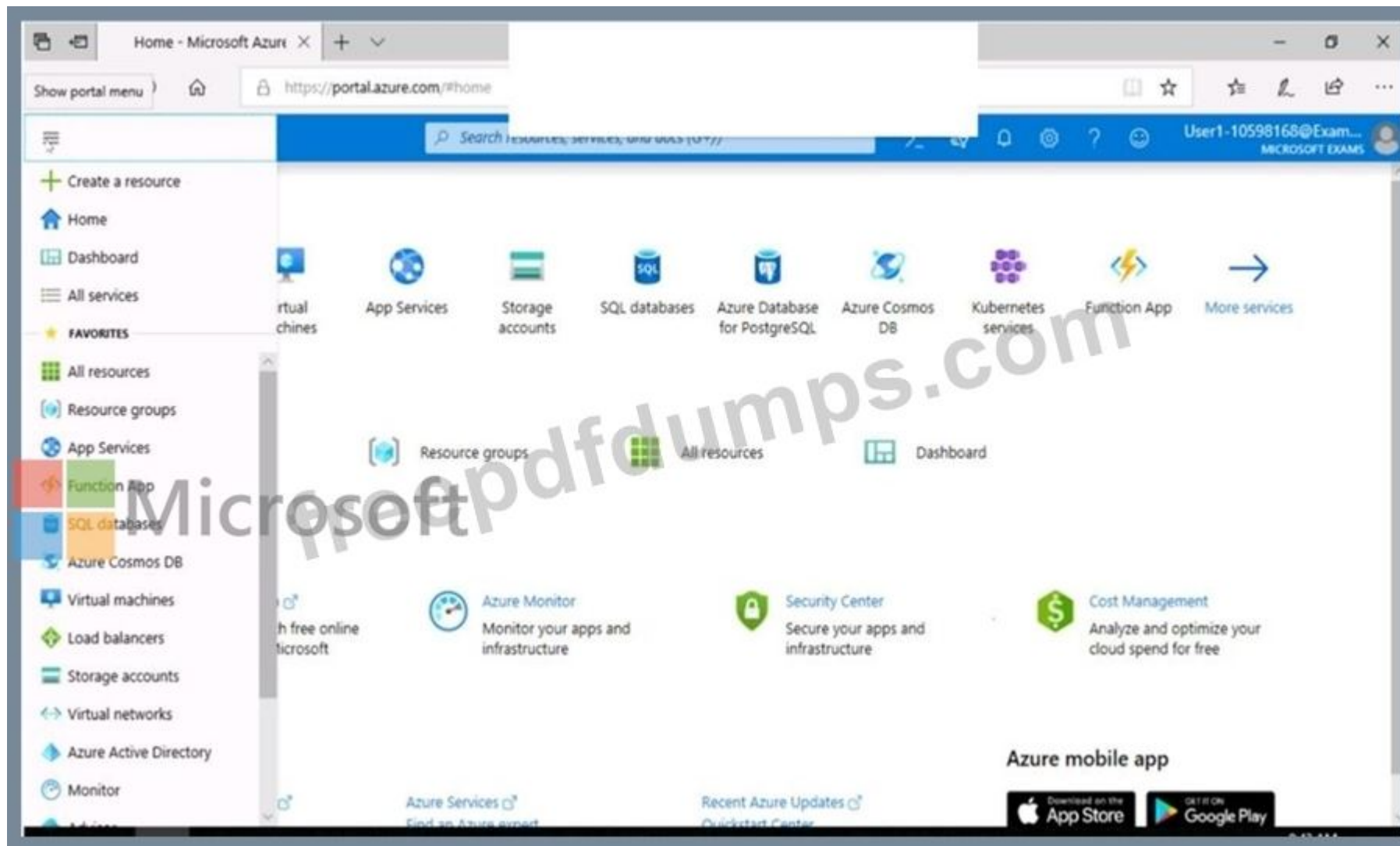
Azure Services

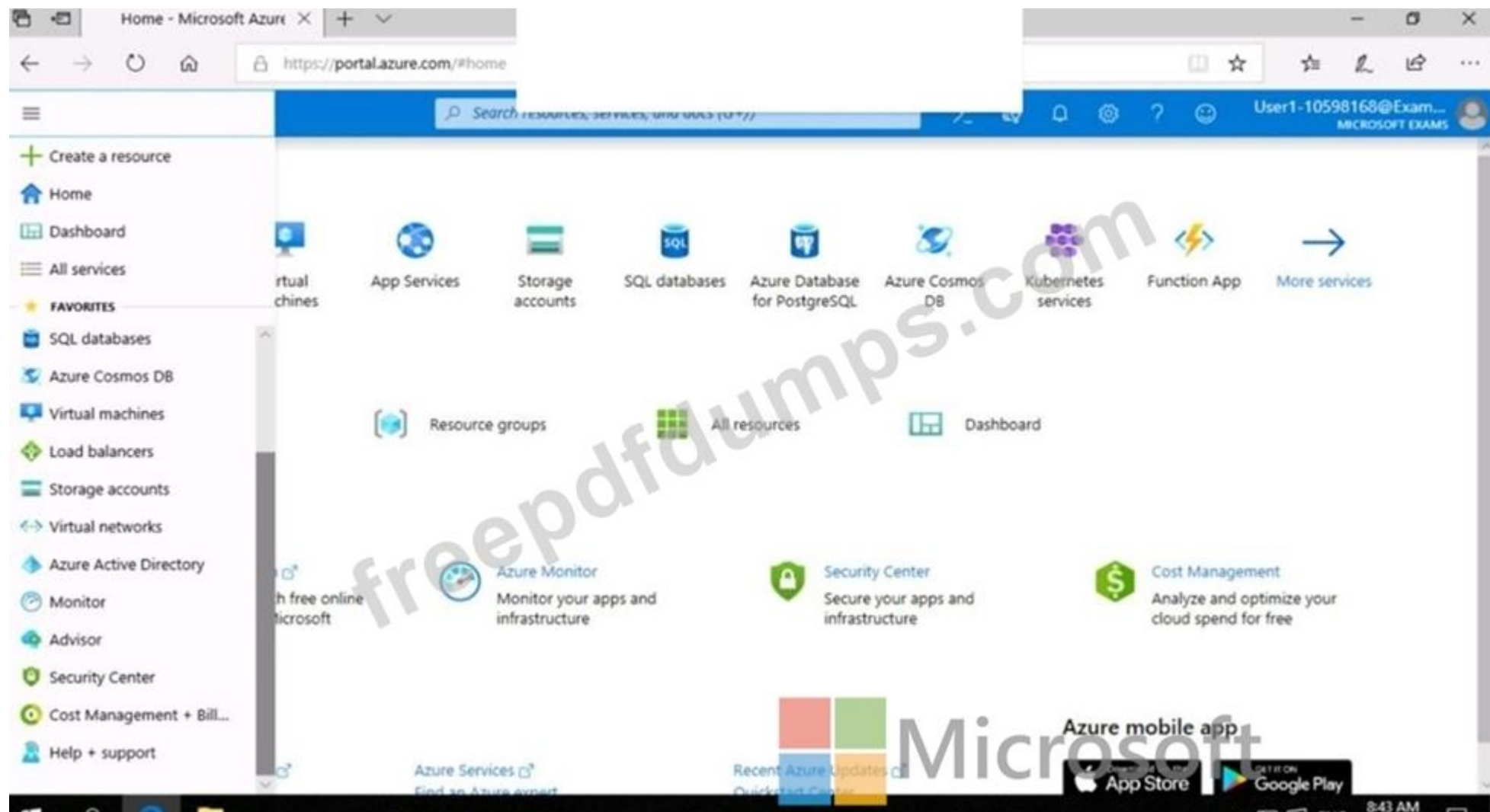
Recent Azure Updates

Azure mobile app

Download on the App Store

GET IT ON Google Play





You need to email an alert to a user named admin1@contoso.com if the average CPU usage of a virtual machine named VM1 is greater than 70 percent for a period of 15 minutes. To complete this task, sign in to the Azure portal.

Answer:

See the explanation below.

Explanation

Create an alert rule on a metric with the Azure portal

1. In the portal, locate the resource, here VM1, you are interested in monitoring and select it.
2. Select Alerts (Classic) under the MONITORING section. The text and icon may vary slightly for different resources.
3. Select the Add metric alert (classic) button and fill in the fields as per below, and click OK.

Metric: CPU Percentage

Condition: Greater than

Period: Over last 15 minutes

Notify via: email

Additional administrator email(s): admin1@contoso.com

Condition  Microsoft ▼

* Threshold

60 ✓ %

Period ⓘ

Over the last 5 minutes ▼

Notify via

Email owners, contributors, and readers

☒

Additional administrator email(s)

admin@contoso.com ✓

Webhook ⓘ

http://www.contoso.com/dowork?param ✓

Reference:

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-insights-alerts-portal>

NEW QUESTION: 266

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.

Microsoft

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

Microsoft

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: 267

You have two Azure virtual machines in the East US2 region as shown in the following table.

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

You deploy and configure an Azure Key vault.

You need to ensure that you can enable Azure Disk Encryption on VM1 and VM2.

What should you modify on each virtual machine? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

VM1:

The operating system version

The tier

The type

Microsoft VM2:

The operating system version

The tier

The type

Answer:

VM1:

	▼
The operating system version	
The tier	
The type	

VM2:

	▼
The operating system version	
The tier	
The type	

Explanation

VM1: The Tier

The Tier needs to be upgraded to standard.

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

VM2: the operating system

References:

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

NEW QUESTION: 268

You have two Azure subscriptions named Sub1 and Sub2. Sub1 contains a resource group named RG1 and an Azure policy named Policy1.

You need to remediate the non-compliant resources in Sub1 based on Policy1.

How should you complete the PowerShell script? To answer, drag the appropriate values to the correct targets.

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.

Values

Get-AzPolicyRemediation

Set-AzContext

Set-AzResourceGroup

Start-AzPolicyComplianceScan

Start-AzPolicyRemediation

Answer Area

```
$policyAssignmentId = "/subscriptions/f0710c27-9663-4c05-19f8-1b4be01e86a5/providers/Microsoft.Authorization/p
```

Value -Subscription "Sub1"

Value -PolicyAssignmentId \$policyAssignmentId -Name "policy1" -ResourceDiscovery

Answer:

Values

Get-AzPolicyRemediation

Set-AzContext

Set-AzResourceGroup

Start-AzPolicyComplianceScan

Start-AzPolicyRemediation

Answer Area

```
$policyAssignmentId = "/subscriptions/f0710c27-9663-4c05-19f8-1b4be01e86a5/providers/Microsoft.Authorization/p
```

Set-AzContext -Subscription "Sub1"

Start-AzPolicyRemediation -PolicyAssignmentId \$policyAssignmentId -Name "policy1" -ResourceDiscovery

Explanation:

For the first blank, use Set-AzContext to set the current subscription context.

For the second blank, use Start-AzPolicyRemediation to create and start a policy remediation for a policy assignment.

The final script should look like this:

```
$policyAssignmentId = "/subscriptions/f0710c27-9663-4c05-1978-1bdbedle86as/providers/Microsoft.
```

```
Authorization/f Value Set-AzContext -Subscription "Sub1" Value Start-AzPolicyRemediation
```

```
-PolicyAssignmentId $policyAssignmentId -Name "policy1" -ResourceDiscovery
```

NEW QUESTION: 269

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.	☐	☒

Reference:

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

NEW QUESTION: 270

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](#))

Explanation

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: 271

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

You need to configure authorization access.

Which authorization types can you use for each storage account? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

storage1:

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

storage2:

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

storage3:

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

Answer:

storage1:

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

storage2:

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

storage3:

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

Reference:

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

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 (517 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 272

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:

- Fusion
- Microsoft Security incident creation
- Scheduled

Configure the playbook to include:

- 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: 273

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

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: 274

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

<https://www.fast2test.com/AZ-500-practice-test.html> 45

Valid Fast2test AZ-500 Exam PDF Dumps - New AZ-500 Real Exam Questions

C. VM1, VM3 and VM4 only

D. VM1, VM2, VM3, and VM4

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

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: 275

On Monday, you configure an email notification in Microsoft Defender for Cloud to notify user1 @contoso.com about alerts that have a severity level of Low, Medium, or High. On Tuesday, Microsoft Defender for Cloud generates the security alerts shown in the following table.

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

How many email notifications will user1 @contoso.com receive on Tuesday? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

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

4

1

2

3

4

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

7

3

4

7

9

11



Microsoft

Answer:

Answer Area

Microsoft

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

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

Answer Area

Microsoft

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

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

NEW QUESTION: 276

You have an Azure subscription that contains a user named User1 and a storage account named storage 1. The storage1 account contains the resources shown in the following table:

Name	Type
container1	Container
folder1	File share
table1	Table

User1 is assigned the following roles for storage1:

- * Storage Blob Data Reader
- * Storage Table Data Contributor
- * Storage File Data SMB Share Reader

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

Answer:

Statements

On October 1, 2022, if User1 accesses folder1 by using SAS1, he can delete the files in folder1.

On October 1, 2022, if User1 maps folder1 as a network drive by using his Azure Active Directory (Azure AD) credentials, he can delete the files in folder1.

On October 1, 2022, User1 can delete the rows in table1 by using SAS1.

Yes

☐

No

☒☒☐☐☒

NEW QUESTION: 277

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

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

You create the Azure Storage accounts shown in the following table.

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

You need to configure auditing for SQL1.

Which storage accounts and Log Analytics workspaces can you use as the audit log destination? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

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

Answer:

Answer Area



Microsoft

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

☒ Storage1 only
☒ Storage2 only
☐ Storage1 and Storage2 only
☐ Storage1, Storage2, and Storage3

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

☐ Analytics1 only
☐ Analytics1 and Analytics2 only
☐ Analytics1 and Analytics3 only
☒ Analytics1, Analytics2, and Analytics3

NEW QUESTION: 278

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

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

You need to configure authorization access.

Which authorization types can you use for each storage account? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

storage1:	▼ Shared Key only Shared access signature (SAS) only Azure Active Directory (Azure AD) only Shared Key and shared access signature (SAS) only Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)
storage2:	▼ Shared Key only Shared access signature (SAS) only Shared Key and shared access signature (SAS)
storage3:	▼ Shared Key only Shared access signature (SAS) only Azure Active Directory (Azure AD) only Shared Key and shared access signature (SAS) only Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

Answer:

storage1:

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

storage2:

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

storage3:

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

Reference:

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

NEW QUESTION: 279

You have an Azure subscription that contains an Azure Sentinel workspace.

Azure Sentinel is configured to ingest logs from several Azure workloads. A third-party service management platform is used to manage incidents.

You need to identify which Azure Sentinel components to configure to meet the following requirements:

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

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

Which component should you identify for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

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

Analytics
Data connectors
Playbooks
Workbooks

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

Analytics
Data connectors
Playbooks
Workbooks

Answer:

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

▼

Analytics

Data connectors

Playbooks

Workbooks

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

▼

Analytics

Data connectors

Playbooks

Workbooks

Reference:

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

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

NEW QUESTION: 280

You have two Azure virtual machines in the East US2 region as shown in the following table.

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

You deploy and configure an Azure Key vault.

You need to ensure that you can enable Azure Disk Encryption on VM1 and VM2.

What should you modify on each virtual machine? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

VM1:

▼

The operating system version

The tier

The type

VM2:

▼

The operating system version

The tier

The type

Answer:

VM1: 

 The operating system version

The tier

The type

VM2: 

The operating system version

The tier

The type

References:

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

NEW QUESTION: 281

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

Name	Type	Attached to	NSG
NSG1	Network security group (NSG)	VM5	Not applicable
NSG2	Network security group (NSG)	Subnet1	Not applicable
Subnet1	Subnet	Not applicable	Not applicable
VM5	Virtual machine	Subnet1	NSG1

An IP address of 10.1.0.4 is assigned to VM5. VM5 does not have a public IP address.

VM5 has just in time (JIT) VM access configured as shown in the following exhibit.

JIT VM access configuration

VM5

+ Add  Save  Discard

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

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

You enable JIT VM access for VM5.

NSG1 has the inbound rules shown in the following exhibit.

Priority	Name	Port	Protocol	Source	Destination	Action
100	SecurityCenter-JITRule-...	3389	Any	Any	10.1.0.4	Allow
1000	SecurityCenter-JITRule_341...	3389	Any	Any	10.1.0.4	Deny
1001	RDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

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
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	☐	☐
Remote Desktop access to VM5 is blocked.	☐	☐
An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.	☐	☐

Answer:

Statements	Yes	No
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	☒	☐
Remote Desktop access to VM5 is blocked.	☒	☐
An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.	☐	☒

NEW QUESTION: 282

You have an app that uses an Azure SQL database.

You need to be notified if a SQL injection attack is launched against the database.

What should you do?

- A. Deploy the SQL Health Check solution in Azure Monitor.
- B. Modify the Diagnostics settings for the database.
- C. Enable server-level auditing for the database.
- D. Enable Azure Defender for SQL for the database.

Answer: (SHOW ANSWER)

NEW QUESTION: 283

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

Name	Role
Admin1	Global administrator
Admin2	Group administrator
Admin3	User administrator

Contoso.com contains a group naming policy. The policy has a custom blocked word list rule that includes the word Contoso.

Which users can create a group named Contoso Sales in contoso.com? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Users who can create a security group named Contoso Sales:

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

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

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

Answer:

Users who can create a security group named Contoso Sales:

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

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

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

Reference:

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

NEW QUESTION: 284

You have an Azure subscription named Sub1 that contains an Azure Storage account named Contosostorage1 and an Azure key vault named Contosokeyvault1.

You plan to create an Azure Automation runbook that will rotate the keys of Contosostorage1 and store them in Contosokeyvault1.

You need to implement prerequisites to ensure that you can implement the runbook.

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

Run Set-AzureRmKeyVaultAccessPolicy

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

Create a user-assigned managed identity.

Create a connection resource in the Azure Automation account.

Answer Area

←

→

↑

↓

Microsoft

Answer:

Actions

Run Set-AzureRmKeyVaultAccessPolicy

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

Create a user-assigned managed identity.

Create a connection resource in the Azure Automation account.

Explanation

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

Create a connection resource in the Azure Automation account.

Answer Area

Microsoft

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

Create a connection resource in the Azure Automation account.

Step 1: Create an Azure Automation account

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

Step 2: Import PowerShell modules to the Azure Automation account

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

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

You can use the sample code below, taken from the AzureAutomationTutorialScript example runbook, to authenticate using the Run As account to manage Resource Manager resources with your runbooks. The AzureRunAsConnection is a connection asset automatically created when we created 'run as accounts' above. This can be found under Assets -> Connections. After the authentication code, run the same code above to get all the keys from the vault.

```
$connectionName = "AzureRunAsConnection"
```

```
try
```

```
{
```

```
# Get the connection "AzureRunAsConnection "
```

```
$servicePrincipalConnection=Get-AutomationConnection -Name $connectionName
```

```
"Logging in to Azure..."
```

```
Add-AzureRmAccount `
```

```
-ServicePrincipal `
```

```
-TenantId $servicePrincipalConnection.TenantId `
```

```
-ApplicationId $servicePrincipalConnection.ApplicationId `
```

```
-CertificateThumbprint $servicePrincipalConnection.CertificateThumbprint
```

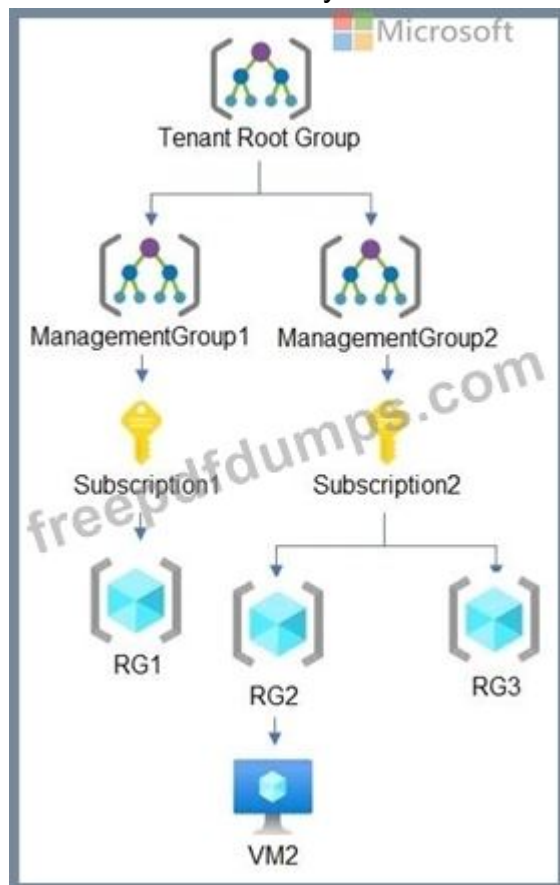
```
}
```

References:

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

NEW QUESTION: 285

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.	☐	☒

NEW QUESTION: 286

What is the membership of Group1 and Group2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Group1:

No members
Only User2
Only User2 and User4
User1, User2, User3, and User4

Group2:

No members
Only User3
Only User1 and User3
User1, User2, User3, and User4

Answer:

Settings

Activity log

Logs

Metrics

Service Health

Answer Area

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

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

Activity log

Logs

Explanation

Group1: ▼

- No members
- Only User2
- Only User2 and User4
- User1, User2, User3, and User4

Group2: ▼

- No members
- Only User3
- Only User1 and User3
- User1, User2, User3, and User4

Box 1: User1, User2, User3, User4

Contains "ON" is true for Montreal (User1), MONTREAL (User2), London (User 3), and Ontario (User4) as string and regex operations are not case sensitive.

Box 2: Only User3

Match "*on" is only true for London (User3).

Scenario:

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"

References:

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

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 (517

Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 287

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

Reference:

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

NEW QUESTION: 288

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

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

You plan to enable Microsoft Defender for Cloud for the subscription. Which resources can be protected by using Microsoft Defender for Cloud?

- A. VM1, storage1, and Vault1 only
- B. VM1 and storage1 only
- C. VM1, VNET1, and storage1 only
- D. VM1.VNET1, storage1, and Vault1
- E. VM1 and VNET only

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

NEW QUESTION: 289

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

Reference:

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

NEW QUESTION: 290

You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016.

You need to implement a policy to ensure that each virtual machine has a custom antimalware virtual machine extension installed.

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

NOTE: Each correct selection is worth one point.


```

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

```

	▼
Append	
Deny	
DeployIfNotExists	

```

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

```

	▼
existenceCondition	
resources	
template	

Answer:

```

{
  "if" : {
    "allOf" : [
      {
        "field" : "type",
        "equals" : "Microsoft.Compute/virtualMachines"
      },
      {
        "field" : "Microsoft.Compute/imageSKU",
        "equals" : "2016-Datacenter",
      }
    ]
  },
  "then" : {
    "effect" : "Append",
    "details" : {
      "type" : "Microsoft.GuestConfiguration/guestConfigurationAssignments",
      "roleDefinitionsIds" : [
        "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
      ],
      "name" : "customExtension",
      "deployment" : {
        "properties" : {
          "mode" : "incremental",
          "parameters" : {
            "existenceCondition": {
              "resources": {
                "template": {

```

Explanation:

```

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

```



Box 1: DeployIfNotExists

DeployIfNotExists executes a template deployment when the condition is met.

Box 2: Template

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

Deployment [required]

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

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

NEW QUESTION: 291

You have an Azure subscription named Sub1.

You have an Azure Active Directory (Azure AD) group named Group1 that contains all the members of your IT team.

You need to ensure that the members of Group1 can stop, start, and restart the Azure virtual machines in Sub1.

The solution must use the principle of least privilege.

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

Create a JSON file.

Run the Update-AzureRmManagementGroup cmdlet.

Create an XML file.

Run the New-AzureRmRoleDefinition cmdlet.

Run the New-AzureRmRoleAssignment cmdlet.

Answer Area



Answer:

Actions

Create a JSON file.

Run the Update-AzureRmManagementGroup cmdlet.

Create an XML file.

Run the New-AzureRmRoleDefinition cmdlet.

Run the New-AzureRmRoleAssignment cmdlet.

Answer Area

Create a JSON file.

Run the New-AzureRmRoleDefinition cmdlet.

Run the New-AzureRmRoleAssignment cmdlet.



Explanation



Create a JSON file.

Run the New-AzureRmRoleDefinition cmdlet.

Run the New-AzureRmRoleAssignment cmdlet.

References:

<https://www.petri.com/cloud-security-create-custom-rbac-role-microsoft-azure>

NEW QUESTION: 292

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: ([SHOW ANSWER](#))

Explanation

References:

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

NEW QUESTION: 293

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.

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:

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.	☒	☐

NEW QUESTION: 294

You have an Azure Active Directory (Azure AD) tenant named contoso.com.

You need to configure diagnostic settings for contoso.com. The solution must meet the following requirements:

- * Retain logs for two years.
- * Query logs by using the Kusto query language.
- * Minimize administrative effort.

Where should you store the logs?

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 295

You have an Azure subscription named Sub1.

You have an Azure Active Directory (Azure AD) group named Group1 that contains all the members of your IT team.

You need to ensure that the members of Group1 can stop, start, and restart the Azure virtual machines in Sub1. The solution must use the principle of least privilege.

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
Create a JSON file.	
Run the Update-AzureRmManagementGroup cmdlet.	
Create an XML file.	
Run the New-AzureRmRoleDefinition cmdlet.	
Run the New-AzureRmRoleAssignment cmdlet.	

Answer:

Actions	Answer Area
Create a JSON file.	Create a JSON file.
Run the Update-AzureRmManagementGroup cmdlet.	Run the Update-AzureRmManagementGroup cmdlet.
Create an XML file.	
Run the New-AzureRmRoleDefinition cmdlet.	Run the New-AzureRmRoleDefinition cmdlet.
Run the New-AzureRmRoleAssignment cmdlet.	

References:

<https://www.petri.com/cloud-security-create-custom-rbac-role-microsoft-azure>

NEW QUESTION: 296

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 297

You have an Azure subscription named Sub1.

In Azure Security Center, you have a workflow automation named WF1. WF1 is configured to send an email message to a user named User1.

You need to modify WF1 to send email messages to a distribution group named Alerts.

What should you use to modify WF1?

- A. Azure Application Insights
- B. Azure Monitor
- C. Azure Logic Apps Designer
- D. Azure DevOps

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

Reference:

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

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

NEW QUESTION: 298

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:



Microsoft

▼

User2 only

User1 and User2 only

User2 and User4 only

User1, User2, and User4

User1, User2, User3, and User4

Answer:

Upload images: ▼

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

Download images: ▼

User2 only
User1 and User2 only
User2 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: 299

You need to ensure that users can access VM0. The solution must meet the platform protection requirements.

What should you do?

- A. Move VM0 to Subnet1.
- B. On Firewall, configure a network traffic filtering rule.
- C. Assign RT1 to AzureFirewallSubnet.
- D. On Firewall, configure a DNAT rule.

Answer: A (LEAVE A REPLY)

Explanation

Azure Firewall has the following known issue:

Conflict with Azure Security Center (ASC) Just-in-Time (JIT) feature.

If a virtual machine is accessed using JIT, and is in a subnet with a user-defined route that points to Azure Firewall as a default gateway, ASC JIT doesn't work. This is a result of asymmetric routing - a packet comes in via the virtual machine public IP (JIT opened the access), but the return path is via the firewall, which drops the packet because there is no established session on the firewall.

Solution: To work around this issue, place the JIT virtual machines on a separate subnet that doesn't have a user-defined route to the firewall.

Scenario:

VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
-----	-----------------	--

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.

Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.

References:

Topic 1, Litware, inc

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided. To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question on this case study. At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next sections of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question on this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

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

Existing Environment

Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4. Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated. The tenant contains the groups shown in the following table.

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

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

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

Azure Security Center is set to the Free tier.

Planned changes

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

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

Litware identifies the following identity and access requirements:

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

Platform Protection Requirements

Litware identifies the following platform protection requirements:

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

Security Operations Requirements

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

NEW QUESTION: 300

You have an Azure subscription named Sub1. Sub1 has an Azure Storage account named Storage1 that contains the resources shown in the following table.

Name	Type
Container1	Blob container
Share1	File share

You generate a shared access signature (SAS) to connect to the blob service and the file service.

Which tool can you use to access the contents in Container1 and Share1 by using the SAS? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Microsoft

Tools for Container1:

- Robocopy.exe
- Azure Storage Explorer
- File Explorer

Tools for Share1:

- Robocopy.exe
- Azure Storage Explorer
- File Explorer

Answer:

Explanation

Tools for Container1:

- Robocopy.exe
- Azure Storage Explorer
- File Explorer

Tools for Share1:

- Robocopy.exe
- Azure Storage Explorer
- File Explorer

NEW QUESTION: 301

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

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

The tenant contains the named locations shown in the following table.

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

You create the conditional access policies for a cloud app named App1 as shown in the following table.

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

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 can access App1 from an IP address of 154.12.18.10.	☐	☐
User2 can access App1 from an IP address of 193.77.10.15.	☐	☐
User2 can access App1 from an IP address of 154.12.18.34.	☐	☐



Answer:

Answer Area

Statements

User1 can access App1 from an IP address of 154.12.18.10.

User2 can access App1 from an IP address of 193.77.10.15.

User2 can access App1 from an IP address of 154.12.18.34.

Yes

No

☐

☒

☒

☐

☐

☒

Explanation:

Answer Area

Statements

User1 can access App1 from an IP address of 154.12.18.10.

User2 can access App1 from an IP address of 193.77.10.15.

User2 can access App1 from an IP address of 154.12.18.34.

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 (517 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 302

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

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

Azure AD Privileged Identity Management (PIM) is enabled for the tenant.

In PIM, the Password Administrator role has the following settings:

Maximum activation duration (hours): 2

Send email notifying admins of activation: Disable

Require incident/request ticket number during activation: Disable

Require Azure Multi-Factor Authentication for activation: Enable

Require approval to activate this role: Enable

Selected approver: Group1

You assign users the Password Administrator role as shown in the following table.

Name	Assignment type
User1	Active
User2	Eligible
user3	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
When User1 signs in, the user is assigned the Password Administrator role automatically.	☐	☐
User2 can request to activate the Password Administrator role.	☐	☐
If User3 wants to activate the Password Administrator role, the user can approve their own request.	☐	☐

Answer:

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

NEW QUESTION: 303

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

Microsoft

Allow access from:

☐ All networks ☒ Selected networks

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

Virtual networks: **i** + Add existing virtual networks + Add new virtual network

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

Firewall: **i**

IPv4 ADDRESS OR CIDR

IPv4 address or CIDR ...

Exception:

Allow trusted Microsoft services to bypass this firewall? **i** ☒ Yes ☐ No

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

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
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:

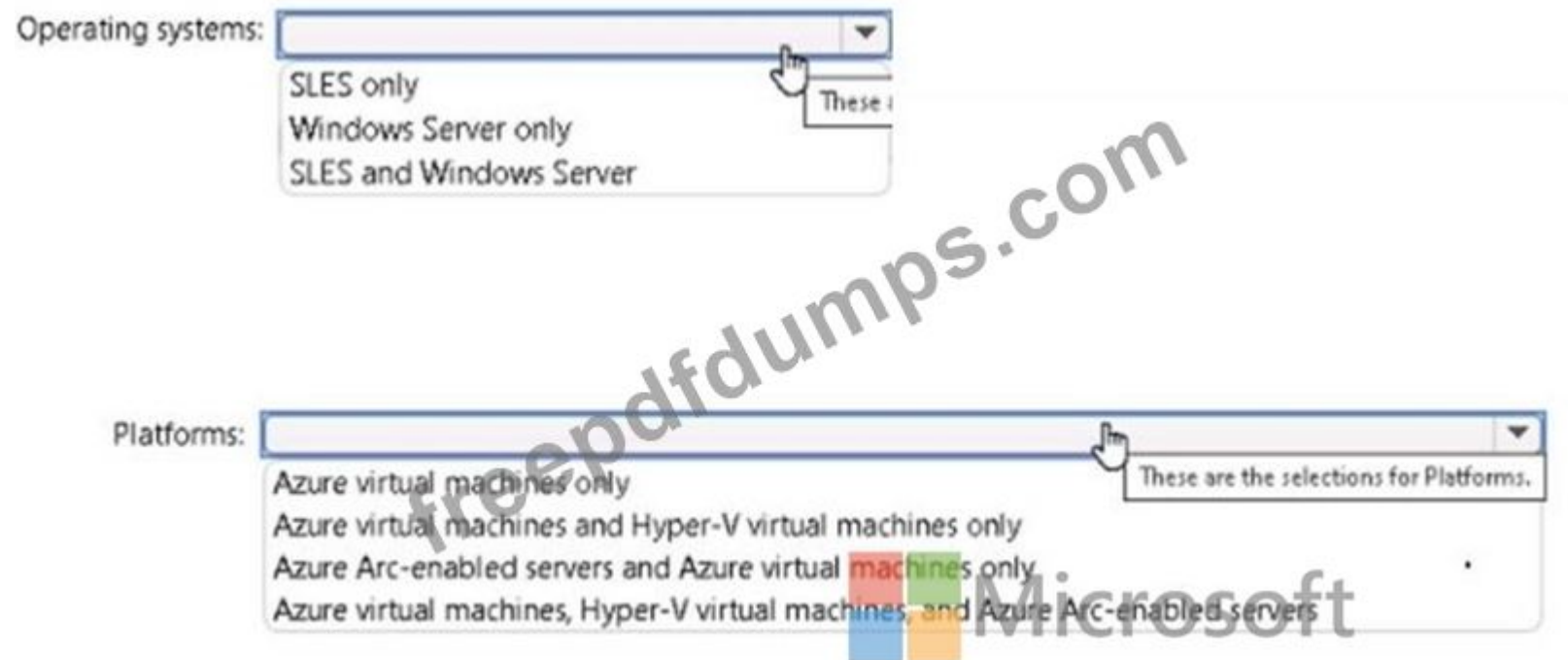
Answer Area		
Statements	Yes	No
From VM1, users can manage the keys and secrets stored in KeyVault1.	☒	☐
From VM2, users can manage the keys and secrets stored in KeyVault1.	☐	☒
VM2 can use KeyVault for Azure Disk Encryption.	☒	☐

NEW QUESTION: 304

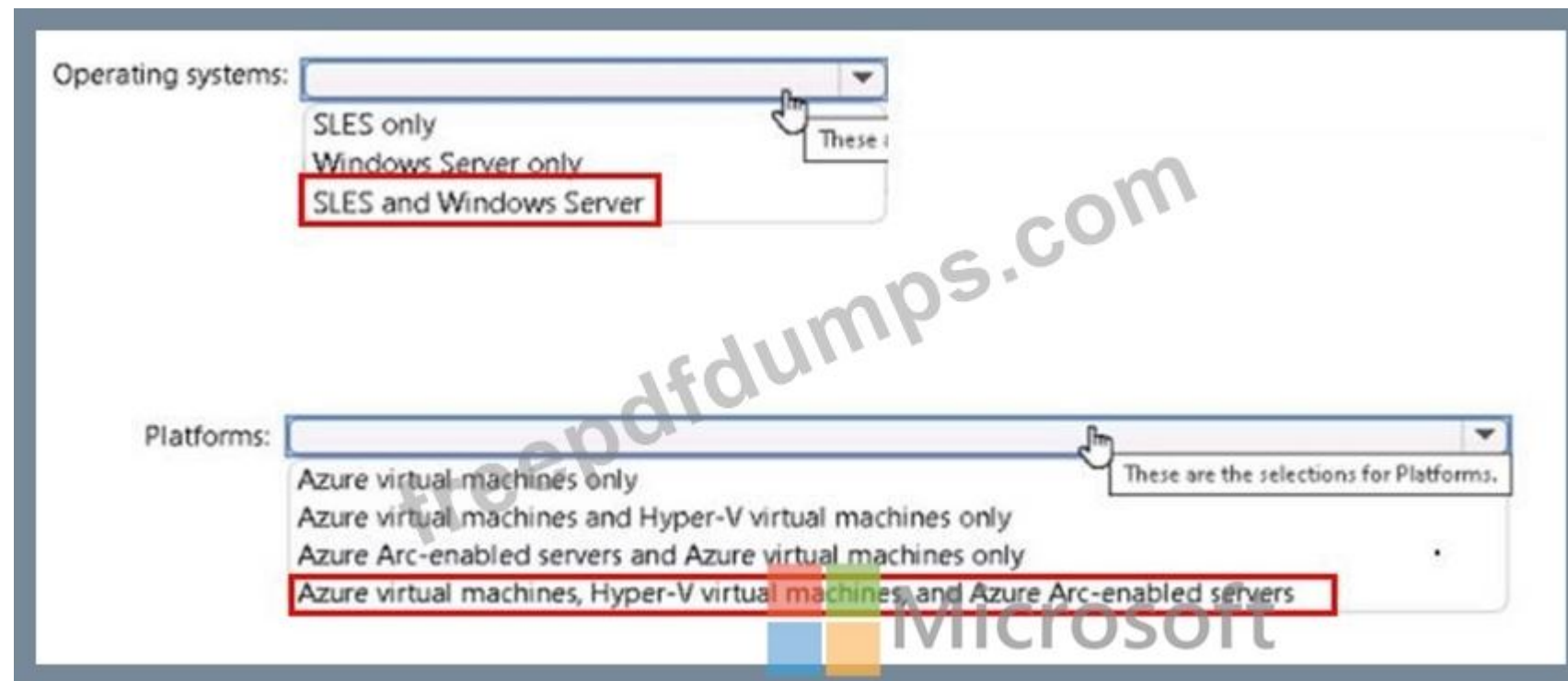
Your on-premises network contains the servers shown in the following table.

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 or SLES. You plan to implement adaptive application controls in Microsoft Defender for Cloud. Which operating systems and platforms can you monitor? To answer, select the appropriate options in the answer area.



Answer:



NEW QUESTION: 305

You have an Azure subscription that contains 100 virtual machines. Azure Diagnostics is enabled on all the virtual machines.

You are planning the monitoring of Azure services in the subscription.

You need to retrieve the following details:

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

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

What should you use in Azure Monitor? To answer, drag the appropriate configuration settings to the correct details. Each configuration setting 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.

Settings	Answer Area
Activity log	
Logs	Identify the user who deleted a virtual machine three weeks ago:
Metrics	Query the security events of a virtual machine that runs Windows Server 2016:
Service Health	

Answer:

Settings	Answer Area
Activity log	
Logs	Identify the user who deleted a virtual machine three weeks ago: Activity log
Metrics	Query the security events of a virtual machine that runs Windows Server 2016: Logs
Service Health	

Reference:

<https://docs.microsoft.com/en-us/azure/security/azure-log-audit>

NEW QUESTION: 306

You plan to use Azure Resource Manager templates to perform multiple deployments of identically configured Azure virtual machines. The password for the administrator account of each deployment is stored as a secret in different Azure key vaults.

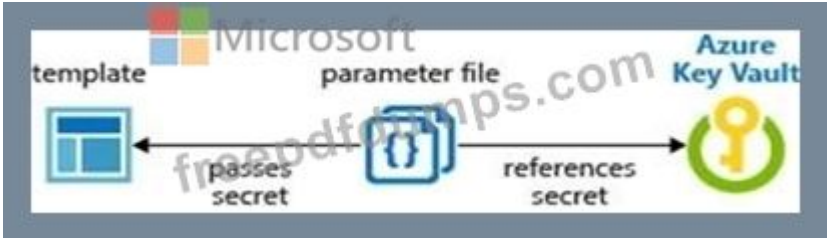
You need to identify a method to dynamically construct a resource ID that will designate the key vault containing the appropriate secret during each deployment. The name of the key vault and the name of the secret will be provided as inline parameters.

What should you use to construct the resource ID?

- A. a key vault access policy
- B. a linked template
- C. a parameters file
- D. an automation account

Answer: ([SHOW ANSWER](#))

You reference the key vault in the parameter file, not the template. The following image shows how the parameter file references the secret and passes that value to the template.



Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-keyvault-parameter>

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

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question on this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next sections of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question on this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

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

Existing Environment

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

Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices.

Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.

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

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

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

Identity and Access Requirements

Azure Security Center is set to the Free tier.

Planned changes

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

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

Litware identifies the following identity and access requirements:

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

Platform Protection Requirements

Litware identifies the following platform protection requirements:

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

Security Operations Requirements

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

Data and Application Requirements

Litware identifies the following data and applications requirements:

- * The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.
- * WebApp1 must enforce mutual authentication.

General Requirements

Litware identifies the following general requirements:

- * Whenever possible, administrative effort must be minimized.
- * Whenever possible, use of automation must be minimized.

NEW QUESTION: 307

You have an Azure Active Directory (Azure AD) tenant named contoso1812.onmicrosoft.com that contains the users shown in the following table.

Name	Username	Type
User1	User1@contoso1812.onmicrosoft.com	Member
User2	User2@contoso1812.onmicrosoft.com	Member
User3	User3@contoso1812.onmicrosoft.com	Member
User4	User4@outlook.com	Guest

You create an Azure Information Protection label named Label1. The Protection settings for Label1 are configured as shown in the exhibit. (Click the Exhibit tab.)

Protection

Contoso1812 - Azure Information Protection

Protections settings ⓘ

Azure (cloud key) HYOK (AD RMS)

Select the protection action type ⓘ

- ☒ Set permissions
- ☐ Set user-defined permissions (Preview)

USERS	PERMISSIONS
AuthenticatedUsers	Viewer
User1@contoso1812.onmicrosoft.com	Co-Author
User2@contoso1812.onmicrosoft.com	Reviewer

+Add permissions



Label1 is applied to a file named File1.

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 print File1.	☐	☐
 User3 can read File1.	☐	☐
User4 can print File1.	☐	☐

Answer:

Statements	Yes	No
User1 can print File1.	☒	☐
User3 can read File1.	☒	☐
User4 can print File1.	☐	☒

NEW QUESTION: 308

You have an Azure subscription that contains an Azure key vault named Vault1.
On January 1, 2019, Vault1 stores the following secrets.


```
Enabled      : False
Expires      :
NotBefore    : 5/1/19 12:00:00 AM
Created      : 12/20/18 2:55:00 PM
Updated      : 12/20/18 2:55:00 PM
ContentType  :
Tags         :
TagTable     :
VaultName    : vault1
Name         : Password1
Version      :
Id           : https://vault1.vault.azure.net:443/secrets/Password1

Enabled      : True
Expires      : 5/1/19 12:00:00 AM
NotBefore    : 3/1/19 12:00:00 AM
Created      : 12/20/18 3:00:00 PM
Updated      : 12/20/18 3:00:00 PM
ContentType  :
Tags         :
TagTable     :
VaultName    : vault1
Name         : Password2
Version      :
Id           : https://vault1.vault.azure.net:443/secrets/Password2
```

Which can each secret be used by an application? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Password1: ▼

- Never
- Always
- Only after May 1, 2019

Password2: ▼

- Never
- Always
- Only between March 1, 2019 and May 1, 2019

Answer:

Password1:

Never

Always

Only after May 1, 2019

 Password2:

Never

Always

Only between March 1, 2019 and May 1. 2019

Reference:

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

NEW QUESTION: 309

Your company has an Azure subscription named Subscription1. Subscription1 is associated with the Azure Active Directory tenant that includes 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: ▼

- User1
- User2
- User3
- User4

Tool: ▼

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

 Microsoft

Answer:

User:

Tool:

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

NEW QUESTION: 310

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

The permissions are assigned to the following role definition:

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

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:

Answer Area

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

Explanation

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

NEW QUESTION: 311

You need to ensure that the audit logs from the SQLdb1 Azure SQL database are stored in the WS11641655 Azure Log Analytics workspace.
To complete this task, sign in to the Azure portal and modify the Azure resources.

Answer:

See explanation below.

Explanation

- 1. In the Azure portal, type SQL in the search box, select SQL databases from the search results then select SQLdb1. Alternatively, browse to SQL databases in the left navigation pane.
- 2. In the properties of SQLdb1, scroll down to the Security section and select Auditing.
- 3. Turn auditing on if it isn't already, tick the Log Analytics checkbox then click on Configure.

Auditing

ON

OFF

Audit log destination (choose at least one):

Storage

☒ Log Analytics (Preview)

Log Analytics details

Configure

☐ Event Hub (Preview)

- 4. Select the WS11641655 Azure Log Analytics workspace.
- 5. Click Save to save the changes.

NEW QUESTION: 312

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: User1-10598168@ExamUsers.com

Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168

← → ↻ 🏠 <https://login.microsoftonline.com/c> ...

ⓘ This site uses cookies for analytics, personalized content and ads. By

Microsoft Azure

 Microsoft

Sign in

to continue to Microsoft Azure

Email, phone, or Skype

No account? [Create one!](#)

[Can't access your account?](#)

Next

 Sign in with GitHub

Microsoft

Terms of use Privacy & cookies

8:39 AM ENG

Home - Microsoft Azure

https://portal.azure.com/#home

Microsoft Azure

Search

User1-10598168@Exam...
MICROSOFT EXAMS

Azure services

Create a resource

Virtual machines

App Services

Storage accounts

SQL databases

Azure Database for PostgreSQL

Azure Cosmos DB

Kubernetes services

Function App

More services

Navigate

Subscriptions

Resource groups

All resources

Dashboard

Tools

Microsoft Learn
Learn Azure with free online training from Microsoft

Azure Monitor
Monitor your apps and infrastructure

Security Center
Secure your apps and infrastructure

Cost Management
Analyze and optimize your cloud spend for free

Useful links

Technical Documentation

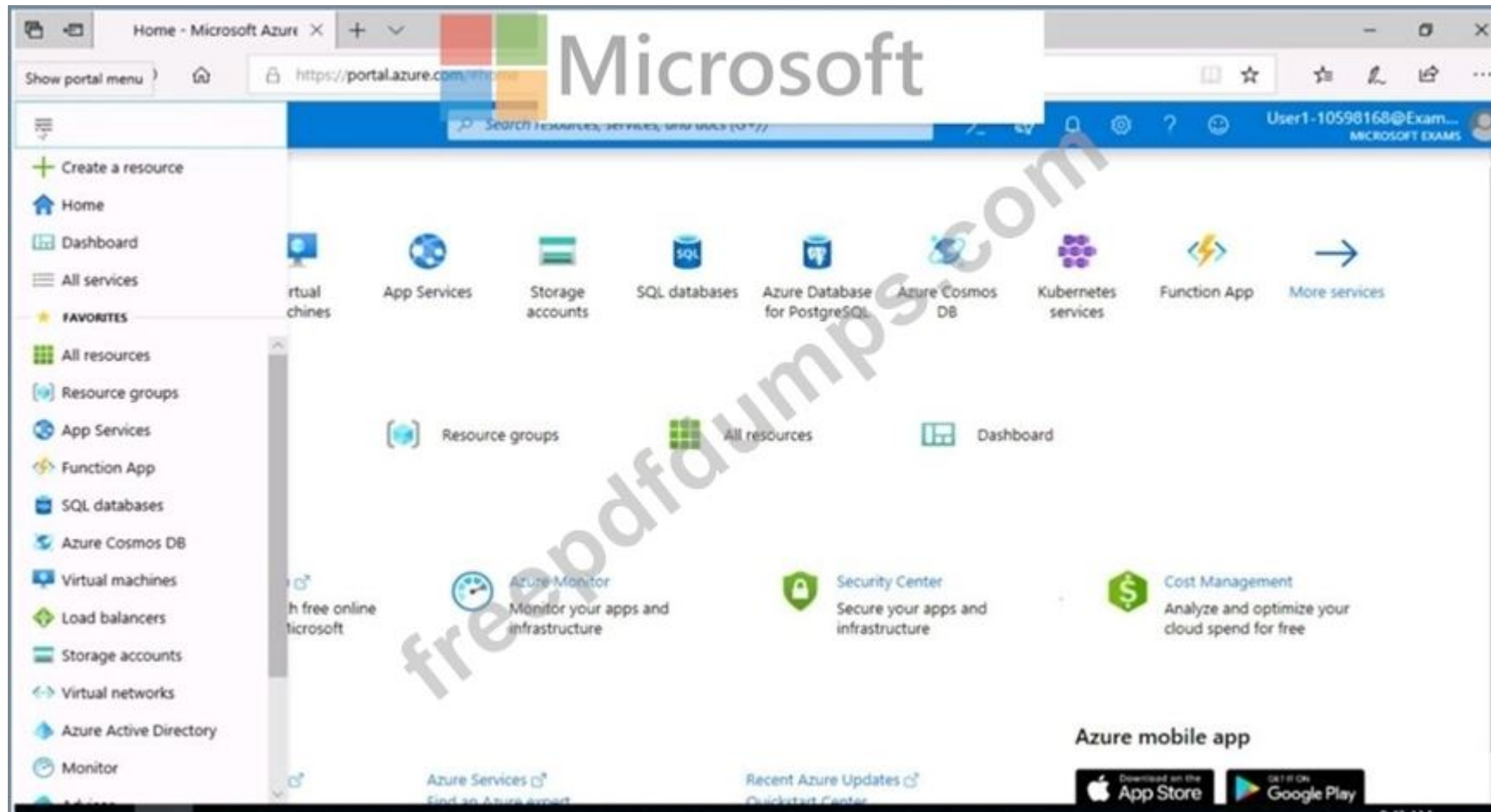
Azure Services

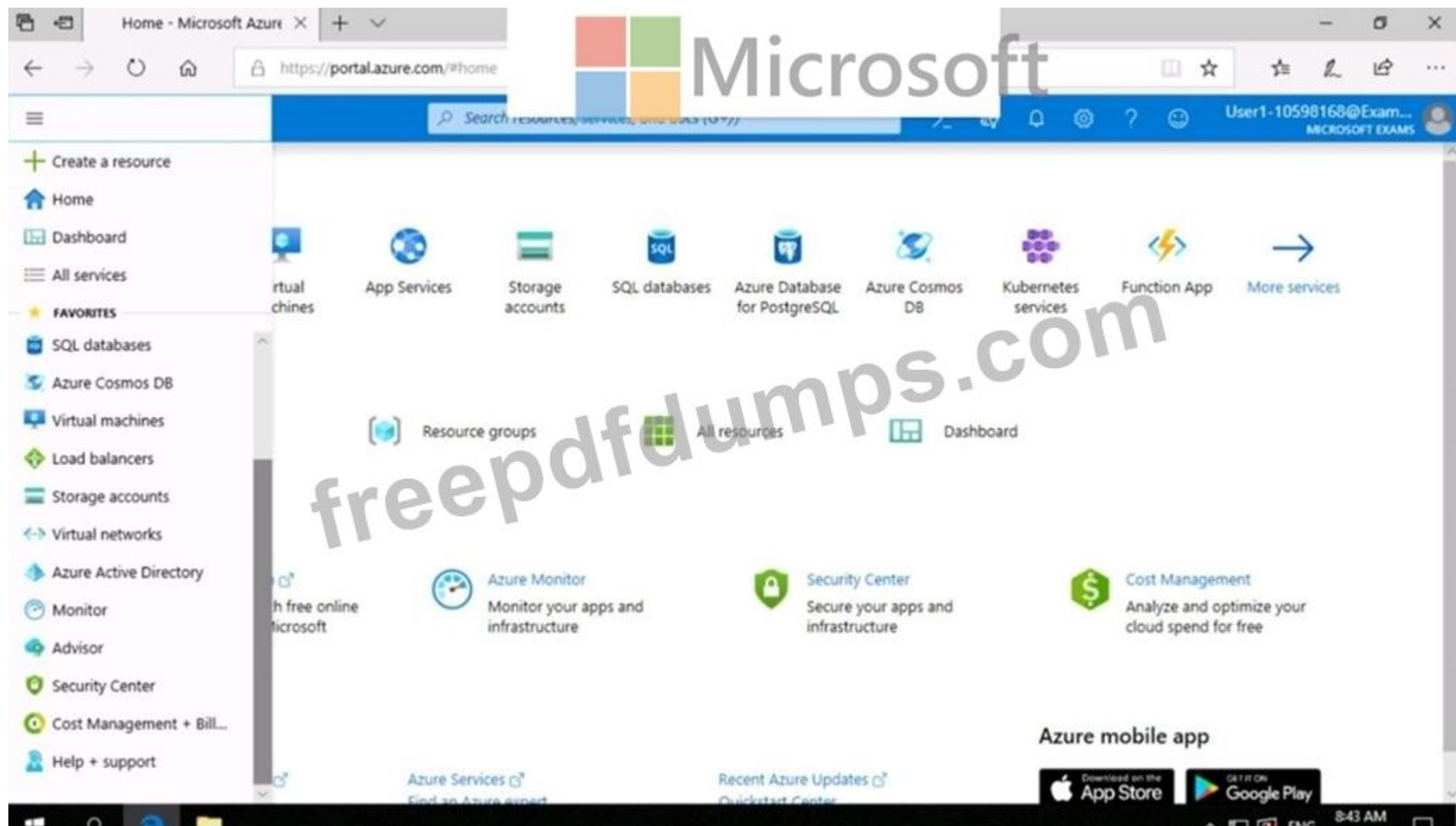
Recent Azure Updates

Azure mobile app

Download on the App Store

GET IT ON Google Play





You need to create a new Azure Active Directory (Azure AD) directory named 10598168.onmicrosoft.com.

The new directory must contain a user named user1@10598168.onmicrosoft.com who is configured to sign in by using Azure Multi-Factor Authentication (MFA).

To complete this task, sign in to the Azure portal.

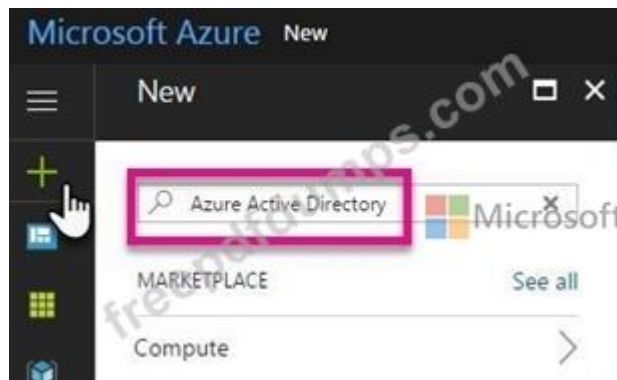
Answer:

See the explanation below.

Explanation

Step 1: Create an Azure Active Directory tenant

1. Browse to the Azure portal and sign in with an account that has an Azure subscription.
2. Select the plus icon (+) and search for Azure Active Directory.



3. Select Azure Active Directory in the search results.



4. Select Create.

5. Provide an Organization name and an Initial domain name (10598168). Then select Create. Your directory

Create directory

* Organization name ⓘ
 ✓

* Initial domain name ⓘ
 ✓
 contosodirect.onmicrosoft.com

Country or region ⓘ
 ▼

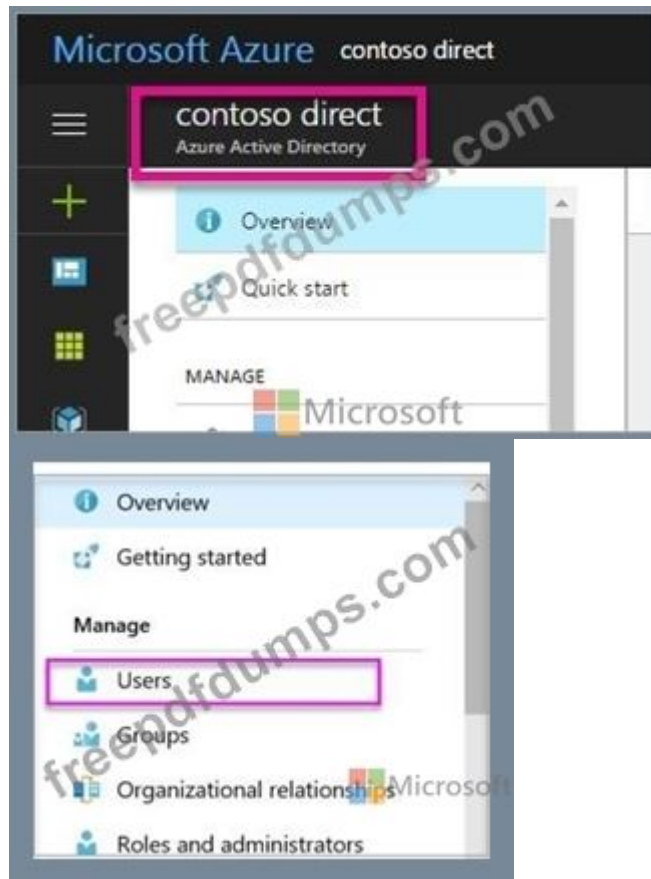
i Directory creation will take about one minute.

is created.

6. After directory creation is complete, select the information box to manage your new directory. Next, you're going to add tenant users.

Step 2: Create an Azure Active Directory tenant user

7. In the Azure portal, make sure you are on the Azure Active Directory fly out.



8. Under Manage, select Users.

9. Select All users and then select + New user.

10. Provide a Name and User name (user1) for the regular user tenant You can also show the temporary password. When you're done, select Create.

Name: user1

User name: user1@10598168.onmicrosoft.com

User
contoso direct

* Name 1
PBI Embed ✓

* User name 2
pbiembed@contosodirect.onmicrosoft.com ✓

Profile
Not configured

Properties
Microsoft
Default >

Groups
0 groups selected >

Directory role 3
User >

Password

☐ Show Password

Reference:

<https://docs.microsoft.com/en-us/power-bi/developer/create-an-azure-active-directory-tenant>

NEW QUESTION: 313

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	



Microsoft

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	

Reference:

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

NEW QUESTION: 314

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>

NEW QUESTION: 315

You have an Azure Active Directory (Azure AD) 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
User3	Group1	Disabled

You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings:

Assignments: Include Group1, exclude Group2

Conditions: Sign-in risk level: Medium and above

Access Allow access, Require multi-factor authentication

You need to identify what occurs when the users sign in to Azure AD.

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.

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

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

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

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

When User3 signs in from an infected device, the user will:

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

Answer:

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

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

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

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

When User3 signs in from an infected device, the user will:

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

Reference:

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

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies>

NEW QUESTION: 316

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.)

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

PS C:\> _
```

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.	☒	☐

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 (517 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 317

You have an Azure subscription that contains a user named Admin1 and a resource group named RG1.

In Azure Monitor, you create the alert rules shown in the following table.

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

Admin1 performs the following actions on RG1:

Adds a virtual network named VNET1

Adds a Delete lock named Lock1

Which rules will trigger an alert as a result of the actions of Admin1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Adding VNET1:

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

Adding Lock1:

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

Answer:

Adding VNET1:

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

Adding Lock1:

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

NEW QUESTION: 318

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

NEW QUESTION: 319

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

NEW QUESTION: 320

You have an Azure subscription that contains the following resources:

- * A virtual network named VNET1 that contains two subnets named Subnet1 and Subnet2.
- * A virtual machine named VM1 that has only a private IP address and connects to Subnet1.

You need to ensure that Remote Desktop connections can be established to VM1 from the internet.

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 a network security group (NSG).	
Create a network rule collection.	
Create a NAT rule collection.	
Create a new subnet.	
Deploy Azure Application Gateway.	
Deploy Azure Firewall.	

Answer:

Actions	Answer Area
Configure a network security group (NSG).	
Create a network rule collection.	
Create a NAT rule collection.	
Create a new subnet.	Create a new subnet.
Deploy Azure Application Gateway.	Deploy Azure Firewall.
Deploy Azure Firewall.	Create a NAT rule collection.

Explanation

Create a new subnet.
Deploy Azure Firewall.
Create a NAT rule collection.

NEW QUESTION: 321

You have an Azure subscription.

You need to create and deploy an Azure policy that meets the following requirements:

When a new virtual machine is deployed, automatically install a custom security extension.

Trigger an autogenerated remediation task for non-compliant virtual machines to install the extension.

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

NOTE: Each correct selection is worth one point.

Definition effect: Microsoft

- Append
- DeployIfNotExists
- EnforceOPAConstraint
- EnforceRegoPolicy
- Modify

Assignment remediation task:

- A managed identity that has the Contributor role
- A managed identity that has the User Access Administrator role
- A service principal that has the Contributor role
- A service principal that has the User Access Administrator role

Answer:

Definition effect: Microsoft

- Append
- DeployIfNotExists
- EnforceOPAConstraint
- EnforceRegoPolicy
- Modify

Assignment remediation task:

- A managed identity that has the Contributor role
- A managed identity that has the User Access Administrator role
- A service principal that has the Contributor role
- A service principal that has the User Access Administrator role

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources>

NEW QUESTION: 322

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](#))

Explanation/Reference:

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

NEW QUESTION: 323

You plan to use Azure Sentinel to create an analytic rule that will detect suspicious threats and automate responses.

Which components are required for the rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Detect suspicious threats:

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

Automate responses:

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



Answer:

Detect suspicious threats:

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

Automate responses:

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



Reference:

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

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

NEW QUESTION: 324

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')]" : "[variable('var1')]",
      "AzureADApplicationID" : "[variable('var1')]",
      "WorkspaceID" : "[variable('var1')]",
      "WorkspaceName" : "[variable('var1')]",
      "WorkspaceURL" : "[variable('var1')]"
    },
    "protectedSettings" : {
      "[variable('var2')]" : "[variable('var2')]",
      "AzureADApplicationSecret" : "[variable('var2')]",
      "StorageAccountKey" : "[variable('var2')]",
      "WorkspaceID" : "[variable('var2')]",
      "WorkspaceKey" : "[variable('var2')]"
    }
  }
}

```

Explanation:

```

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

```

References:

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

NEW QUESTION: 325

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

Name	Type
RG1	Resource group
VM1	Virtual machine

You perform the following tasks:

Create a managed identity named Managed1.

Create a Microsoft 365 group named Group1.

You need to identify which service principals were created and which identities can be assigned the Reader role for RG1. What should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Service Principals: Managed1, VM1, and App1 only

Identities: Managed1 and VM1 only

Answer:

Answer Area

Service Principals: Managed1, VM1, and App1 only

Identities: Managed1 and VM1 only

NEW QUESTION: 326

You need to create Role1 to meet the platform protection requirements.

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

NOTE: Each correct selection is worth one point.

```
(
  "Name" | "Role1",
  "Id" | "11111111-1111-1111-1111-111111111111",
  "IsCustom" : true,
  "Description": "VM storage operator",
  "Actions" : [
    {
      "Microsoft.Compute/disks/*",
      "Microsoft.Resources/storageAccounts/*",
      "Microsoft.Storage/virtualMachines/disks/*"
    }
  ],
  "NotActions": [
  ],
  "AssignableScopes" : [
  ]
)
```

Answer:

Answer Area



Microsoft

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

Storage1 only

Storage2 only

Storage1 and Storage2 only

Storage1, Storage2, and Storage3

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

Analytics1 only

Analytics1 and Analytics2 only

Analytics1 and Analytics3 only

Analytics1, Analytics2, and Analytics3

Explanation

```

{
  "Name" | "Role1",
  "Id" | "11111111-1111-1111-1111-111111111111",
  "IsCustom" : true,
  "Description": "VM storage operator"
  "Actions" : [

    {
      "Microsoft.Compute/ disks/*",
      "Microsoft.Resources/ storageAccounts/*",
      "Microsoft.Storage/ virtualMachines/disks/*",
    },
    {
      "NotActions": [
      ],
      "AssignableScopes" : [
      ]
    }
  ],
  "AssignableScopes" : [
  ]
},

```

Scenario: A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.

Azure RBAC template managed disks "Microsoft.Storage/"

References:

<https://blogs.msdn.microsoft.com/azureedu/2017/02/11/new-managed-disk-storage-option-for-your-azure-vms/>

NEW QUESTION: 327

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: 

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:

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: 328

You need to configure an access review. The review will be assigned to a new collection of reviews and reviewed by resource owners.

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
Create an access review program.	
Set Reviewers to Selected users.	
Create an access review audit.	
Create an access review control.	
Set Reviewers to Group owners.	
Set Reviewers to Members.	

Microsoft

Answer:

Answer Area
Create an access review program
Create an access review control
Set Reviewers to Group owners

Microsoft

1 - Create an access review program

2 - Create an access review control

3 - Set Reviewers to Group owners

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: 329

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:

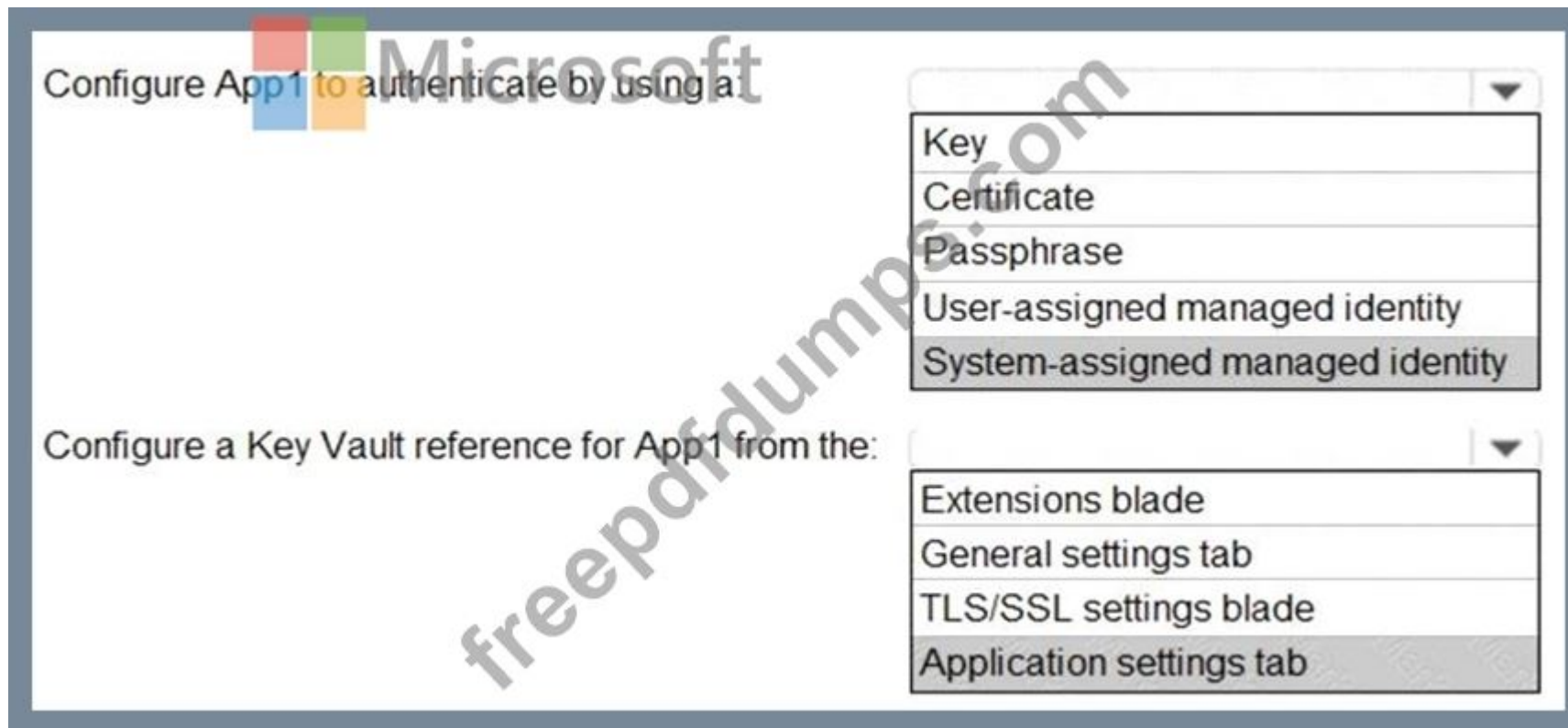
Configure App1 to authenticate by using a:

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:



Reference:

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

NEW QUESTION: 330

You have an Azure subscription that contains the following resources:

- * An Azure key vault
- * An Azure SQL database named Database1
- * Two Azure App Service web apps named AppSrv1 and AppSrv2 that are configured to use system-assigned managed identities and access Database1 You need to implement an encryption solution for Database1 that meets the following requirements:
- * The data in a column named Discount in Database1 must be encrypted so that only AppSrv1 can decrypt the data.
- * AppSrv1 and AppSrv2 must be authorized by using managed identities to obtain cryptographic keys.

How should you configure the encryption settings for Database1 To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point



Answer:

Statements	Yes	No
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	☐	☐
Remote Desktop access to VM5 is blocked.	☐	☐
An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.	☐	☐

Explanation

Text Description automatically generated with medium confidence

To configure the encryption of Database1:

▼

☐ Always Encrypted by using Azure Key Vault.
 ☐ Always Encrypted by using the Windows Certificate Store.
 ☐ Transparent Data Encryption (TDE) by using Azure Key Vault integration.
 ☐ Transparent Data Encryption (TDE) by using Bring Your Own Key (BYOK).

To obtain the cryptographic keys:

▼

☐ Create an access policy in Azure Key Vault.
 ☐ Generate a key on an HSM device.
 ☐ Import App Service certificates to AppSrv1 and AppSrv2.
 ☐ Register an enterprise application in Azure AD.

Reference:

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

NEW QUESTION: 331

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains a user named User1.

You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains an Azure Storage account named storage1. Storage1 contains an Azure file share named share1.

Currently, the domain and the tenant are not integrated.

You need to ensure that User1 can access share1 by using his domain credentials.

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

Create a private link to storage1.

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

Implement Azure AD Connect.

Create a service endpoint to storage1.

Assign share-level permissions for share1.

Answer Area

Answer:

Explanation



Reference:

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

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 (517 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 332

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

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: 333

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)

Explanation

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

Topic 1, Litware, inc

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

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question on this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next sections of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question on this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

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

Existing Environment

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

Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices.

Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.

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

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

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

Azure Security Center is set to the Free tier.

Planned changes

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

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

Litware identifies the following identity and access requirements:

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

Platform Protection Requirements

Litware identifies the following platform protection requirements:

- * Microsoft Antimalware must be installed on the virtual machines in Resource Group1.
- * The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.
- * Azure AD users must be to authenticate to AKS1 by using their Azure AD credentials.

* Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.

* A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.

Security Operations Requirements

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

NEW QUESTION: 334

You plan to use Azure Sentinel to create an analytic rule that will detect suspicious threats and automate responses.

Which components are required for the rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

detect suspicious threats

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

Automate responses:

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

Answer:

Detect suspicious threats:

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

Automate responses:

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

Reference:

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

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

NEW QUESTION: 335

You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016.

You need to implement a policy to ensure that each virtual machine has a custom antimalware virtual machine extension installed.

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

NOTE: Each correct selection is worth one point.

 Microsoft

```
{
  "if" : {
    "allOf": [
      {
        "field" : "type",
        "equals": "Microsoft.Compute/virtualMachines"
      }
    ],
    "field" : "Microsoft.Compute/imageSKU",
    "equals" : "2016-Datacenter",
  },
  "then" : {
    "effect" : "
    Append
    Deny
    DeployIfNotExists
  ",
  },
  "details" : {
    "type" : "Microsoft.GuestConfiguration/guestConfigurationAssignments",
    "roleDefinitionsIds" : [
      "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
    ],
    "name" : "customExtension",
    "deployment" : {
      "properties" : {
        "mode": "incremental",
        "parameters" : {
          "
          existenceCondition
          resources
          template
        "
      }
    }
  }
}
```

Answer:

```

{
  "if" : {
    "allOf": [
      {
        "field" : "type",
        "equals": "Microsoft.Compute/virtualMachines"
      }
    ],
    "then" : {
      "effect" : "
    },
    "details" : {
      "type" : "Microsoft.GuestConfiguration/guestConfigurationAssignments",
      "roleDefinitionsIds" : [
        "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
      ],
      "name" : "customExtension",
      "deployment" : {
        "properties" : {
          "mode": "incremental",
          "parameters" : {
            "
          },
          "
        }
      }
    }
  }
}

```

Append
Deny
DeployIfNotExists

existenceCondition
resources
template



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

NEW QUESTION: 336

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](#))

Explanation

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: 337

You 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.	☒	☐

NEW QUESTION: 338

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.Authorization
Microsoft.Resources
Microsoft.Support

Assignable scope:

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

Answer:

Resource provider:

Microsoft.Authorization
Microsoft.Resources
Microsoft.Support

Assignable scope:

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

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: 339

You suspect that users are attempting to sign in to resources to which they have no access.

You need to create an Azure Log Analytics query to identify failed user sign-in attempts from the last three days. The results must only show users who had more than five failed sign-in attempts.

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

NOTE: Each correct selection is worth one point.

```

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

```

Dropdown menu options: ActivityID, DataType, EventID, QuantityUnit

Dropdown menu value: ==4625

```

Summarize failed_login_attempts=

```

Dropdown menu options: Count(), Countif(), Makeset(), Split()

```

latest_failed_login=arg_max(TimeGenerated by Account

```

Answer:

```

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

```

Dropdown menu options: ActivityID, DataType, EventID, QuantityUnit

Dropdown menu value: ==4625

```

| Summarize failed_login_attempts=

```

Dropdown menu options: Count(), Countif(), Makeset(), Split()

```

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

```

Explanation

```

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

| Summarize failed_login_attempts=
    Count(),
    Countif(),
    Makeset(),
    Split(),

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

```

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

```

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

```

References:

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

NEW QUESTION: 340

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

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.	☐	☒

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal>

NEW QUESTION: 341

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

Name	Region	Description
HubVNet	East US	HubVNet is a virtual network connected to the on-premises network by using a site-to-site VPN that has BGP route propagation enabled. HubVNet contains a subnet named HubVNetSubnet0.
SpokeVNet	East US	SpokeVNet is a virtual network connected to HubVNet by using VNet peering. SpokeVNet contains a subnet named SpokeVNetSubnet0.

The Azure virtual machines on SpokeVNetSubnet0 can communicate with the computers on the on-premises network.

You plan to deploy an Azure firewall to HubVNet.

You create the following two routing tables:

RT1: Includes a user-defined route that points to the private IP address of the Azure firewall as a next hop address RT2: Disables BGP route propagation and defines the private IP address of the Azure firewall as the default gateway You need to ensure that traffic between SpokeVNetSubnet0 and the on-premises network flows through the Azure firewall.

To which subnet should you associate each route table? To answer, drag the appropriate subnets to the correct route tables. Each subnet 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.

Subnets

Answer Area

Azure FirewallSubnet

RT1:

GatewaySubnet

RT2:

HubVNetSubnet0

Answer:

Subnets

Azure FirewallSubnet

GatewaySubnet

HubVNetSubnet0

Answer Area

RT1:

GatewaySubnet

RT2:

HubVNetSubnet0

Explanation

Answer Area

RT1:

GatewaySubnet

RT2:

HubVNetSubnet0

Microsoft

NEW QUESTION: 342

You assign User8 the Owner role for RG4, RG5, and RG6.

In which resource groups can User8 create virtual networks and NSGs? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

User8 can create virtual networks in:

RG4 only

RG6 only

RG4 and RG6 only

RG4, RG5, and RG6

User8 can create NSGs in:

RG4 only

RG4 and RG5 only

RG4 and RG6 only

RG4, RG5, and RG6

Microsoft

Answer:

User8 can create virtual networks in:

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

User8 can create NSGs in:

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

NEW QUESTION: 343

You have the Azure key vaults shown in the following table.

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

KV1 stores a secret named Secret1 and a key for a managed storage account named Key1.

You back up Secret1 and Key1.

To which key vaults can you restore each backup? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

You can restore the Secret1 backup to:

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

You can restore the Key1 backup to:

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

Answer:

You can restore the Secret1 backup to:

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

You can restore the Key1 backup to:

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

NEW QUESTION: 344

You company has an Azure subscription named Sub1. Sub1 contains an Azure web app named WebApp1 that uses Azure Application Insights. WebApp1 requires users to authenticate by using OAuth 2.0 client secrets.

Developers at the company plan to create a multi-step web test app that preforms synthetic transactions emulating user traffic to Web App1.

You need to ensure that web tests can run unattended.

What should you do first?

- A. In Microsoft Visual Studio, modify the .webtest file.
- B. Upload the .webtest file to Application Insights.
- C. Register the web test app in Azure AD.
- D. Add a plug-in to the web test app.

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

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/availability-multistep>

NEW QUESTION: 345

You have an Azure key vault named KeyVault1 that contains the items shown in the following table.

Name	Type
Item1	Key
Item2	Secret
Policy1	Access policy

In KeyVault, the following events occur in sequence:

Item1 is deleted

Administrator enables soft delete

Item2 and Policy1 are deleted.

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 recover Policy1.	☐	☐
You can add a new key named Item1.	☐	☐
You can add a new secret named Item2.	☐	☐

Answer:

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

NEW QUESTION: 346

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

Name	Pattern	Case sensitivity
Condition1	White	On
Condition2	Black	Off

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

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

You need to identify how Azure Information Protection will label files.

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

NOTE: Each correct selection is worth one point.

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



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

▼

No label

Label1 only

Label2 only

Label1 and Label2

▼

No label

Label1 only

Label2 only

Label1 and Label2

Answer:

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

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

No label
Label1 only
Label2 only
Label1 and Label2

No label
Label1 only
Label2 only
Label1 and Label2

Reference:

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

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 (517 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 347

You need to ensure that the audit logs from the SQLdb1 Azure SQL database are stored in the WS11641655 Azure Log Analytics workspace.

To complete this task, sign in to the Azure portal and modify the Azure resources.

Answer:

1. In the Azure portal, type SQL in the search box, select SQL databases from the search results then select SQLdb1. Alternatively, browse to SQL databases in the left navigation pane.
2. In the properties of SQLdb1, scroll down to the Security section and select Auditing.
3. Turn auditing on if it isn't already, tick the Log Analytics checkbox then click on Configure.

Auditing ⓘ

☒ ON ☐ OFF

Audit log destination (choose at least one):

☐ Storage

☒ Log Analytics (Preview) 

Log Analytics details

[Configure](#)

☐ Event Hub (Preview)

4. Select the WS11641655 Azure Log Analytics workspace.
5. Click Save to save the changes.

NEW QUESTION: 348

You have an Azure SQL database.

You implement Always Encrypted.

You need to ensure that application developers can retrieve and decrypt data in the database.

What information should you provide to the developers? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a stored access policy
- B. a shared access signature (SAS)
- C. the column encryption key
- D. user credentials
- E. the column master key

Answer: C,E (LEAVE A REPLY)

Always Encrypted uses two types of keys: column encryption keys and column master keys. A column encryption key is used to encrypt data in an encrypted column. A column master key is a key-protecting key that encrypts one or more column encryption keys.

References:

<https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine>

NEW QUESTION: 349

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:

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.	☒	☐

NEW QUESTION: 350

You have a hybrid configuration of Azure Active Directory (Azure AD). You have an Azure SQL Database instance that is configured to support Azure AD authentication. Database developers must connect to the database instance and authenticate by using their on-premises Active Directory account. You need to ensure that developers can connect to the instance by using Microsoft SQL Server Management Studio. The solution must minimize authentication prompts. Which authentication method should you recommend?

- A. Active Directory - Password
- B. Active Directory - Universal with MFA support
- C. SQL Server Authentication
- D. Active Directory - Integrated

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

Use Active Directory password authentication when connecting with an Azure AD principal name using the Azure AD managed domain.

Use this method to authenticate to SQL DB/DW with Azure AD for native or federated Azure AD users. A native user is one explicitly created in Azure AD and being authenticated using user name and password, while a federated user is a Windows user whose domain is federated with Azure AD. The latter method (using user & password) can be used when a user wants to use their windows credential, but their local machine is not joined with the domain (for example, using a remote access). In this case, a Windows user can indicate their domain account and password and can authenticate to SQL DB/DW using federated credentials.

Incorrect Answers:

D: Use Active Directory integrated authentication if you are logged in to Windows using your Azure Active Directory credentials from a federated domain.

References:

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure>

NEW QUESTION: 351

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: (SHOW ANSWER)

References:

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

NEW QUESTION: 352

You have an Azure subscription that contains a user named Admin1 and a resource group named RG1.

In Azure Monitor, you create the alert rules shown in the following table.

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

Admin1 performs the following actions on RG1:

Adds a virtual network named VNET1

Adds a Delete lock named Lock1

Which rules will trigger an alert as a result of the actions of Admin1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Adding VNET1:

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

Adding Lock1:

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

Answer:

Adding VNET1:	<table border="1"><tr><td>Rule2 only</td></tr><tr><td>Rule4 only</td></tr><tr><td>Rule2 and Rule 4 only</td></tr><tr><td>Rule3 and Rule 4 only</td></tr><tr><td>Rule1, Rule2, Rule3 and Rule 4</td></tr></table>	Rule2 only	Rule4 only	Rule2 and Rule 4 only	Rule3 and Rule 4 only	Rule1, Rule2, Rule3 and Rule 4
Rule2 only						
Rule4 only						
Rule2 and Rule 4 only						
Rule3 and Rule 4 only						
Rule1, Rule2, Rule3 and Rule 4						
Adding Lock1:	<table border="1"><tr><td>Rule2 only</td></tr><tr><td>Rule4 only</td></tr><tr><td>Rule2 and Rule 4 only</td></tr><tr><td>Rule3 and Rule 4 only</td></tr><tr><td>Rule1, Rule2, Rule3 and Rule 4</td></tr></table>	Rule2 only	Rule4 only	Rule2 and Rule 4 only	Rule3 and Rule 4 only	Rule1, Rule2, Rule3 and Rule 4
Rule2 only						
Rule4 only						
Rule2 and Rule 4 only						
Rule3 and Rule 4 only						
Rule1, Rule2, Rule3 and Rule 4						

Explanation:

Adding VNET1:

Rule2 only

Rule4 only

Rule2 and Rule 4 only

Rule3 and Rule 4 only

Rule1, Rule2, Rule3 and Rule 4

Adding Lock1:

Rule2 only

Rule4 only

Rule2 and Rule 4 only

Rule3 and Rule 4 only

Rule1, Rule2, Rule3 and Rule 4

NEW QUESTION: 353

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

Name	Pattern	Case sensitivity
Condition1	White	On
Condition2	Black	Off

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

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

You need to identify how Azure Information Protection will label files.

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

NOTE: Each correct selection is worth one point.

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



	▼
No label	
Label1 only	
Label2 only	
Label1 and Label2	

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

	▼
No label	
Label1 only	
Label2 only	
Label1 and Label2	

Answer:

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

	▼
No label	
Label1 only	
Label2 only	
Label1 and Label2	

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

	▼
No label	
Label1 only	
Label2 only	
Label1 and Label2	

Reference:

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

NEW QUESTION: 354

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

Name	Pattern	Case sensitivity
Condition1	White	On
Condition2	Black	Off

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

Name	Applies to	Use label	Set the default label
Global	<i>Not applicable</i>	<i>None</i>	None
Policy1	User1	Label1	None
Policy2	User1	Label2	None

You need to identify how Azure Information Protection will label files.

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

NOTE: Each correct selection is worth one point.

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

No label
Label1 only
Label2 only
Label1 and Label2

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

No label
Label1 only
Label2 only
Label1 and Label2



Microsoft

Answer:

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

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

Explanation

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

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

Box 1: Label 2 only

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

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

Box 2: No Label

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

References:

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

NEW QUESTION: 355

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?

- 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)

Section: [none]

Explanation:

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

Reference:

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

NEW QUESTION: 356

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

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

Which users can enable Azure AD Privileged Identity Management (PIM)?

- A. User2 and User3 only
- B. User1 and User2 only
- C. User2 only
- D. User1 only

Answer: B (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 357

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: 358

Lab Task

Task 2

You need to ensure that the events in the NetworkSecurityGroupRuleCounter log of the VNET01-Subnet0-NSG network security group (NSG) are stored in the logs31330471 Azure Storage account for 30 days.

Answer:

see the task answer with step by step below:

Enable diagnostic resource logging for the NSG. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to select the Rule counter category under Logs and choose the logs31330471 storage account as the destination.

Configure the retention policy for the storage account to keep the logs for 30 days. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to specify the days parameter as 30 for the Set-AzStorageServiceProperty cmdlet or the az storage logging update command. View and analyze the logs in the storage account. You can use any tool that can read JSON files, such as Azure Storage Explorer or Visual Studio Code. You can also export the logs to any visualization tool, SIEM solution, or IDS of your choice

NEW QUESTION: 359

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

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

Explanation

Permission that must be granted to users on VM:

	▼
Read	
Update	
View	
Write	

TCP port that must be allowed:

	▼
22	
25	
3389	
5986	

NEW QUESTION: 360

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:

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: 361

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.

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		

Reference:

<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 (517 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 362

You need to ensure that User2 can implement PIM.

What should you do first?

- A. Assign User2 the Global administrator role.
- B. Configure authentication methods for contoso.com.
- C. Configure the identity secure score for contoso.com.
- D. Enable multi-factor authentication (MFA) for User2.

Answer: A (LEAVE A REPLY)

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

1. Sign in to the Azure portal as a Global Administrator of your directory.

You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com), to enable PIM for a directory.

Scenario: Technical requirements include: Enable Azure AD Privileged Identity Management (PIM) for contoso.com References:

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-started> Manage identity and access Question Set 3

NEW QUESTION: 363

You have 20 Azure subscriptions and a security group named Group1. The subscriptions are children of the root management group.

Each subscription contains a resource group named RG1.

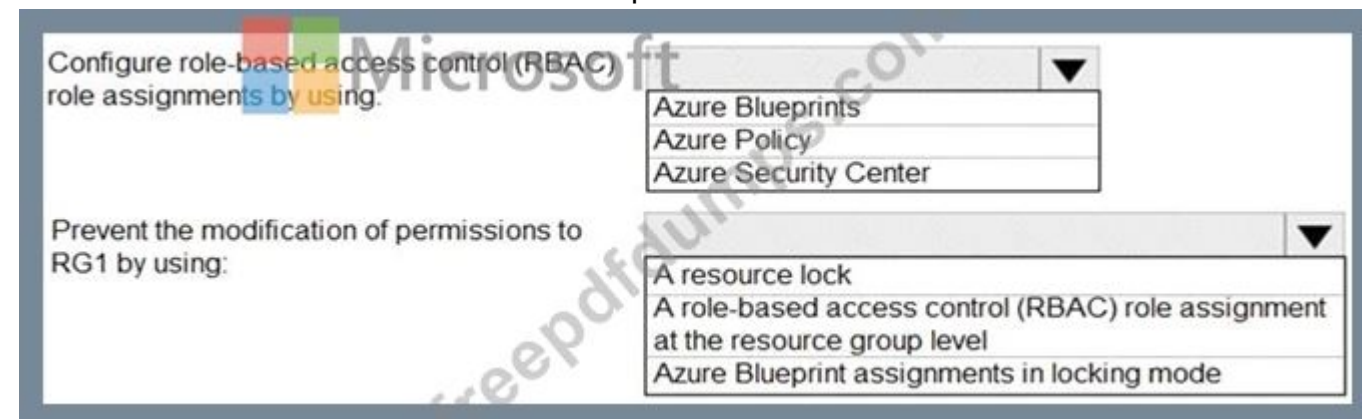
You need to ensure that for each subscription RG1 meets the following requirements:

The members of Group1 are assigned the Owner role.

The modification of permissions to RG1 is prevented.

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

NOTE: Each correct selection is worth one point.



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

- Azure Blueprints
- Azure Policy
- Azure Security Center

Prevent the modification of permissions to RG1 by using:

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

Answer:

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

- Azure Blueprints
- Azure Policy
- Azure Security Center

Prevent the modification of permissions to RG1 by using:

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

Explanation:

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

- Azure Blueprints
- Azure Policy
- Azure Security Center

Prevent the modification of permissions to RG1 by using:

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

NEW QUESTION: 364

You need to ensure that the Azure AD application registration and consent configurations meet the identity and access requirements.

What should you use in the Azure portal? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

To configure the registration settings:

- Azure AD – User settings
- Azure AD – App registrations settings
- Enterprise Applications – User settings

To configure the consent settings:

- Azure AD – User settings
- Azure AD – App registrations settings
- Enterprise Applications – User settings

Answer:

To configure the registration settings:

▼

Azure AD – User settings

Azure AD – App registrations settings

Enterprise Applications – User settings

To configure the consent settings:

▼

Azure AD – User settings

Azure AD – App registrations settings

Enterprise Applications – User settings

Explanation

To configure the registration settings:

▼

Azure AD – User settings

Azure AD – App registrations settings

Enterprise Applications – User settings

To configure the consent settings:

▼

Azure AD – User settings

Azure AD – App registrations settings

Enterprise Applications – User settings

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent>

NEW QUESTION: 365

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

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: 366

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

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

From Azure Security Center, you turn on Auto Provisioning.
You deploy the virtual machines shown in the following table.

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

On which virtual machines is the Log Analytics agent installed?

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

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

Explanation

When automatic provisioning is On, Security Center provisions the Log Analytics Agent on all supported Azure VMs and any new ones that are created.

Supported Operating systems include: Ubuntu 14.04 LTS (x86/x64), 16.04 LTS (x86/x64), and 18.04 LTS (x64) and Windows Server 2008 R2, 2012, 2012 R2, 2016, version 1709 and 1803

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection>

NEW QUESTION: 367

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).	

freepdfdumps.com

Microsoft

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.	

NEW QUESTION: 368

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.

Reference:

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

NEW QUESTION: 369

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.

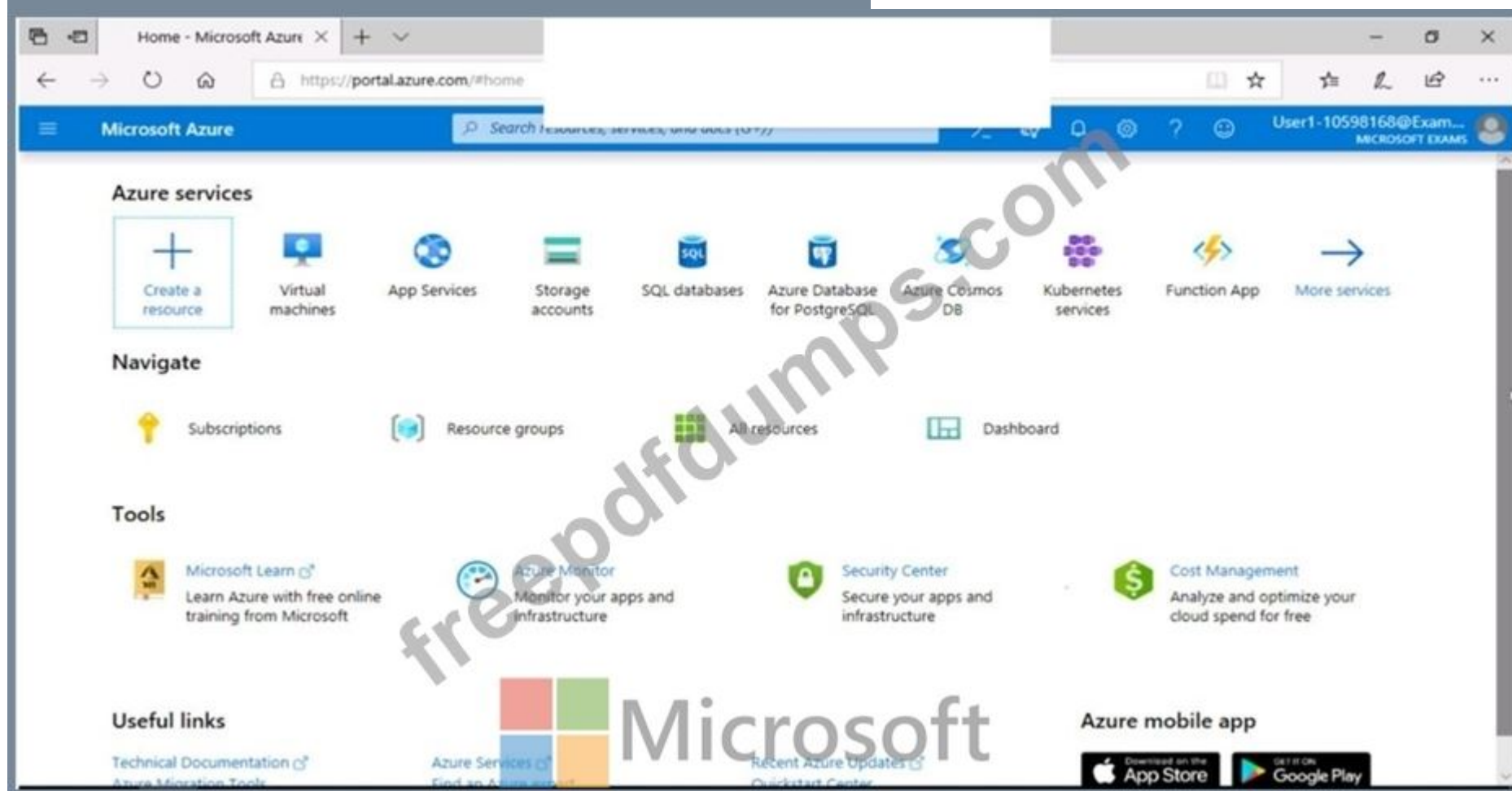
To enter your password, place your cursor in the Enter password box and click on the password below.

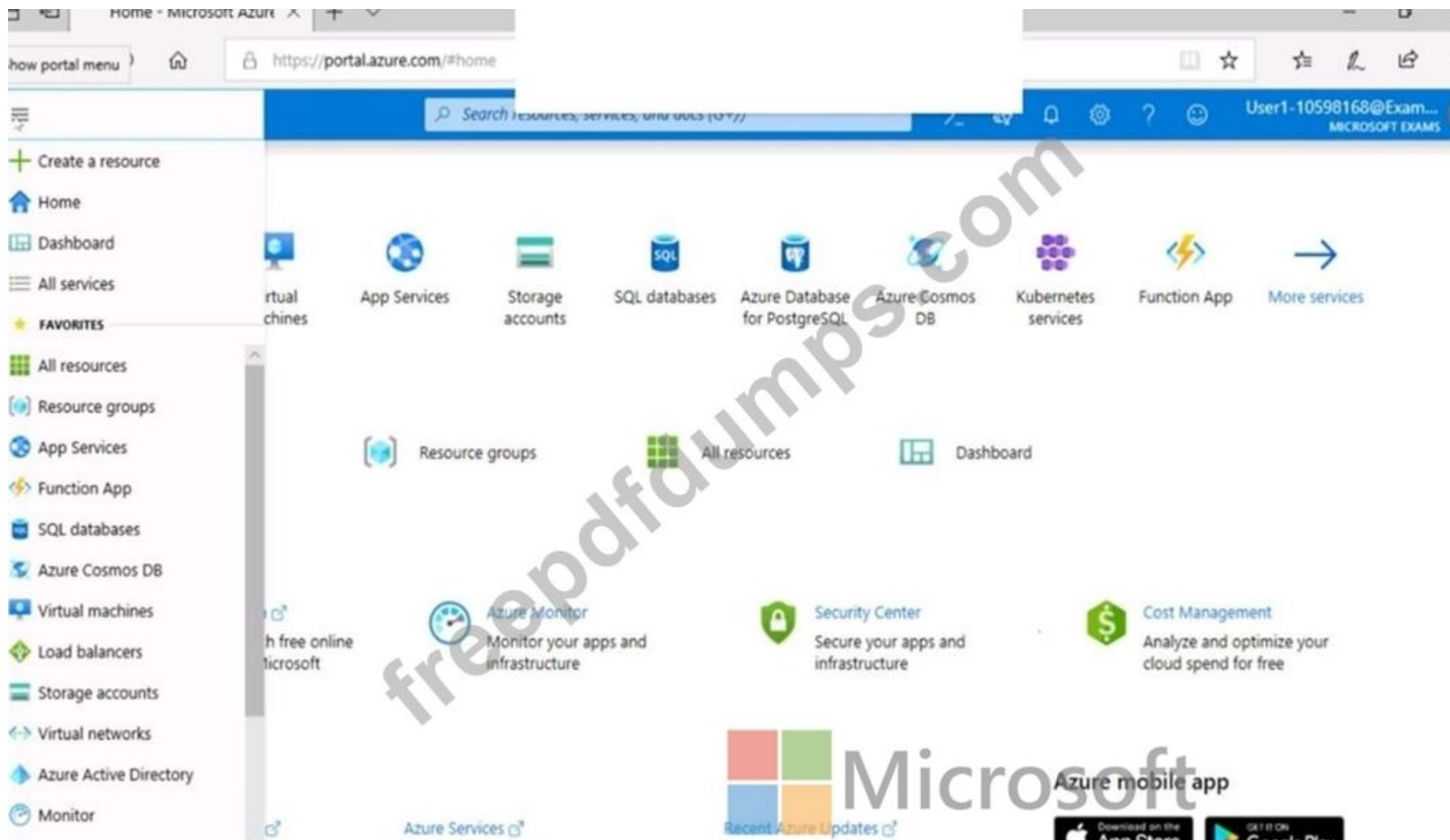
Azure Username: User1-10598168@ExamUsers.com

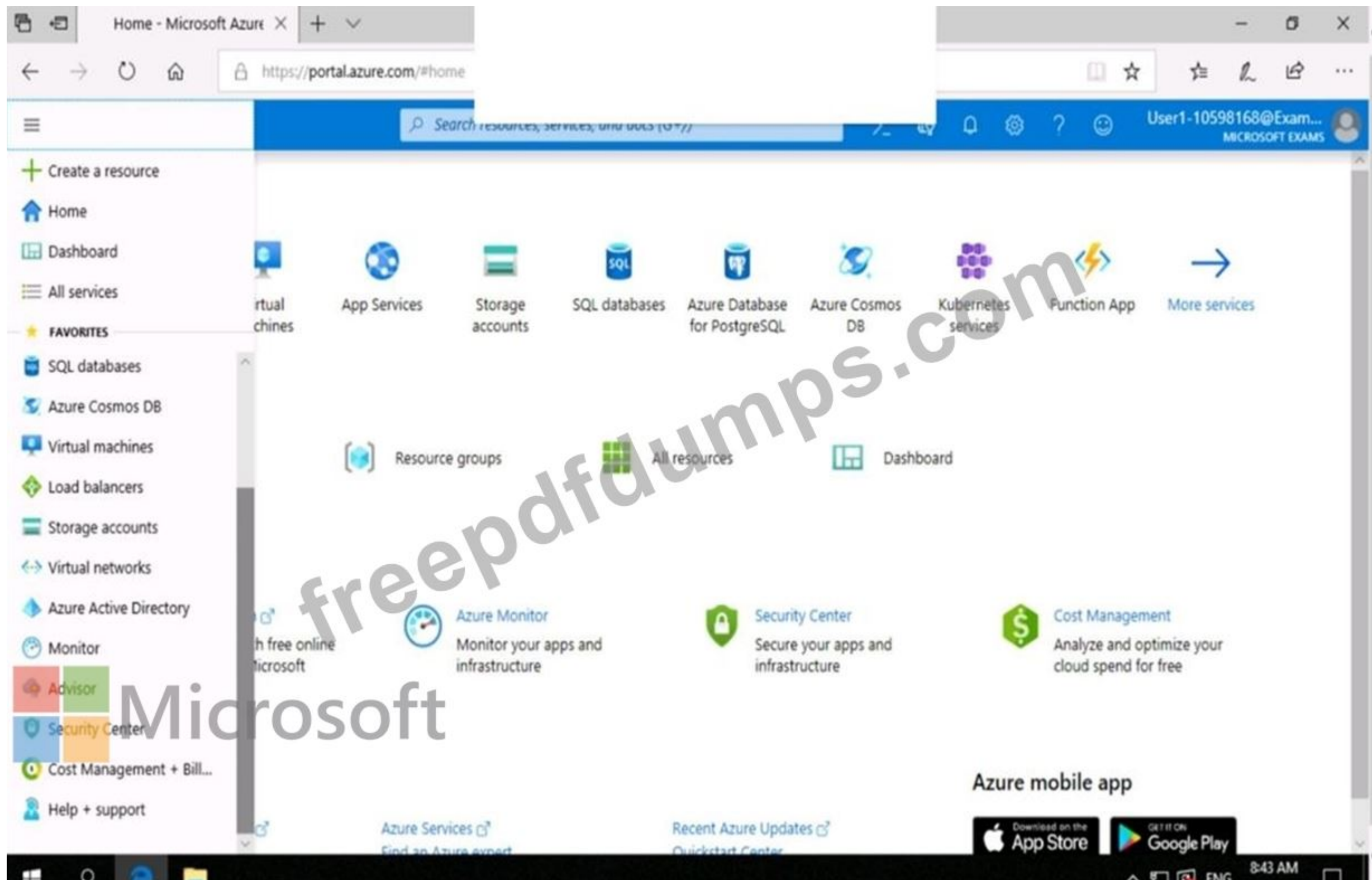
Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168







You need to ensure that only devices connected to a 131.107.0.0/16 subnet can access data in the rg1lod10598168 Azure Storage account.

To complete this task, sign in to the Azure portal.

Answer:

See the explanation below.

Explanation

Step 1:

1. In Azure portal go to the storage account you want to secure. Here: rg1lod10598168
2. Click on the settings menu called Firewalls and virtual networks.

- 3. To deny access by default, choose to allow access from Selected networks. To allow traffic from all networks, choose to allow access from All networks.
- 4. Click Save to apply your changes.

Step 2:

- 1. Go to the storage account you want to secure. Here: rg1lod10598168
- 2. Click on the settings menu called Firewalls and virtual networks.
- 3. Check that you've selected to allow access from Selected networks.
- 4. To grant access to a virtual network with a new network rule, under Virtual networks, click Add existing virtual network, select Virtual networks and Subnets options. Enter the 131.107.0.0/16 subnet and then click Add.

Note: When network rules are configured, only applications requesting data over the specified set of networks can access a storage account. You can limit access to your storage account to requests originating from specified IP addresses, IP ranges or from a list of subnets in an Azure Virtual Network (VNet).

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security>

NEW QUESTION: 370

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.)

```
PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet
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 State
-----
Allow  /subscriptions/a90c8c8f-d8bc-4112-abfb-dac4906573dd/resourceGroups/RG1/providers/Microsoft.Network/virtualNetworks/VNET1/subnets/Subnet1 Succeeded

PS C:\> _
```

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: 371

You have an Azure subscription that contains the following resources:

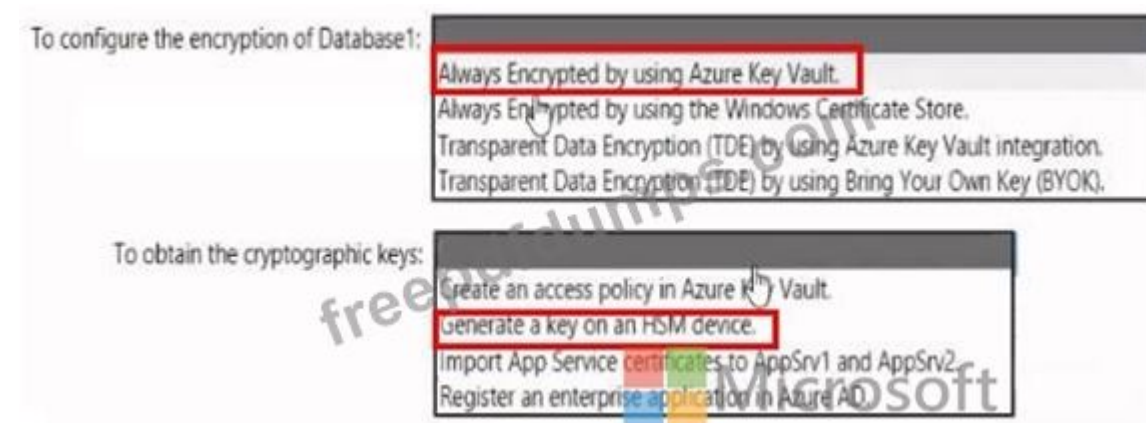
- * An Azure key vault
- * An Azure SQL database named Database1
- * Two Azure App Service web apps named AppSrv1 and AppSrv2 that are configured to use system-assigned managed identities and access Database1 You need to implement an encryption solution for Database1 that meets the following requirements:
- * The data in a column named Discount in Database1 must be encrypted so that only AppSrv1 can decrypt the data.
- * AppSrv1 and AppSrv2 must be authorized by using managed identities to obtain cryptographic keys.

How should you configure the encryption settings for Database1 To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point



Answer:



Reference:

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

NEW QUESTION: 372

You need to deploy Microsoft Antimalware to meet the platform protection requirements.

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

NOTE: Each correct selection is worth one point.

Create a custom policy definition that has effect set to:

▼

Append
Deny
DeployIfNotExists

Create a policy assignment and modify:



▼

The Create a Managed Identify setting
The exclusion settings
The scope

Answer:

Create a custom policy definition that has effect set to:



▼

Append
Deny
DeployIfNotExists

Create a policy assignment and modify:

▼

The Create a Managed Identify setting
The exclusion settings
The scope

Explanation

Create a custom policy definition that has effect set to:



▼

Append
Deny
DeployIfNotExists

Create a policy assignment and modify:

▼

The Create a Managed Identify setting
The exclusion settings
The scope

Scenario: Microsoft Antimalware must be installed on the virtual machines in RG1.

RG1 is a resource group that contains Vnet1, VM0, and VM1.

Box 1: DeployIfNotExists

DeployIfNotExists executes a template deployment when the condition is met.

Azure policy definition Antimalware

Reference:

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

NEW QUESTION: 373

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

The company develops a mobile application named App1. App1 uses the OAuth 2 implicit grant type to acquire Azure AD access tokens.

You need to register App1 in Azure AD.

What information should you obtain from the developer to register the application?

A. a redirect URI

B. a reply URL

C. a key

D. an application ID

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

For Native Applications you need to provide a Redirect URI, which Azure AD will use to return token responses.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/v1-protocols-oauth-code>

NEW QUESTION: 374

You have an Azure Storage account that contains a blob container named container1 and a client application named App1.

You need to enable App1 access to container1 by using Azure Active Directory (Azure AD) authentication.

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

NOTE: Each correct selection is worth one point.

From Azure AD:

- Register App1.
- Create an access package.
- Implement an application proxy.
- Modify the authentication methods.

From the storage account:

- Add a private endpoint.
- Regenerate the access key.
- Configure Access control (IAM).
- Generate a shared access signature (SAS).

Answer:

From Azure AD:

- Register App1.
- Create an access package.
- Implement an application proxy.
- Modify the authentication methods.

From the storage account:

- Add a private endpoint.
- Regenerate the access key.
- Configure Access control (IAM).
- Generate a shared access signature (SAS).

Explanation

From Azure AD:

- Register App1.
- Create an access package.
- Implement an application proxy.
- Modify the authentication methods.

From the storage account:

- Add a private endpoint.
- Regenerate the access key.
- Configure Access control (IAM).
- Generate a shared access signature (SAS).

Reference:

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

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/storage/common/storage-auth-aad-rbac-portal.>

NEW QUESTION: 375

You need to delegate the creation of RG2 and the management of permissions for RG1. Which users can perform each task? To answer select the appropriate options in the answer are a. NOTE:

Each correct selection is worth one point

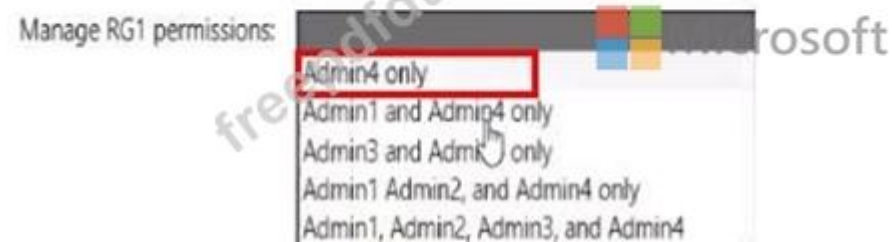
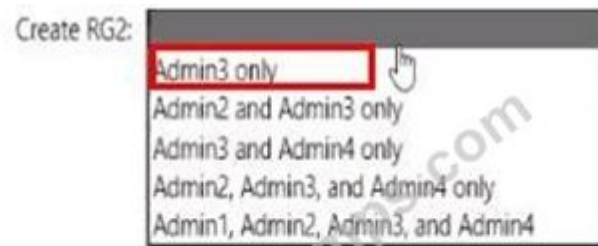
Create RG2:

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

Manage RG1 permissions:

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

Answer:



NEW QUESTION: 376

You have three Azure subscriptions and a user named User1.

You need to provide User1 with the ability to manage and view costs for the resources across all three subscriptions. The solution must use the principle of least privilege.

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.

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Actions

Create a management group.

Add the three subscriptions to the management group.

Assign User1 the Global administrator role.

Assign User1 the Owner role for the management group.

Assign User1 the Cost Management Contributor role for the management group.

Answer:

Answer Area

Assign User 1 the Cost Management Reader role for the management group.

Assign User 1 the Global administrator role.

Add the there subscription to the management group.

1 - Assign User 1 the Cost Management Reader role for the management group.

2 - Assign User 1 the Global administrator role.

3 - Add the there subscription to the management group.

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 (517 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 377

You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016.

You need to implement a policy to ensure that each virtual machine has a custom antimalware virtual machine extension installed.

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

NOTE: Each correct selection is worth one point.

```

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

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

```

Answer:


```

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

|                   |   |
|-------------------|---|
|                   | ▼ |
| Append            |   |
| Deny              |   |
| DeployIfNotExists |   |


    ",

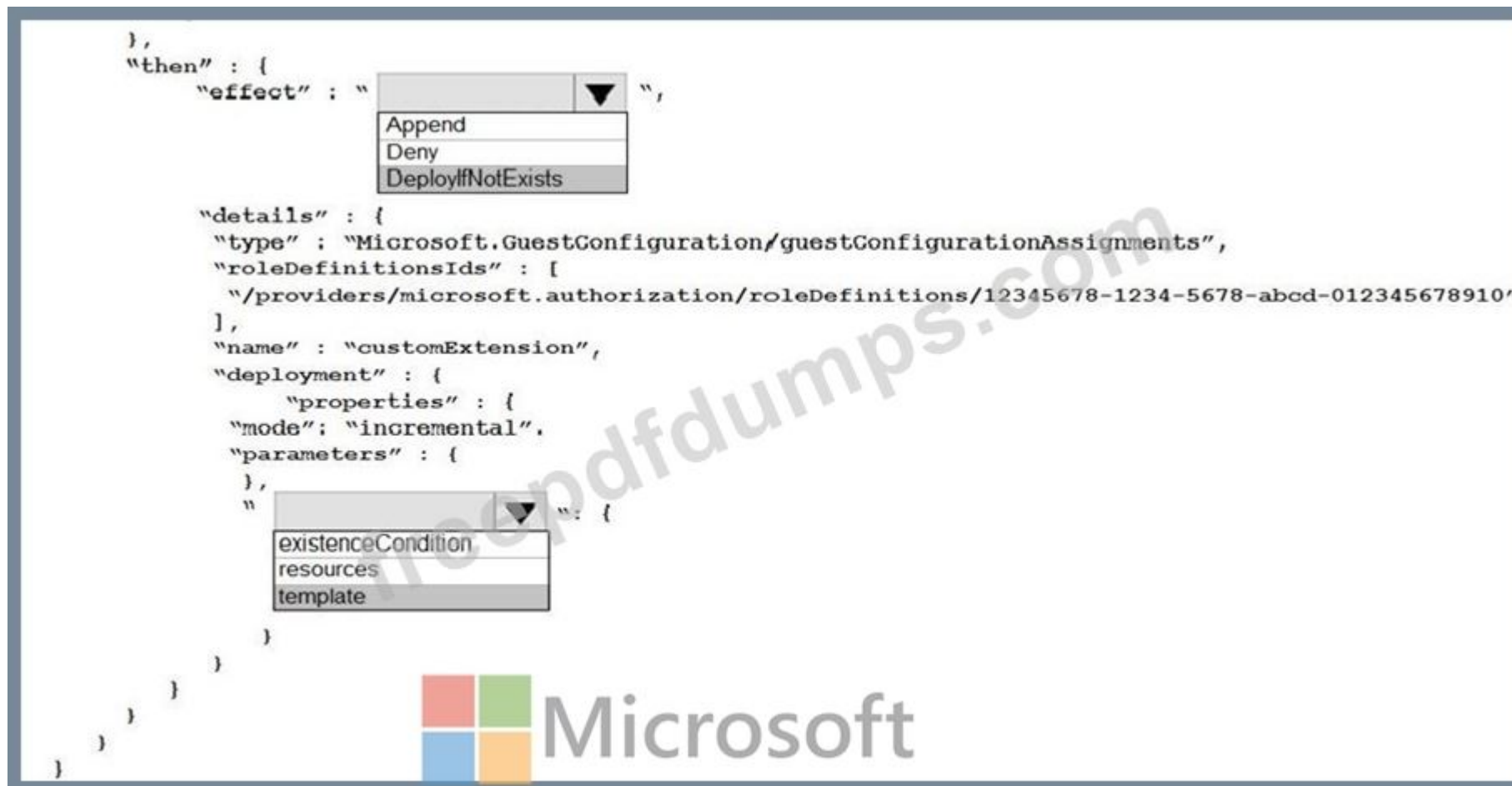
    "details" : {
      "type" : "Microsoft.GuestConfiguration/guestConfigurationAssignments",
      "roleDefinitionsIds" : [
        "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
      ],
      "name" : "customExtension",
      "deployment" : {
        "properties"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

|                    |   |
|--------------------|---|
|                    | ▼ |
| existenceCondition |   |
| resources          |   |
| template           |   |


            ": {
          }
        }
      }
    }
  }
}

```

Explanation



Box 1: DeployIfNotExists

DeployIfNotExists executes a template deployment when the condition is met.

Box 2: Template

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

Deployment [required]

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

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

NEW QUESTION: 378

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

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 Area

⬅

➡

⬆

⬆



Microsoft

Answer:

Answer Area

Consent to PIM

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

Sign up PIM for Azure AD roles

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

References:

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

NEW QUESTION: 379

You need to ensure that the events in the NetworkSecurityGroupRuleCounter log of the VNET01-Subnet0-NSG network security group (NSG) are stored in the logs11597200 Azure Storage account for 30 days.

To complete this task, sign in to the Azure portal.

Answer:

See the explanation below.

Explanation

You need to configure the diagnostic logging for the NetworkSecurityGroupRuleCounter log.

* In the Azure portal, type Network Security Groups in the search box, select Network Security Groups from the search results then select . Alternatively, browse to Network Security Groups in the left navigation pane.

* In the properties of the Network Security Group, click on Diagnostic Settings.

- * Click on the Add diagnostic setting
- * Provide a name in the Diagnostic settings name field. It doesn't matter what name you provide for the exam.
- * In the Log section, select NetworkSecurityGroupRuleCounter
- * In the Destination details section, select
- * In the Storage account field, select the logs11597200 storage account.
- * In the Retention (days) field, enter 30.
- * Click the Save button to save the changes.

NEW QUESTION: 380

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.

Answer Area		
Statements	Yes	No
You can start VM1.	☐	☐
You can start VM2.	☐	☐
You can create a virtual machine in RG2.	☐	☐

Answer:

Answer Area


Microsoft

Statements	Yes	No
You can start VM1.	☐	☒
You can start VM2.	☒	☐
You can create a virtual machine in RG2.	☒	☐

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

- NEW QUESTION: 381**
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: 382
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

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.	☐	☒

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal>

NEW QUESTION: 383

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: Component
A data connector for the firewall software	Create an incident: Component
A playbook	Initiate a script to configure the firewall rule: Component
A rule	
A Security Events connector	
A workbook	

Answer:

Components

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

Answer Area

Enable alert notifications from Security Center:
Create an incident:
Initiate a script to configure the firewall rule:

A data connector for Security Center
A 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: 384

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](#))

Explanation

References:

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

NEW QUESTION: 385

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.)

Role settings



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 approvers

No 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>

NEW QUESTION: 386

You need to create Role1 to meet the platform protection requirements.

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

NOTE: Each correct selection is worth one point.

```
{
  "Name": "Role1",
  "Id": "11111111-1111-1111-1111-111111111111",
  "IsCustom": true,
  "Description": "VM storage operator"
  "Actions": [
    {
      "Microsoft.Compute/":
      "Microsoft.Resources/":
      "Microsoft.Storage/":
    },
    {
      "NotActions": [
      ],
      "AssignableScopes": [
        {
          "/":
          "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4/resourceGroups/Resource Group1"
          "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4"
        }
      ]
    }
  ]
}
```

Microsoft.Compute/	disks/**,
Microsoft.Resources/	storageAccounts/**,
Microsoft.Storage/	virtualMachines/disks/**,

/
/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4/resourceGroups/Resource Group1
/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4



Answer:

```
{
  "Name": "Role1",
  "Id": "11111111-1111-1111-1111-111111111111",
  "IsCustom": true,
  "Description": "VM storage operator"
  "Actions": [
```

Microsoft.Compute/	disks/**
Microsoft.Resources/	storageAccounts/**
Microsoft.Storage/	virtualMachines/disks/**

```
    ],
  "NotActions": [
  ],
  "AssignableScopes": [
```

/*
/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4/resourceGroups/Resource Group1
/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4

```
    ]
```

```
}
```



NEW QUESTION: 387

You have two Azure virtual machines in the East US2 region as shown in the following table.

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

You deploy and configure an Azure Key vault.

You need to ensure that you can enable Azure Disk Encryption on VM1 and VM2.

What should you modify on each virtual machine? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

VM1:  Microsoft ▼

The operating system version
The tier
The type

VM2: ▼

The operating system version
The tier
The type

Answer:

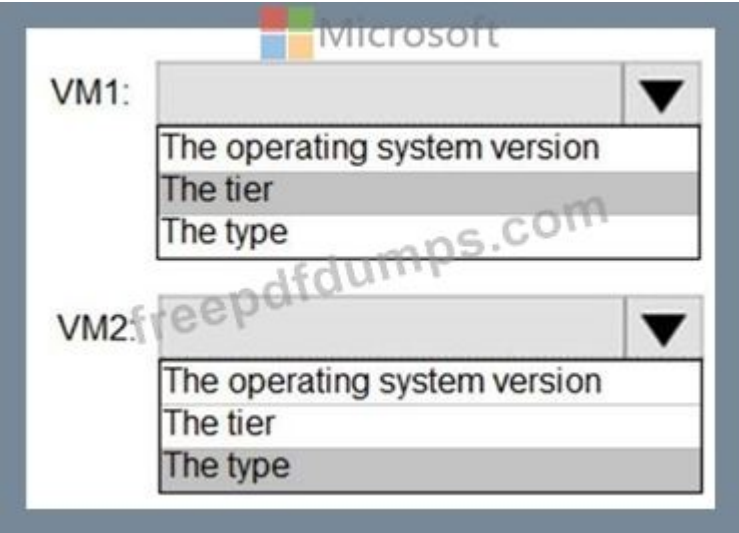
VM1: ▼

The operating system version
The tier
The type

VM2:  Microsoft ▼

The operating system version
The tier
The type

Explanation



VM1: The Tier

The Tier needs to be upgraded to standard.

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

VM2: The type

Need to change the VMtype to any of A, D, DS, G, GS, F, and so on, series IaaS VMs.

Not the operating system version: Ubuntu 16.04 is supported.

References:

<https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview>

https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-faq#bkmk_LinuxOSSupport

NEW QUESTION: 388

Your company has two offices in Seattle and New York. Each office connects to the Internet by using a NAT device. The offices use the IP addresses shown in the following table.

Location	IP address space	Public NAT segment
Seattle	10.10.0.0/16	190.15.1.0/24
New York	172.16.0.0/16	194.25.2.0/24

The company has an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

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

The MFA service settings are configured as shown in the exhibit. (Click the Exhibit tab.)

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

10.10.0.0/16
194.25.2.0/24



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

Methods available to users:

☒ Call to phone

☒ Text message to phone

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

NOTE: Each correct selection is worth one point.

	Yes	No
If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.	☐	☐
If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app.	☐	☐
If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone	☐	☐

Answer:

	Yes	No
If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.	☒	☐
If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app.	☐	☒
If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone	☐	☒

Reference:

<https://www.cayosoft.com/difference-enabling-enforcing-mfa/>

NEW QUESTION: 389

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. Security Posture
- B. GDPRCompliance
- C. Attack Surface Summary
- D. OWASPTopIO

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 390

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.

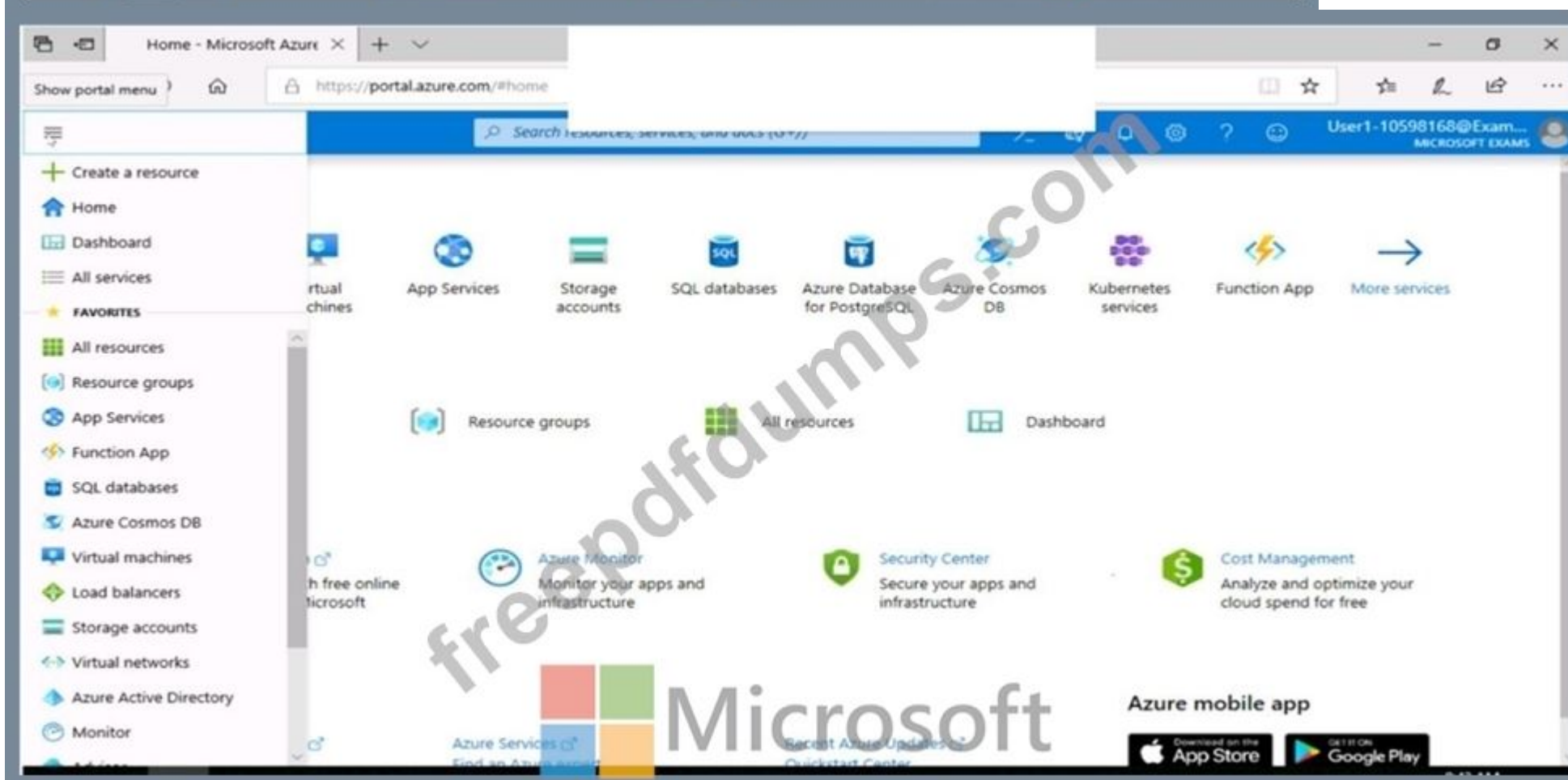
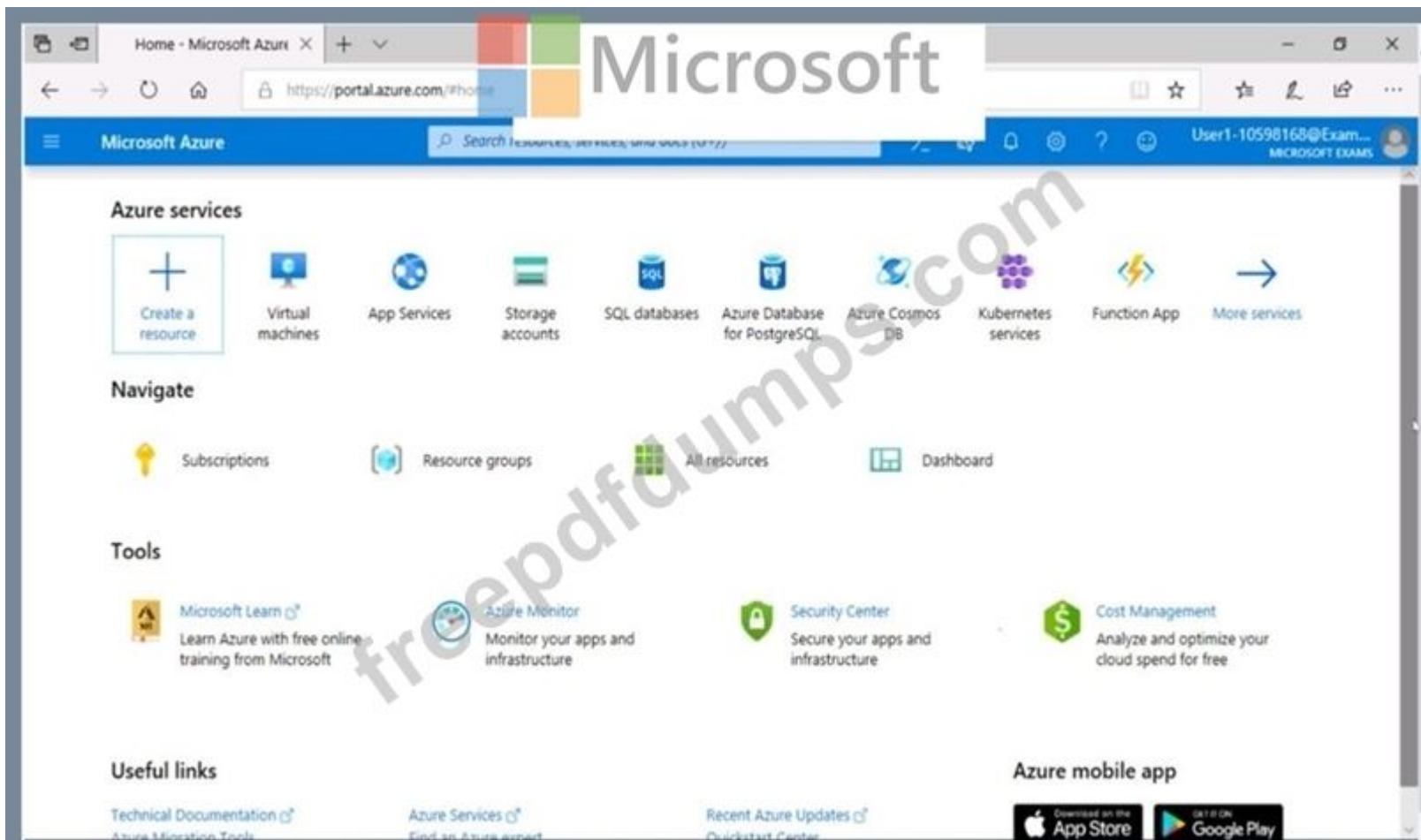
Azure Username: User1-10598168@ExamUsers.com

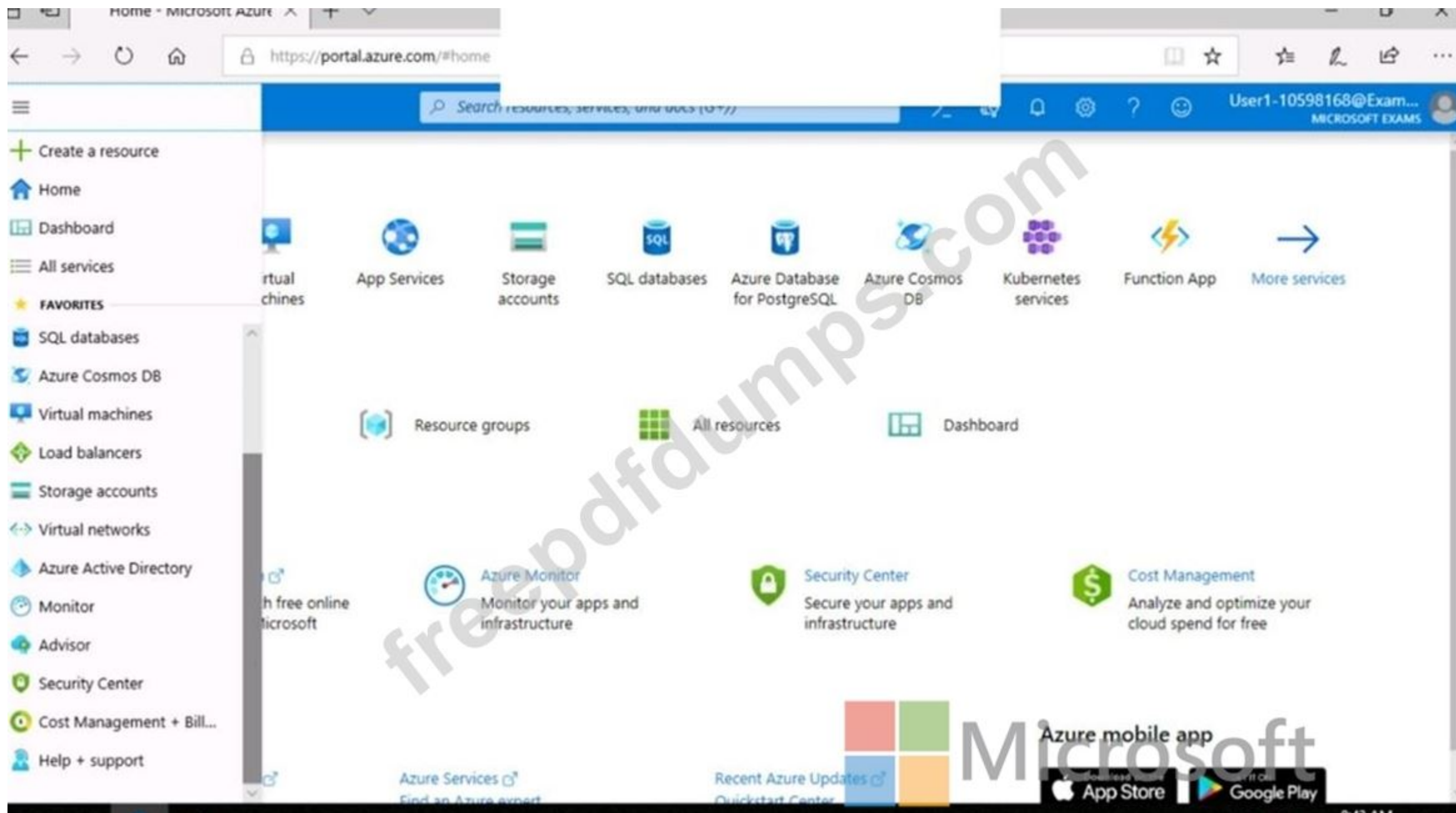
Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168







You need to prevent administrative users from accidentally deleting a virtual network named VNET1. The administrative users must be allowed to modify the settings of VNET1. To complete this task, sign in to the Azure portal.

Answer:

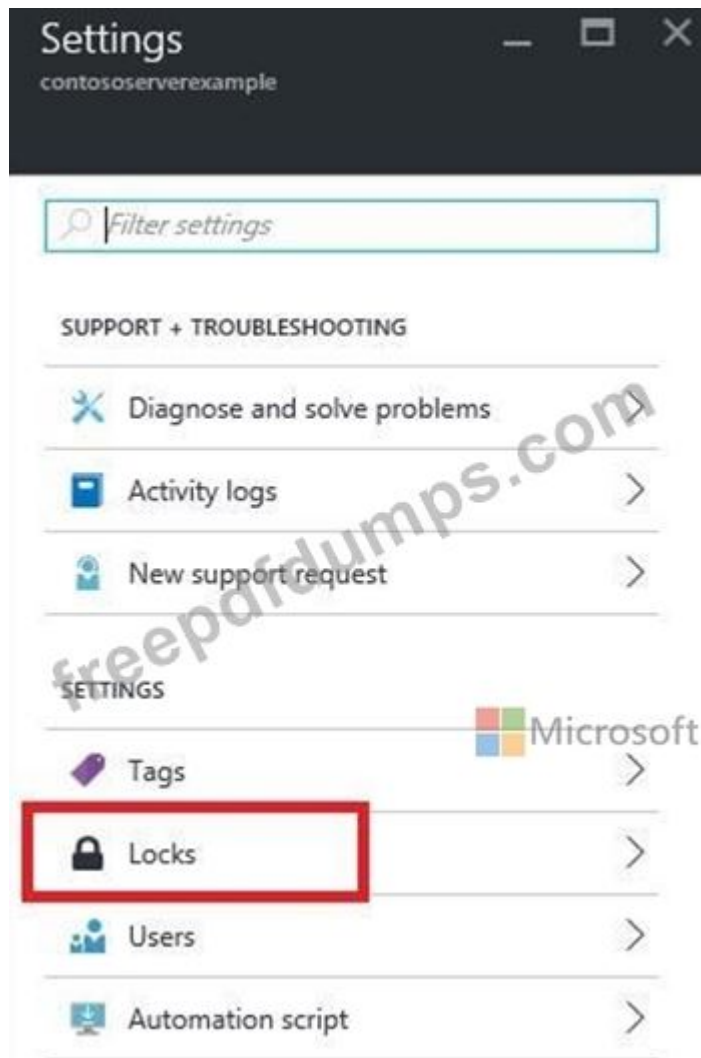
See the explanation below.

Explanation

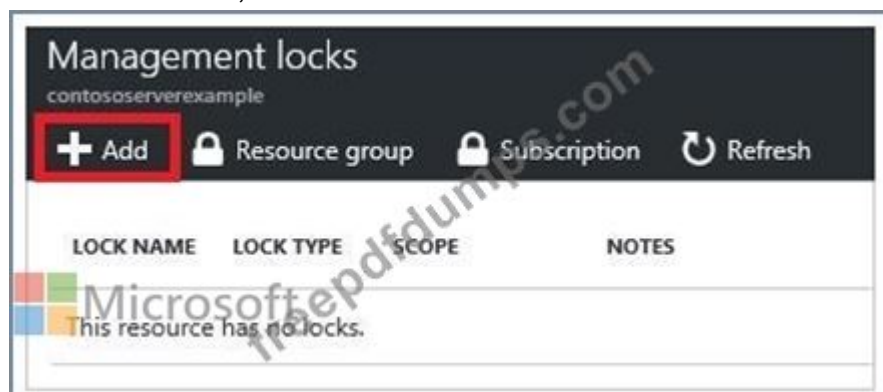
Locking prevents other users in your organization from accidentally deleting or modifying critical resources, such as Azure subscription, resource group, or resource.

Note: In Azure, the term resource refers to an entity managed by Azure. For example, virtual machines, virtual networks, and storage accounts are all referred to as Azure resources.

1. In the Settings blade for virtual network VNET, select Locks.



2. To add a lock, select Add.



3. For Lock type select Delete lock, and click OK

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources>

NEW QUESTION: 391

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.

- C.** Install the container network interface (CNI) plug-in.

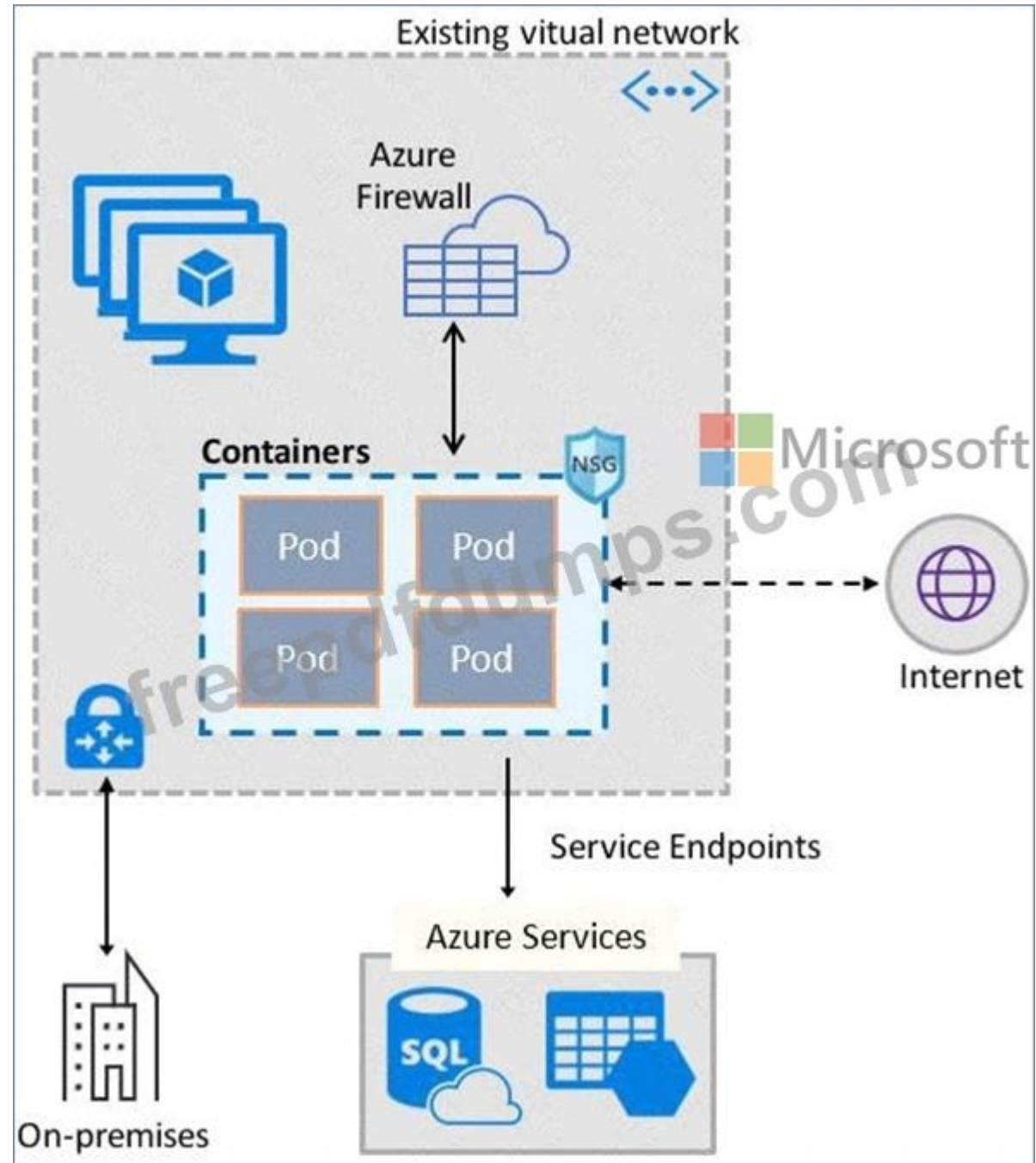
Answer: C (LEAVE A REPLY)

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>

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 (517 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 392

You are evaluating the security of VM1, VM2, and VM3 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 the Internet, you can connect to the web server on VM1 by using HTTP.	☐	☐
From the Internet, you can connect to the web server on VM2 by using HTTP.	☐	☐
From the Internet, you can connect to the web server on VM3 by using HTTP.	☐	☐

Answer:
Answer Area

Statements	Yes	No
From the Internet, you can connect to the web server on VM1 by using HTTP.	☒	☐
From the Internet, you can connect to the web server on VM2 by using HTTP.	☐	☒
From the Internet, you can connect to the web server on VM3 by using HTTP.	☒	☐

NEW QUESTION: 393

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.)

Role settings

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 approvers

No 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>

NEW QUESTION: 394

You 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: 395

You have an Azure Active Directory (Azure AD) tenant that contains a group named Group1. You need to ensure that the members of Group1 sign in by using passwordless authentication. What should you do?

- A. Configure the certificate-based authentication (CBA) policy.
- B. Configure the Microsoft Authenticator authentication method policy.
- C. Configure the sign-in risk policy.
- D. Create a Conditional Access policy.

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

NEW QUESTION: 396

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.	☐	☒

NEW QUESTION: 397

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

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

SQL1 has the following configurations:

* Auditing: Enabled

* Audit log destination: storage1, Workspace1

DB1 has the following configurations:

* Auditing: Enabled

* Audit log destination: storage2

DB2 has auditing disabled.

Where are the audit logs for DB1 and DB2 stored? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point.

Answer Area

DB1: storage1, storage2, and Workspace1

DB2: storage1 and Workspace1 only

DB2: Workspace1 only

Answer:

Answer Area

DB1: storage1, storage2, and Workspace1

DB2: storage1 and Workspace1 only

DB2: Workspace1 only

Explanation:

Answer Area

DB1: storage1, storage2, and Workspace1

DB2: Workspace1 only

NEW QUESTION: 398

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

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

Temporary Access Pass settings

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

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

Enable and Target

Configure

Enable

☒

Include

Exclude

Target

☐ All users

☒ Select groups

Add groups

Name	Type	Registration
Group1	Group	Optional

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

Admin1 can view the Temporary Access Pass of Admin2.

Yes

☐

No

☐

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

☐☐

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

☐☐

Answer:

Answer Area

Statements

Admin1 can view the Temporary Access Pass of Admin2.

Yes

☐

No

☒

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

☒☐

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

☐☒

Explanation:

Answer Area

Statements

Admin1 can view the Temporary Access Pass of Admin2.

Yes

☐

No

☒

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

☒☐

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

☐☒

NEW QUESTION: 399

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 passowrds [\(learn more\)](#)

- ☒ 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 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 to a new device from the Seattle office on June 7, the user will be prompted for MFA.	☒	☐

Explanation

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 to a new device from the Seattle office on June 7, the user will be prompted for MFA.	☒	☐

NEW QUESTION: 400

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

<https://www.fast2test.com/AZ-500-practice-test.html> 38

Valid Fast2test AZ-500 Exam PDF Dumps - New AZ-500 Real Exam Questions

Name	Operating system	State
VM1	Windows Server 2012	Running
VM2	Windows Server 2012 R2	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](#))

Explanation/Reference:

References:

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

NEW QUESTION: 401

You have an Azure Storage account named storage1 that has a container named container1. You need to prevent the blobs in container1 from being modified. What should you do?

- A. From container1, change the access level.
- B. From container1 add an access policy.
- C. From container1, modify the Access Control (IAM) settings.
- D. From storage1 , enable soft delete for blobs.

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

Reference:

<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutable-storage?tabs=azure-portal>

NEW QUESTION: 402

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:  Microsoft ▼

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:

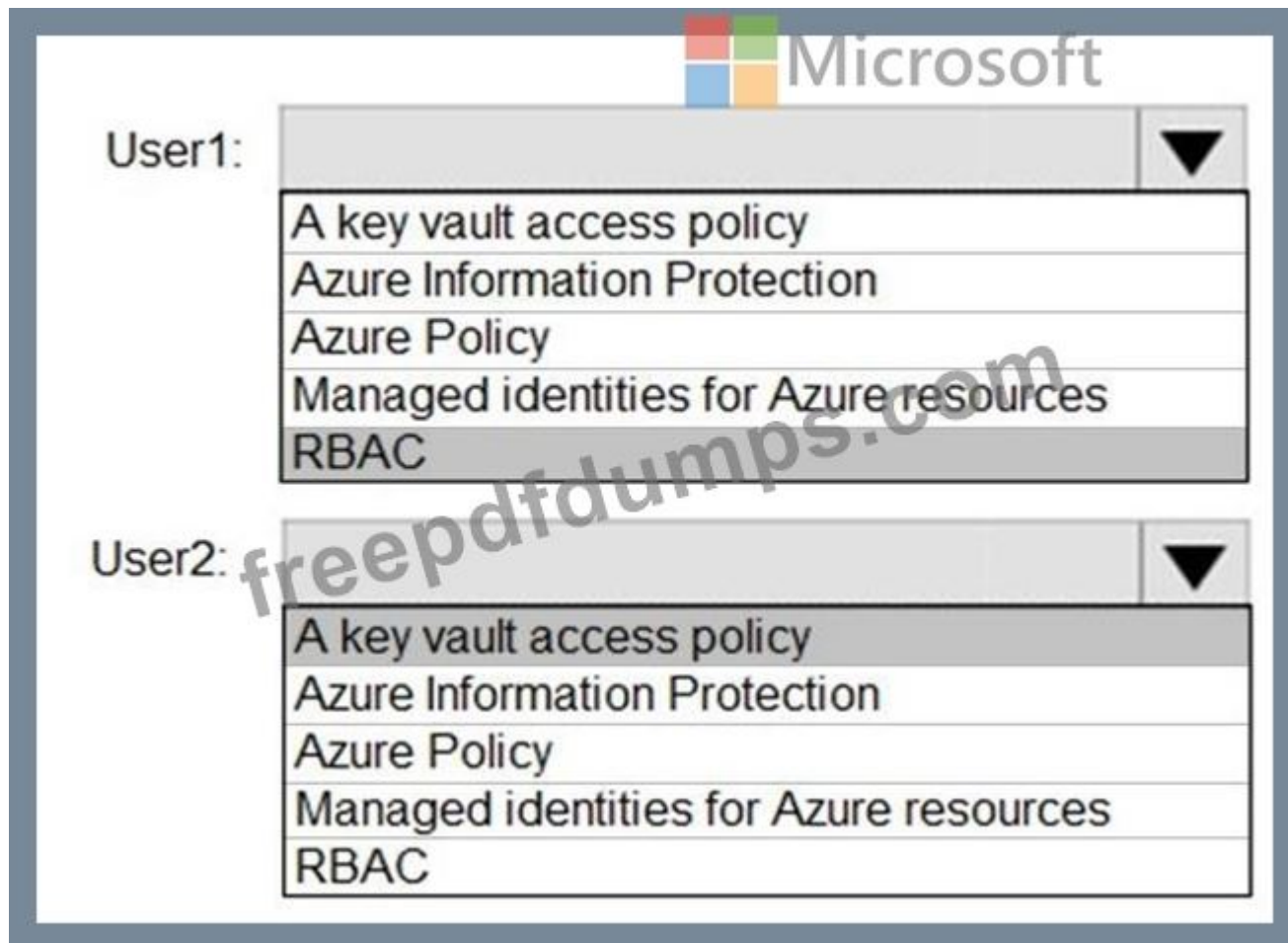
User1: ▼

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: 403

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

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/11111111-1234-1234-1234-1111111111

Answer:

 Microsoft

Permission that must be granted to users on VM:

- Read
- Update
- View
- Write

TCP port that must be allowed:

- 22
- 25
- 3389
- 5986

Explanation

Text, application Description automatically generated

Resource provider:  Microsoft

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

Assignable scope:

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

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: 404

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.

Microsoft

Permission that must be granted to users on VM:

☐	Read
☐	Update
☐	View
☐	Write

TCP port that must be allowed:

☐	22
☐	25
☐	3389
☐	5986

Answer:

Microsoft

Permission that must be granted to users on VM:

☒	Read
☐	Update
☐	View
☐	Write

TCP port that must be allowed:

☐	22
☐	25
☐	3389
☒	5986

NEW QUESTION: 405

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. User administrator
- B. Security administrator
- C. Cloud application administrator
- D. Application administrator
- E. Application developer

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

NEW QUESTION: 406

You need to deploy AKS1 to meet the platform protection requirements.

Which four 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.

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Actions

Deploy an AKS cluster.

Create a client application.

Create a server application.

Create an RBAC binding.

Create a custom RBAC role.

Answer Area

 Microsoft

Answer:

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

Explanation



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

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

Step 1: Create a server application

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

Step 2: Create a client application

The second application is a client component that's used when you're prompted by the CLI for authentication.

This client application uses the server application for the actual authentication of the credentials provided by the client.

Step 3: Deploy an AKS cluster.

Use the az group create command to create a resource group for the AKS cluster.

Use the az aks create command to deploy the AKS cluster.

Step 4: Create an RBAC binding.

Before you use an Azure Active Directory account with an AKS cluster, you must create role-binding or cluster role-binding. Roles define the permissions to grant, and bindings apply them to desired users. These assignments can be applied to a given namespace, or across the entire cluster.

Reference:

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

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 (517 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 407

You have an Azure Active Directory (Azure AD) 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
User3	Group1	Disabled

You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings:

Assignments: Include Group1, exclude Group2

Conditions: Sign-in risk level: Medium and above

Access Allow access, Require multi-factor authentication

You need to identify what occurs when the users sign in to Azure AD.

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.

When User1 signs in from an anonymous IP address,
the user will:

	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

When User2 signs in from an unfamiliar location,
the user will:

	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

When User3 signs in from an infected device,
the user will:

	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

Answer:

When User1 signs in from an anonymous IP address, the user will:

	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

When User2 signs in from an unfamiliar location, the user will:

	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

When User3 signs in from an infected device, the user will:

	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

Reference:

<http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/>

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies>

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

NEW QUESTION: 408

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: B (LEAVE A REPLY)

Incorrect Answers:

A, C: You can create a dynamic group for devices or for users, but you can't create a rule that contains both users and devices.

D: For assigned group you can only add individual members.

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>

Topic 2, Contoso

Contoso

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: 409

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	10.1.1.4	13.80.73.87
VM2	VNET2/Subnet2	10.2.1.4	213.199.133.190
VM3	VNET2/Subnet2	10.2.1.5	None

Subnet1 and Subnet2 have a Microsoft.Storage service endpoint configured.

You have an Azure Storage account named storageacc1 that is configured as shown in the following exhibit.

Save Discard Refresh

Allow access from
☐ All networks ☒ Selected networks

Configure network security for your storage accounts. [Learn more.](#)

Virtual networks
Secure your storage account with virtual networks. [+ Add existing virtual network](#)
[+ Add new virtual network](#)

VIRTUAL NETWORK	SUBNET	ADDRESS RANGE	ENDPOINT STATUS	RESOURCE GROUP	SUBSCRIPTION
No network selected.					

Firewall
Add IP ranges to allow access from the internet on your on-premises networks. [Learn more.](#)

Address Range

13.80.73.87

Exceptions
☒ Allow trusted Microsoft services to access this storage account ⓘ
☐ Allow read access to storage logging from any network
☐ Allow read access to storage metrics from any network

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Statements

From VM1, you can upload a blob to storageacc1.

Yes

No

☐☐

From VM2, you can upload a blob to storageacc1.

☐☐

From VM3 , you can upload a blob to storageacc1.

☐☐

Answer:

Statements	Yes	No
From VM1, you can upload a blob to storageacc1.	☐	☐
From VM2, you can upload a blob to storageacc1.	☐	☐
From VM3 , you can upload a blob to storageacc1.	☐	☐

Explanation

Statements

Yes

No

From VM1, you can upload a blob to storageacc1.

☐☐

From VM2, you can upload a blob to storageacc1.

☐☐

From VM3 , you can upload a blob to storageacc1.

☐☐

Box 1: Yes

The public IP of VM1 is allowed through the firewall.

Box 2: No

The allowed virtual network list is empty so VM2 cannot access storageacc1 directly. The public IP address of VM2 is not in the allowed IP list so VM2 cannot access storageacc1 over the Internet.

Box 3: No

The allowed virtual network list is empty so VM3 cannot access storageacc1 directly. VM3 does not have a public IP address so it cannot access storageacc1 over the Internet.

Reference:

<https://docs.microsoft.com/en-gb/azure/storage/common/storage-network-security>

NEW QUESTION: 410

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to implement an application that will consist of the resources shown in the following table.

Name	Type	Description
CosmosDBAccount1	Azure Cosmos DB account	A Cosmos DB account containing a database named CosmosDB1 that serves as a back-end tier of the application
WebApp1	Azure web app	A web app configured to serve as the middle tier of the application

Users will authenticate by using their Azure AD user account and access the Cosmos DB account by using resource tokens.

You need to identify which tasks will be implemented in CosmosDB1 and WebApp1.

Which task should you identify for each resource? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

CosmosDB1: 

Authenticate Azure AD users and generate resource tokens.
Authenticate Azure AD users and relay resource tokens.
Create database users and generate resource tokens.

WebApp1: 

Authenticate Azure AD users and generate resource tokens.
Authenticate Azure AD users and relay resource tokens.
Create database users and generate resource tokens.

Answer:

CosmosDB1:  

Authenticate Azure AD users and generate resource tokens.
Authenticate Azure AD users and relay resource tokens.
Create database users and generate resource tokens.

WebApp1: 

Authenticate Azure AD users and generate resource tokens.
Authenticate Azure AD users and relay resource tokens.
Create database users and generate resource tokens.

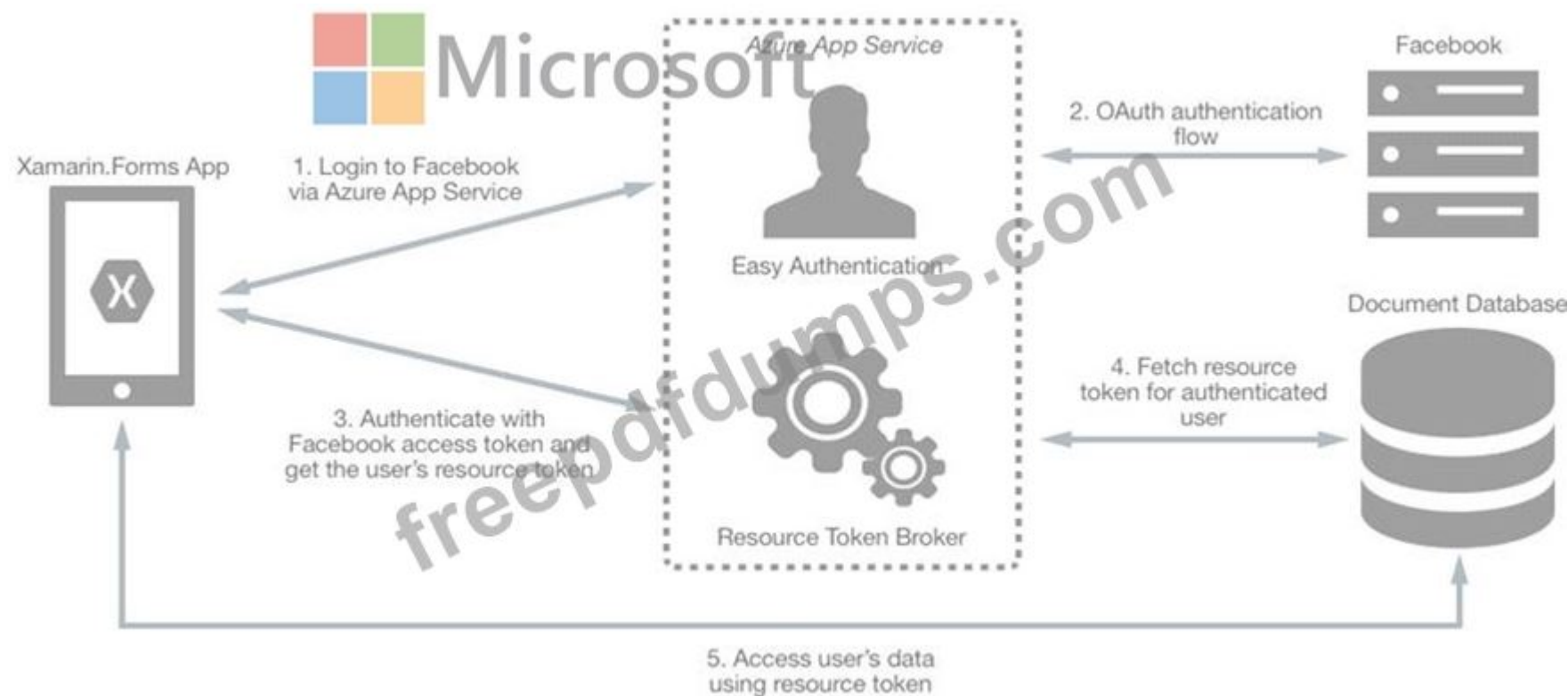
Explanation:

CosmosDB1: Create database users and generate resource tokens.

Azure Cosmos DB resource tokens provide a safe mechanism for allowing clients to read, write, and delete specific resources in an Azure Cosmos DB account according to the granted permissions.

WebApp1: Authenticate Azure AD users and relay resource tokens

A typical approach to requesting, generating, and delivering resource tokens to a mobile application is to use a resource token broker. The following diagram shows a high-level overview of how the sample application uses a resource token broker to manage access to the document database data:



References:

<https://docs.microsoft.com/en-us/xamarin/xamarin-forms/data-cloud/cosmosdb/authentication>

NEW QUESTION: 411

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: 412

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:

Network security rules:

Answer:

NSGs:

Network security rules:

Explanation

NSGs: ▼

1
2
3
4

Network security rules: ▼

1
2
3
4

NSGs: 2

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: 413

You have an Azure subscription that contains the Azure Log Analytics workspaces shown in the following table.

Name	Location	Description
Workspace1	East US	Used by Azure Sentinel
Workspace2	West US	Not applicable

You create the virtual machines shown in the following table.

Name	Location	Operating system	Connected to
VM1	East US	Windows Server 2019	None
VM2	East US	Windows Server 2019	Workspace2
VM3	West US	Windows Server 2019	None
VM4	West US	Windows Server 2019	Workspace2

You plan to use Azure Sentinel to monitor Windows Defender Firewall on the virtual machines.

Which virtual machines you can connect to Azure Sentinel?

- A. VM1 and VM3 only
- B. VM1 Only
- C. VM1 and VM2 only
- D. VM1, VM2, VM3 and VM4

Answer: D ([LEAVE A REPLY](#))

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/connect-windows-firewall>

NEW QUESTION: 414

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

Permission that must be granted to users on VM:

	▼
Read	
Update	
View	
Write	



TCP port that must be allowed:

	▼
22	
25	
3389	
5986	

NEW QUESTION: 415

You need to deploy AKS1 to meet the platform protection requirements.

Which four 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.

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Actions	Answer Area
Deploy an AKS cluster.	
Create a client application.	
Create a server application.	
Create an RBAC binding.	
Create a custom RBAC role.	

Answer:

Actions

Deploy an AKS cluster.

Create a client application.

Create a server application.

Create an RBAC binding.

Create a custom RBAC role.

Answer Area

Create a server application.

Create a client application.

Deploy an AKS cluster.

Create an RBAC binding.

Reference:

<https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration>

NEW QUESTION: 416

You suspect that users are attempting to sign in to resources to which they have no access.

You need to create an Azure Log Analytics query to identify failed user sign-in attempts from the last three days. The results must only show users who had more than five failed sign-in attempts.

How should you configure the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

```
let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AccountType == 'User' and
    [Summary failed login attempts=
    latest_failed_login=arg_max(TimeGenerated by Account
| where failed login attempts > 5
```

Answer:

```
let timeframe = 3d;
securityEvent
where TimeGenerated > ago(3d)
where AccountType == 'User' and
Summarize failed_login_attempts=
latest_failed_login=arg_max(TimeGenerated by AccountID)
```

Dropdown menu 1 (next to 'and') options: ActivityID, DataType, EventID, QuantityUnit. EventID is selected.

Dropdown menu 2 (next to '=') options: Count(), Countif(), Makeset(), Split(). Count() is selected.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/examples>

NEW QUESTION: 417

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.

New-AzureRmKeyVault -VaultName 'KeyVault1' -ResourceGroupName 'RG1'

-Location 'East US'

Dropdown menu 1 options: -EnabledForDeployment, -EnablePurgeProtection, -Tag. -EnablePurgeProtection is selected.

Dropdown menu 2 options: -Confirm, -DefaultProfile, -EnableSoftDelete, -SKU. -EnableSoftDelete is selected.

Answer:



Explanation



Box 1: -EnablePurgeProtection

If specified, protection against immediate deletion is enabled for this vault; requires soft delete to be enabled as well.

Box 2: -EnableSoftDelete

Specifies that the soft-delete functionality is enabled for this key vault. When soft-delete is enabled, for a grace period, you can recover this key vault and its contents after it is deleted.

References:

<https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/new-azurermkeyvault>

NEW QUESTION: 418

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-w>

NEW QUESTION: 419

You 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.	☒	☐

NEW QUESTION: 420

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:

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

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: 421

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 configuration policies in Microsoft Intune
- B. an Azure Desired State Configuration (DSC) virtual machine extension
- C. security policies in Azure Security Center
- D. Azure Logic Apps

Answer: B ([LEAVE A REPLY](#))

Explanation

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 DSC-Service 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.

Reference:

<https://docs.microsoft.com/en-us/azure/automation/automation-dsc-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 (517 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 422

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Location	In resource group
RG1	Resource group	East US	Not applicable
RG2	Resource group	West US	Not applicable
RG3	Resource group	Central US	Not applicable
VNet1	Virtual network	Central US	RG2

VNet1 contains the subnets shown in the following table.

Name	Description
AzureFirewall	Contains no resources
AzureFirewallSubnet	Contains no resources
Subnet1	Contains a virtual machine
Subnet2	Contains no resources

You plan to use the Azure portal to deploy an Azure firewall named AzFW1 to VNet1.

Which resource group and subnet can you use to deploy AzFW1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Resource group: RG2

Subnet: AzureFirewallSubnet only

Answer:

Resource group: RG2

Subnet: AzureFirewallSubnet only

NEW QUESTION: 423

Your network contains an on-premises Active Directory domain named corp.contoso.com.

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

You sync all on-premises identities to Azure AD.

You need to prevent users who have a givenName attribute that starts with TEST from being synced to Azure AD. The solution must minimize administrative effort.

What should you use?

- A. Synchronization Rules Editor
- B. Web Service Configuration Tool
- C. the Azure AD Connect wizard
- D. Active Directory Users and Computers

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: 424

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.

You configure the Authentication methods - Password Protection settings for adatum.com as shown in the following exhibit.

Custom smart lockout

Lockout threshold ⓘ 10 ✓

Lockout duration in seconds ⓘ 60 ✓

Custom banned passwords

Enforce custom list ⓘ Yes No

Custom banned password list ⓘ

Adatum ✓

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ Yes No

Mode ⓘ Enforced Audit

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!.	☒	☐

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>

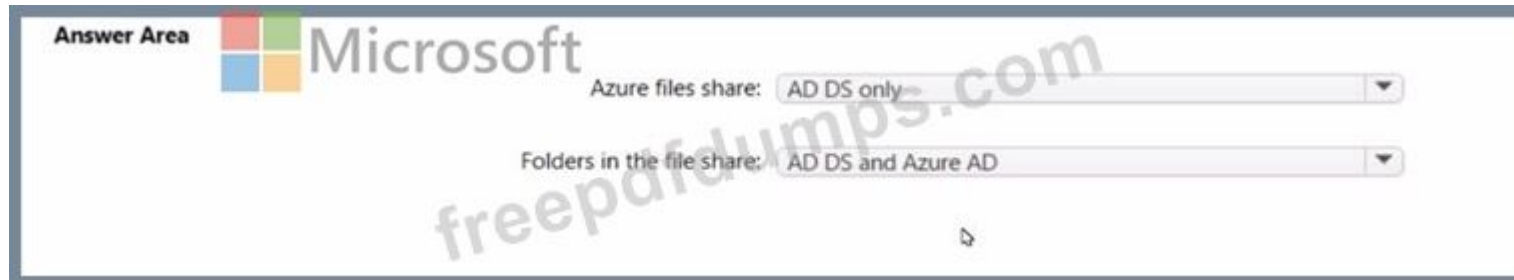
NEW QUESTION: 425

You have an Azure Active directory tenant that syncs with an Active Directory Domain Services (AD DS) domain.

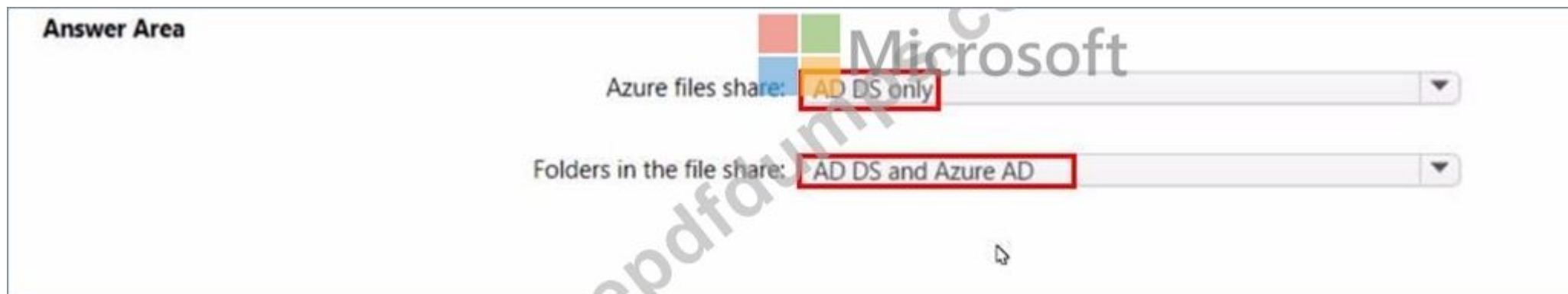
You plan to create an Azure file share that will contain folders and files.

Which identity store can you use to assign permissions to the Azure file share and folders within the share? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 426

You have an Azure subscription that contains an Azure Key Vault Standard key vault named Vault1. Vault1 hosts a 2048-bit RSA key named key1.

You need to ensure that key1 is rotated every 90 days.

What should you do first?

- A. Create a key rotation policy.
- B. Recreate key1 as an EC key.
- C. Modify the Access policies settings of Vault1.
- D. Upgrade Vault1 to Key Vault Premium.

Answer: A ([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 (517 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)