

az-500 Dumps

Microsoft Azure Security Technologies

<https://www.certleader.com/az-500-dumps.html>



NEW QUESTION 1

- (Exam Topic 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 (Azure AD). You have an Azure HDInsight cluster on a virtual network.

You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials. You need to configure the environment to support the planned authentication.

Solution: You deploy an Azure AD Application Proxy.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.

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

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

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

NEW QUESTION 2

- (Exam Topic 4)

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 3

- (Exam Topic 4)

You have 10 on-premises servers that run Windows Server 2019.

You plan to implement Azure Security Center vulnerability scanning for the servers. What should you install on the servers first?

- A. the Security Events data connector in Azure Sentinel
- B. the Microsoft Endpoint Configuration Manager client
- C. the Azure Arc enabled servers Connected Machine agent
- D. the Microsoft Defender for Endpoint agent

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/azure-arc/servers/agent-overview> <https://docs.microsoft.com/en-us/azure/security-center/deploy-vulnerability-assessment->

vm

NEW QUESTION 4

- (Exam Topic 4)

You have multiple development teams that will create apps in Azure.

You plan to create a standard development environment that will be deployed for each team.

You need to recommend a solution that will enforce resource locks across the development environments and ensure that the locks are applied in a consistent manner.

What should you include in the recommendation?

- A. an Azure policy
- B. an Azure Resource Manager template
- C. a management group
- D. an Azure blueprint

Answer: D

Explanation:

Reference:

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

NEW QUESTION 5

- (Exam Topic 4)

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

What should you do?

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

Answer: A

NEW QUESTION 6

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1. You plan to publish several apps in the tenant.

You need to ensure that User1 can grant admin consent for the published apps.

Which two possible user roles can you assign to User1 to achieve this goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Application developer
- B. Security administrator
- C. Application administrator
- D. User administrator
- E. Cloud application administrator

Answer: CE

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent>

NEW QUESTION 7

- (Exam Topic 4)

You have an Azure subscription.

You plan to create two custom roles named Role1 and Role2.

The custom roles will be used to perform the following tasks:

- Members of Role1 will manage application security groups.
- Members of Role2 will manage Azure Bastion. You need to add permissions to the custom roles.

Which resource provider should you use for each role? To answer, drag the appropriate resource providers to the correct roles. Each resource provider 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

Resource Providers

Microsoft.Compute

Microsoft.Network

Microsoft.Security

Microsoft.Solutions

Answer Area

Role1:

Role2:

- A. Mastered
- B. Not Mastered

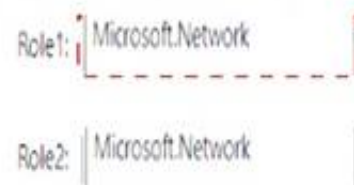
Answer: A

Explanation:

Resource Providers



Answer Area



NEW QUESTION 8

- (Exam Topic 4)

You have an Azure SQL Database server named SQL1.

You plan to 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 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

Explanation:

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 9

- (Exam Topic 4)

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. Modify the Diagnostics settings for the database.
- B. Deploy the SQL Health Check solution in Azure Monitor.
- C. Enable Azure Defender for SQL for the database.
- D. Enable server-level auditing for the database.

Answer: C

NEW QUESTION 10

- (Exam Topic 4)

You plan to deploy Azure container instances.

You have a containerized application that validates credit cards. The application is comprised of two containers: an application container and a validation container.

The application container is monitored by the validation container. The validation container performs security checks by making requests to the application container and waiting for responses after every transaction.

You need to ensure that the application container and the validation container are scheduled to be deployed together. The containers must communicate to each other only on ports that are not externally exposed.

What should you include in the deployment?

- A. application security groups
- B. network security groups (NSGs)
- C. management groups
- D. container groups

Answer: D

Explanation:

Azure Container Instances supports the deployment of multiple containers onto a single host using a container group. A container group is useful when building an application sidecar for logging, monitoring, or any other configuration where a service needs a second attached process.

Reference:

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

NEW QUESTION 10

- (Exam Topic 4)

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.	<input type="radio"/>	<input type="radio"/>
User2 can delete VM1.	<input type="radio"/>	<input type="radio"/>
User3 can sign in to VM1 by using Azure AD credentials.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can delete VM1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can delete VM1.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can sign in to VM1 by using Azure AD credentials.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 13

- (Exam Topic 4)
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 2
You need to add the network interface of a virtual machine named VM1 to an application security group named ASG1.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To add the network interface of a virtual machine named VM1 to an application security group named ASG1, you can follow these steps:

- In the Azure portal, search for and select the virtual machine named VM1.
- In the left pane, select Networking.
- In the Networking pane, select the network interface that you want to add to the application security group named ASG1.
- In the network interface pane, select Application security groups.
- In the Application security groups pane, select Add.
- In the Add application security group pane, select the application security group named ASG1.
- Select Save.

You can find more information on this topic in the following Microsoft documentation: Add a network interface to an application security group using the Azure portal.

NEW QUESTION 17

- (Exam Topic 4)

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         :
TagsTable    :
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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Never Password1 is disabled.

Box 2: Only between March 1, 2019 and May 1, Password2:

```
Expires      : 5/1/19 12:00:00 AM
NotBefore    : 3/1/19 12:00:00 AM
```

Reference:

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

NEW QUESTION 19

- (Exam Topic 4)

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

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: app 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 23

- (Exam Topic 4)

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

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

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

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

You plan to enable Azure Disk Encryption on VM1.

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

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

Answer: C

Explanation:

"Your key vault and VMs must be in the same subscription. Also, to ensure that encryption secrets don't cross regional boundaries, Azure Disk Encryption requires the Key Vault and the VMs to be co-located in the same region." <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault>

NEW QUESTION 25

- (Exam Topic 4)

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

Explanation:

References:

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

NEW QUESTION 27

- (Exam Topic 4)

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

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 29

- (Exam Topic 4)

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

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

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

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

You assign Role1 to User1 on RG1.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can add VM1 to VNET1.	<input type="radio"/>	<input type="radio"/>
User1 can start and stop App1.	<input type="radio"/>	<input type="radio"/>
User1 can start and stop cont1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text Description automatically generated

Reference:

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

NEW QUESTION 32

- (Exam Topic 4)

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

You need to configure maximum number of days for Which new keys are valid. The solution must minimize administrative effort.

What should you use?

- A. Key Vault properties
- B. Azure Policy
- C. Azure Purview
- D. Azure Blueprints

Answer: B

NEW QUESTION 35

- (Exam Topic 4)

Your network contains an Active Directory forest named contoso.com. The forest contains a single domain. You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to deploy Azure AD Connect and to integrate Active Directory and the Azure AD tenant. You need to recommend an integration solution that meets the following requirements:

Ensures that password policies and user logon restrictions apply to user accounts that are synced to the Tenant Minimizes the number of servers required for the solution.

Which authentication method should you include in the recommendation?

- A. federated identity with Active Directory Federation Services (AD FS)
- B. password hash synchronization with seamless single sign-on (SSO)
- C. pass-through authentication with seamless single sign-on (SSO)

Answer: C

Explanation:

* 1. Ensures that password policies and user logon restrictions apply to user accounts that are synced to the tenant

>> Pass-Through Authentication enforce on-premises user account states, password policies, and sign-in hours.

* 2. Minimizes the number of servers required for the solution.

>> Pass-through needs a lightweight agent to be installed one (or more) on-premises servers.

>> PW Hash also require installing Azure AD Connect on your existing DC.

NEW QUESTION 37

- (Exam Topic 4)

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.	<input type="radio"/>	<input type="radio"/>
User2 has App1 listed on her My Apps portal.	<input type="radio"/>	<input type="radio"/>
User3 has App1 listed on her My Apps portal.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal>

NEW QUESTION 41

- (Exam Topic 4)

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.

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

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.

Assign User1 the Cost Management Contributor role for the management group.

Assign User1 the Global administrator role.

Add the three subscriptions to the management group.

NEW QUESTION 44

- (Exam Topic 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 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 add an extension to each virtual machine.

Does this meet the goal?

- A. Yes
B. No

Answer: A

Explanation:

You can use Visual Studio to enable and configure the Microsoft Antimalware service. This entails selecting Microsoft Antimalware extension from the dropdown list under Installed Extensions and click Add to configure with default antimalware configuration.

References:

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

NEW QUESTION 46

- (Exam Topic 4)

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

Name	Days to retain deleted vaults	Purge protection	Permission model
KeyVault1	10	Enabled	Azure role-based access control (Azure RBAC)
KeyVault2	15	Disabled	Azure role-based access control (Azure RBAC)

The subscription contains the users shown in the following table.

Name	Role	Assigned to
Admin1	Key Vault Contributor	KeyVault1
Admin2	Key Vault Secrets Officer	KeyVault2
Admin3	Key Vault Administrator	KeyVault1

On June 1, you perform the following actions:

- Delete a key named key1 from KeyVault1.
- Delete a secret named secret 1 from KeyVault2.

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

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Yes
Yes No

NEW QUESTION 51

- (Exam Topic 4)

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

Explanation:

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

NEW QUESTION 56

- (Exam Topic 4)

You plan to deploy an app that will modify the properties of Azure Active Directory (Azure AD) users by using Microsoft Graph. You need to ensure that the app can access Azure AD. What should you configure first?

- A. a custom role-based access control (RBAC) role
B. an external identity
C. an Azure AD Application Proxy
D. an app registration

Answer: D

Explanation:

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

NEW QUESTION 61

- (Exam Topic 4)

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

Name	Performance	Account kind	Azure Data Lake Storage Gen2
storage1	Standard	BlobStorage	Enabled
storage2	Premium	BlockBlobStorage	Disabled
storage3	Standard	Storage	Disabled
storage4	Premium	FileStorage	Disabled
storage5	Standard	StorageV2	Enabled

You enable Microsoft Defender for Storage.

Which storage services of storages are monitored by Microsoft Defender for Storage, and which storage accounts are protected by Microsoft Defender for Storage? To answer, select the appropriate options in the answer area.

Answer Area

Monitored storage5 services:

Protected storage accounts:

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Monitored storage5 services:

Protected storage accounts:

NEW QUESTION 65

- (Exam Topic 4)

You have an Azure subscription that contains virtual machines. You enable just in time (JIT) VM access to all the virtual machines. You need to connect to a virtual machine by using Remote Desktop. What should you do first?

- A. From Azure Directory (Azure AD) Privileged Identity Management (PIM), activate the Security administrator user role.
B. From Azure Active Directory (Azure AD) Privileged Identity Management (PIM), activate the Owner role for the virtual machine.
C. From the Azure portal, select the virtual machine, select Connect, and then select Request access.
D. From the Azure portal, select the virtual machine and add the Network Watcher Agent virtual machine extension.

Answer: C

Explanation:

Reference:

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

NEW QUESTION 69

- (Exam Topic 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 use Azure Security Center for the centralized policy management of three Azure subscriptions. You use several policy definitions to manage the security of the subscriptions.

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

Solution: You create an initiative and an assignment that is scoped to a management group. Does this meet the goal?

- A. Yes
B. No

Answer: A

Explanation:

References:

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

NEW QUESTION 70

- (Exam Topic 4)

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Box 1: able to connect to East US 2
The StorageEA2Allow has DestinationAddressPrefix {Storage/EastUS2} Box 2: dropped
Reference:
<https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group>

NEW QUESTION 74

- (Exam Topic 4)
You have an Azure AD turned that contains a user named User1. You purchase an App named App1. User1 needs to publish App1 by using Azure AD Application Proxy. Which role should you assign to User1?

- A. Hybrid identity Administrator
- B. Cloud App Security Administrator
- C. Application Administrator
- D. Cloud Application Administrate

Answer: C

NEW QUESTION 77

- (Exam Topic 4)

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.	<input type="radio"/>	<input type="radio"/>
User can modify the properties of storage1.	<input type="radio"/>	<input type="radio"/>
User1 can attach the network interface of VM1 to VNET1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NO NO NO

Reference:

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

NEW QUESTION 80

- (Exam Topic 4)

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 7

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.

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

To collect all the audit failure data from the security log of a virtual machine named VM1 to an Azure Storage account, you can follow these steps:

- In the Azure portal, search for and select the virtual machine named VM1.
- In the left pane, select Diagnostic settings.
- Select Add diagnostic setting.
- In the Add diagnostic setting pane, enter the following information:
- Name: Enter a name for the diagnostic setting.
- Destination: Select Storage account.
- Storage account: Select the storage account you want to use.
- Logs: Select Windows Event Logs.
- Categories: Select Security.
- Event types: Select Audit Failure.
- Select Save.

NEW QUESTION 81

- (Exam Topic 4)

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

Users must be able to select between a Google identity or a Microsoft identity when authenticating to App1. You need to add Google as an identity provider in Azure AD.

Which two pieces of information should you configure? Each correct answer presents part of the solution. Each correct selection is worth one point

- A. a tenant name
B. a tenant ID
C. the endpoint URL Of an application
D. a client ID
E. a client secret

Answer: DE

Explanation:

<https://learn.microsoft.com/en-us/azure/app-service/configure-authentication-provider-google>

NEW QUESTION 84

- (Exam Topic 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 use Azure Security Center for the centralized policy management of three Azure subscriptions. You use several policy definitions to manage the security of the subscriptions.

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

Solution: You create a resource graph and an assignment that is scoped to a management group. Does this meet the goal?

- A. Yes
B. No

Answer: B

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/governance/management-groups/create>

NEW QUESTION 85

- (Exam Topic 4)

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.	<input type="radio"/>	<input type="radio"/>
You can start VM2.	<input type="radio"/>	<input type="radio"/>
You can create a virtual machine in RG2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 87

- (Exam Topic 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 use Azure Security Center for the centralized policy management of three Azure subscriptions. You use several policy definitions to manage the security of the subscriptions.

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

Solution: You create a policy definition and assignments that are scoped to resource groups. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

References:

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

NEW QUESTION 90

- (Exam Topic 4)

DRAG DROP

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

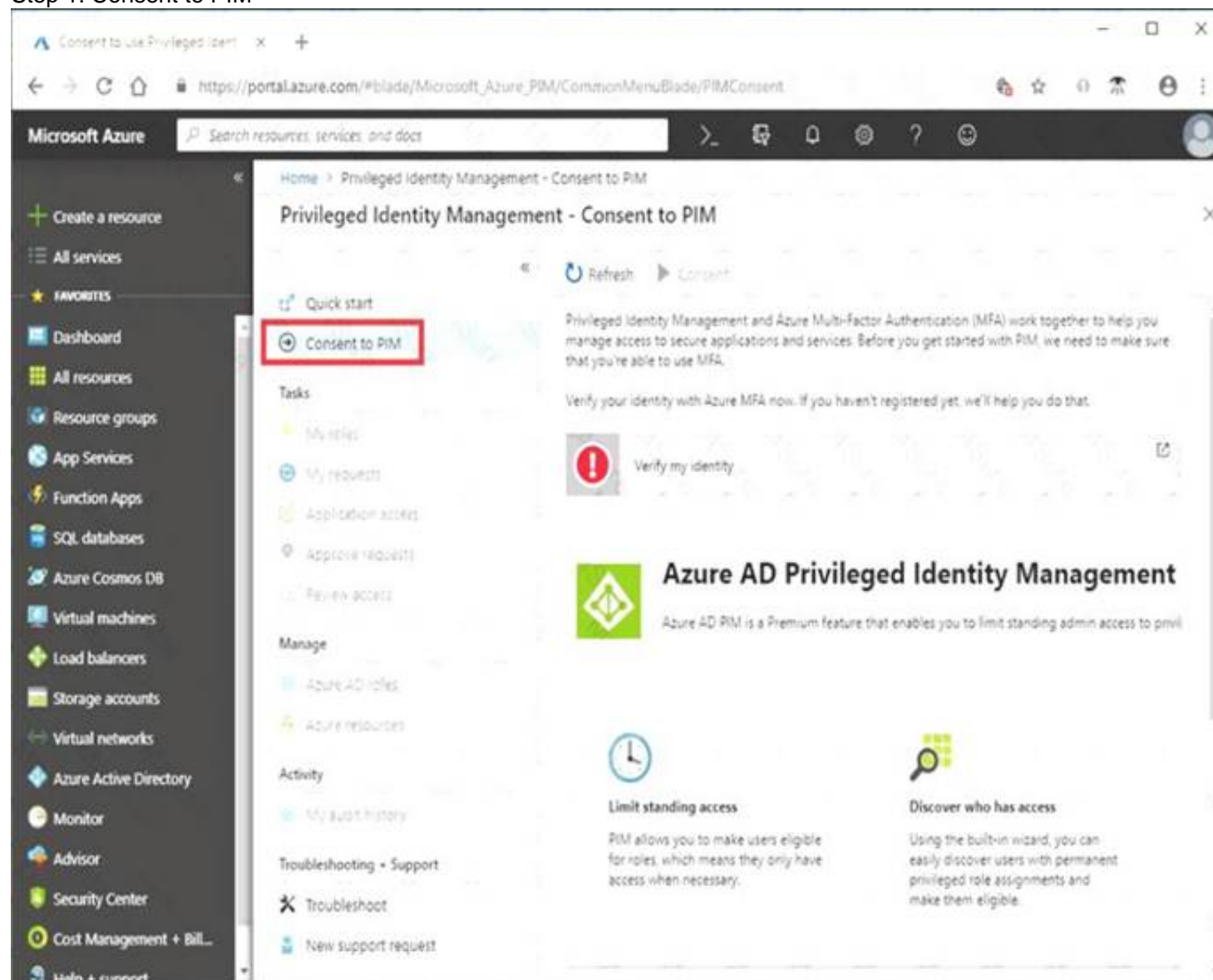


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Step 1: Consent to PIM



Step: 2 Verify your identity by using multi-factor authentication (MFA)

Click Verify my identity to verify your identity with Azure MFA. You'll be asked to pick an account. Step 3: Sign up PIM for Azure AD roles

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

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

NEW QUESTION 94

- (Exam Topic 4)

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

⬆

⬇

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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 96

- (Exam Topic 4)

Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD).

The Azure AD tenant contains the users shown in the following table.

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

You configure the Authentication methods – Password Protection settings for adatum.com as shown in the following exhibit.

Custom smart logout

Lockout threshold ⓘ ✓

Lockout duration in seconds ⓘ ✓

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.	<input type="radio"/>	<input type="radio"/>
User2 can change the password to @d@tum_C0mpleX123.	<input type="radio"/>	<input type="radio"/>
User3 can change the password to Adatum123!.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Text Description automatically generated

Reference:

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

NEW QUESTION 97

- (Exam Topic 4)

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

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

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

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

You enable just in time (JIT) VM access for all the virtual machines. You need to identify which virtual machines are protected by JIT. Which virtual machines should you identify?

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

Answer: C

Explanation:

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 102

- (Exam Topic 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 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 SAS 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

Explanation:

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 104

- (Exam Topic 4)

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.	

A. Mastered

B. Not Mastered

Answer: A

Explanation:

References:

<https://www.petri.com/cloud-security-create-custom-rbac-role-microsoft-azure>

NEW QUESTION 108

- (Exam Topic 4)

You have an Azure subscription named Sub1 that contains the storage accounts shown in the following table

Name	Resource group
storage1	RG1
storage2	RG1
storage3	RG2

The storage3 storage account is encrypted by using customer-managed keys.

YOU need to enable Microsoft Defender for storage to meet the following requirements.

* The storage1 and storage2 account must be include in the defender for storage requirement.

* The storage3 account must be exclude from the Defender for Storage protections.

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

Actions

For storage3, disable the customer-managed keys.

Disable Defender for Storage for storage3.

Enable the Defender for Storage plan for Sub1.

For storage3, assign the AzDefenderPlanAutoEnable tag and set the value to off.

Enable the Defender for Storage plan for RG1.

Answer Area

1

2

3

>

<

>

<

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

For storage3, disable the customer-managed keys.

Disable Defender for Storage for storage3.

Enable the Defender for Storage plan for Sub1.

For storage3, assign the AzDefenderPlanAutoEnable tag and set the value to off.

Enable the Defender for Storage plan for RG1.

Answer Area

1

2

3

>

<

>

<

NEW QUESTION 112

- (Exam Topic 4)

You have an Azure Sentinel deployment.

You need to create a scheduled query rule named Rule1. What should you use to define the query rule logic for Rule1?

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 114

- (Exam Topic 4)

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

Name	Type
storage1	Storage account
KeyVault1	Azure key vault

You need to configure storage1 to regenerate keys automatically every 90 days. Which cmdlet should you run?

- A. set -A=StorageAccount
- B. Add-A:StorogcAccountmanagementPolicyAction
- C. Set-A;StorageAccountimanagementPolicy
- D. Add-AsKeyVaultmanageStorageAccount

Answer: D

NEW QUESTION 117

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com. The User administrator role is assigned to a user named Admin1.

An external partner has a Microsoft account that uses the user1@outlook.com sign in.

Admin1 attempts to invite the external partner to sign in to the Azure AD tenant and receives the following error message: “Unable to invite user user1@outlook.com Generic authorization exception.”

You need to ensure that Admin1 can invite the external partner to sign in to the Azure AD tenant.

What should you do?

- A. From the Roles and administrators blade, assign the Security administrator role to Admin1.
- B. From the Organizational relationships blade, add an identity provider.
- C. From the Custom domain names blade, add a custom domain.
- D. From the Users blade, modify the External collaboration settings.

Answer: D

Explanation:

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

NEW QUESTION 118

- (Exam Topic 4)

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 Microsoft Monitoring agent installed?

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

Answer: D

Explanation:

When automatic provisioning is enabled, Security Center provisions the Microsoft Monitoring Agent on all supported Azure VMs and any new ones that are created.

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

References:

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

NEW QUESTION 120

- (Exam Topic 4)

HOTSPOT

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
    [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
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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 122

- (Exam Topic 4)

Lab Task

Task 1

You need to ensure that connections from the Internet to VNET1\subnet0 are allowed only over TCP port 7777. The solution must use only currently deployed resources.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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

NEW QUESTION 126

- (Exam Topic 4)

You have a web app hosted on an on-premises server that is accessed by using a URL of <https://www.contoso.com>. You plan to migrate the web app to Azure. You will continue to use <https://www.contoso.com>. You need to enable HTTPS for the Azure web app. What should you do first?

- A. Export the public key from the on-premises server and save the key as a P7b file.
- B. Export the private key from the on-premises server and save the key as a PFX file that is encrypted by using TripleDES.
- C. Export the public key from the on-premises server and save the key as a CER file.
- D. Export the private key from the on-premises server and save the key as a PFX file that is encrypted by using AES256.

Answer: B

Explanation:

<https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate#private-certificate-requirements>

NEW QUESTION 128

- (Exam Topic 4)

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

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

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

What should you do?

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

Answer: A

Explanation:

Reference:

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

NEW QUESTION 133

- (Exam Topic 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 an Azure Subscription named Sub1.

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

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

You discover that unauthorized users accessed both the file service and the blob service. You need to revoke all access to Sa1.

Solution: You create a new stored access policy. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

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

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

NEW QUESTION 134

- (Exam Topic 4)

You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant. From the Azure portal, you register an enterprise application. Which additional resource will be created in Azure AD?

- A. a service principal
- B. an X.509 certificate
- C. a managed identity
- D. a user account

Answer: A

Explanation:

Reference:

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

NEW QUESTION 136

- (Exam Topic 4)

You are securing access to the resources in an Azure subscription.

A new company policy states that all the Azure virtual machines in the subscription must use managed disks. You need to prevent users from creating virtual machines that use unmanaged disks.

What should you use?

- A. Azure Monitor
- B. Azure Policy
- C. Azure Security Center
- D. Azure Service Health

Answer: B

NEW QUESTION 141

- (Exam Topic 4)

You create a new Azure subscription that is associated to a new Azure Active Directory (Azure AD) tenant. You create one active conditional access policy named Portal Policy. Portal Policy is used to provide access to the Microsoft Azure Management cloud app.

The Conditions settings for Portal Policy are configured as shown in the Conditions exhibit. (Click the Conditions tab.)

The screenshot displays the 'Portal Policy' configuration in the Azure portal. The 'Conditions' tab is active, showing the following settings:

- Device platforms:** Not configured
- Locations:** 1 included
- Client apps (preview):** Not configured
- Device state (preview):** Not configured

The 'Locations' tab is also visible, showing the following settings:

- Control user access based on their physical location:** Learn more
- Configure:** Yes (selected), No
- Include:** Any location, All trusted locations, Selected locations (selected)
- Select:** Contoso

The Grant settings for Portal Policy are configured as shown in the Grant exhibit. (Click the Grant tab.)

Portal Policy

Info

Delete

Name

Portal Policy

Assignments

Users and groups

All users

Cloud apps

1 app included

Conditions

1 condition selected

Access controls

Grant

2 controls selected

Session

0 controls selected

Grant

Select the controls to be enforced.

Block access

Grant access

Require multi-factor authentication

Require device to be marked as compliant

Require Hybrid Azure AD joined device

Require approved client app

See list of approved client apps

For multiple controls

Require all the selected controls

Require one of the selected controls

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
Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	<input type="radio"/>	<input type="radio"/>
Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription.	<input type="radio"/>	<input type="radio"/>
Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box 1: No
The Contoso location is excluded Box 2: NO
Box 3: NO
Reference:
<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

NEW QUESTION 144

- (Exam Topic 4)

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:

Tool:

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Table Description automatically generated

Reference:

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

NEW QUESTION 145

- (Exam Topic 4)

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.	<input type="radio"/>	<input type="radio"/>
User2 can access App1 from an IP address of 193.77.10.15.	<input type="radio"/>	<input type="radio"/>
User2 can access App1 from an IP address of 154.12.18.34.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can access App1 from an IP address of 154.12.18.10.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access App1 from an IP address of 193.77.10.15.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can access App1 from an IP address of 154.12.18.34.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 148

- (Exam Topic 4)

You have an Azure subscription that contains an Azure Files share named share1 and a user named User1. Identity-based authentication is configured for share1. User1 attempts to access share1 from a Windows 10 device by using SMB. Which type of token will Azure Files use to authorize the request?

- A. OAuth 20
- B. JSON Web Token (JWT)
- C. Kerberos
- D. SAML

Answer: C

Explanation:

<https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-domain-service>

NEW QUESTION 149

- (Exam Topic 4)

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.Authorization
- Microsoft.Resources
- Microsoft.Support

Assignable scope:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text, application Description automatically generated

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 151

- (Exam Topic 4)

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 state accounts in a privileged role.

Answer: D

Explanation:

Reference:

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

NEW QUESTION 156

- (Exam Topic 4)

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

Explanation:

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 161

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant named Contoso.com and an Azure Service (AKS) cluster AKS1.

You discover that AKS1 cannot be accessed by using accounts from Contoso.com

You need to ensure AKS1 can be accessed by using accounts from Contoso.com The solution must minimize administrative effort.

What should you do first?

- A. From Azure recreate AKS1,
- B. From AKS1, upgrade the version of Kubermetes.
- C. From Azure AD, implement Azure AD Premium P2.
- D. From Azure AD, configure the User settings

Answer: A

Explanation:

Reference:

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

NEW QUESTION 164

- (Exam Topic 4)

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

Name	Type
Key1	Key
Secret1	Secret
Cert1	Certificate

Which resources support the creation of a rotation policy?

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

Answer: C

NEW QUESTION 167

- (Exam Topic 4)

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

Name	Location	Connected to
VM1	West US 2	VNET1/Subnet1
VM2	West US 2	VNET1/Subnet1
VM3	West US 2	VNET1/Subnet2
VM4	East US	VNET2/Subnet3
VM5	West US 2	VNET5/Subnet5

Each virtual machine has a single network interface.

You add the network interface of VM1 to an application security group named ASG1.

You need to identify the network interfaces of which virtual machines you can add to ASG1. What should you identify?

- A. VM2 only
- B. VM2, VM3, VM4, and VM5
- C. VM2, VM3, and VM5 only
- D. Vm2 and Vm3 only

Answer: D

Explanation:

Reference:

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

NEW QUESTION 171

- (Exam Topic 4)

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

Explanation:

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-p>

NEW QUESTION 175

- (Exam Topic 4)

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	<i>None</i>
User2	Contributor	<i>None</i>
User3	Security Admin	<i>None</i>
User4	<i>None</i>	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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Only an owner can change permissions on resources.
Box 2: A Contributor can create/modify/delete anything in the subscription but cannot change permissions.

NEW QUESTION 177

- (Exam Topic 4)
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: <input type="text"/>
Low	Users with leaked credentials: <input type="text"/>
Medium	Sign ins from IP addresses with suspicious activity: <input type="text"/>

- A. Mastered
- B. Not Mastered

Answer: A

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 178

- (Exam Topic 4)
You are configuring and securing a network environment.
You deploy an Azure virtual machine named VM1 that is configured to analyze network traffic. You need to ensure that all network traffic is routed through VM1.
What should you configure?

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

Answer: C

Explanation:

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

Note: User Defined Routes
For most environments you will only need the system routes already defined by Azure. However, you may need to create a route table and add one or more routes in specific cases, such as:

- > Force tunneling to the Internet via your on-premises network.
- > Use of virtual appliances in your Azure environment.
- > In the scenarios above, you will have to create a route table and add user defined routes to it.

Reference:
<https://github.com/uglide/azure-content/blob/master/articles/virtual-network/virtual-networks-udr-overview.md>

NEW QUESTION 182

- (Exam Topic 4)
You are configuring an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry.
You need to use the auto-generated service principal to authenticate to the Azure Container Registry. What should you create?

- A. an Azure Active Directory (Azure AD) group

- B. an Azure Active Directory (Azure AD) role assignment
- C. an Azure Active Directory (Azure AD) user
- D. a secret in Azure Key Vault

Answer: B

Explanation:

When you create an AKS cluster, Azure also creates a service principal to support cluster operability with other Azure resources. You can use this auto-generated service principal for authentication with an ACR registry. To do so, you need to create an Azure AD role assignment that grants the cluster's service principal access to the container registry.

References:

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

NEW QUESTION 184

- (Exam Topic 4)

Lab Task

use the following login credentials as needed:

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

To enter your password, place your cursor in the Enter password box and click on the password below. Azure Username: User1 -28681041@ExamUsers.com

Azure Password: GpOAe4@IDg

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

The following information is for technical support purposes only: Lab Instance: 28681041

Task 4

You need to ensure that a user named user2-28681041 can manage the properties of the virtual machines in the RG1lod28681041 resource group. The solution must use the principle of least privilege.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To ensure that a user named user2-28681041 can manage the properties of the virtual machines in the RG1lod28681041 resource group using the principle of least privilege, you can follow these steps:

- In the Azure portal, search for and select the resource group named RG1lod28681041.
- In the left pane, select Access control (IAM).
- Select Add.
- In the Add role assignment pane, enter the following information:
- Role: Select the appropriate role for your scenario. For example, Virtual Machine Contributor.
- Assign access to: Select User, group, or service principal.
- Select: Enter the name of the user you want to assign the role to. For example, user2-28681041.
- Select Save.

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

NEW QUESTION 188

- (Exam Topic 4)

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

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 193

- (Exam Topic 4)

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

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

You enable passwordless authentication for the tenant.

Which authentication method can each user use for passwordless authentication? To answer, drag the appropriate authentication methods to the correct users.

Each authentication method 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.

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

User1:	Authentication method
User2:	Authentication method

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

User1:	Microsoft Authenticator app only
User2:	Windows Hello for Business only

NEW QUESTION 194

- (Exam Topic 4)

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: ▼

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

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 197

- (Exam Topic 4)

You are configuring network connectivity for two Azure virtual networks named VNET1 and VNET2. You need to implement VPN gateways for the virtual networks to meet the following requirements:

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

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

NOTE: Each correct selection is worth one point

SKUs

Basic	VpnGw1	VpnGw2	VpnGw3
-------	--------	--------	--------

Answer Area

VNET1: SKU

VNET2: SKU

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 200

- (Exam Topic 4)

You have an Azure subscription named Subscription1 that contains a resource group named RG1 and the users shown in the following table.

Name	User principal name (UPN)	Type
User1	User1@outlook.com	Guest
User2	User2@outlook.com	Guest

You perform the following tasks:

- Assign User1 the Network Contributor role for Subscription1.
- Assign User2 the Contributor role for RG1.

To Subscription1 and RG1, you assign the following policy definition: External accounts with write permissions should be removed from your subscription.

What is the Compliance State of the policy assignments?

- A. The Compliance State of both policy assignments is Non-compliant.
B. The Compliance State of the policy assignment to Subscription1 is Compliant, and the Compliance State of the policy assignment to RG1 is Non-compliant.
C. The Compliance State of the policy assignment to Subscription1 is Non-compliant, and the Compliance State of the policy assignment to RG1 is Compliant.
D. The Compliance State of both policy assignments is Compliant.

Answer: A

NEW QUESTION 201

- (Exam Topic 4)

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

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.

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Text Description automatically generated with medium confidence

Reference:

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

NEW QUESTION 205

- (Exam Topic 4)

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

Explanation:

Reference:

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

NEW QUESTION 206

- (Exam Topic 4)

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.	<input type="radio"/>	<input type="radio"/>
From VM2, users can manage the keys and secrets stored in KeyVault1.	<input type="radio"/>	<input type="radio"/>
VM2 can use KeyVault for Azure Disk Encryption	<input type="radio"/>	<input type="radio"/>

A. Mastered

B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 207

- (Exam Topic 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 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.

The Leader of IT Certification

visit - <https://www.certleader.com>

Solution: You regenerate the Azure storage account access keys. Does this meet the goal?

- A. Yes
B. No

Answer: A

Explanation:

Generating new storage account keys will invalidate all SAS's that were based on the previous keys.

NEW QUESTION 210

- (Exam Topic 4)

You have an Azure subscription linked to an Azure Active Directory Premium Plan 1 tenant. You plan to implement Azure Active Directory (Azure AD) Identity Protection.

You need to ensure that you can configure a user risk policy and a sign-in risk policy. What should you do first?

- A. Purchase Azure Active Directory Premium Plan 2 licenses for all users.
B. Register all users for Azure Multi-Factor Authentication (MFA).
C. Enable security defaults for Azure AD.
D. Upgrade Azure Security Center to the standard tier.

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa>

NEW QUESTION 215

- (Exam Topic 4)

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 for Role2 are shown in the following role definition file.

```
"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.	<input type="radio"/>	<input type="radio"/>
User2 can delete VM1.	<input type="radio"/>	<input type="radio"/>
User3 can delete VM1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 220

- (Exam Topic 4)

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

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

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

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

You plan to enable Azure Disk Encryption on VM1.

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

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

Answer: A

Explanation:

In order to make sure the encryption secrets don't cross regional boundaries, Azure Disk Encryption needs the Key Vault and the VMs to be co-located in the same region. Create and use a Key Vault that is in the same region as the VM to be encrypted.

Reference:

<https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-prerequisites>

NEW QUESTION 225

- (Exam Topic 4)

You have an Azure subscription that contains an Azure SQL database named DB1 in the East US Azure region. You create the storage accounts shown in the following table.

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

You plan to enable auditing for DB1.

Which storage accounts can you use as the auditing destination for DB1?

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

Answer: C

NEW QUESTION 226

- (Exam Topic 4)

You have an Azure subscription that contains a web app named Appl. App1 provides users with product images and videos. Users access App1 by using a URL of [HTTPS://appl.contoso.com](https://appl.contoso.com). You deploy two server pools named Pool1 and Pool2. Pool1 hosts product images. Pool2 hosts product videos. You need to optimize

The performance of Appl. The solution must meet the following requirements:

- Minimize the performance impact of TLS connections on Pool1 and Pool2.

- Route user requests to the server pools based on the requested URL path. What should you include in the solution?

A. Azure Traffic Manager
B. Azure Bastion
C. Azure Application Gateway
D. Azure Front Door

Answer: C

NEW QUESTION 230

- (Exam Topic 4)

Lab Task

Task 4

You need to ensure that when administrators deploy resources by using an Azure Resource Manager template, the deployment can access secrets in an Azure key vault named KV31330471.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Grant permission to the application that is used to deploy the resources to access the secrets in the key vault. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to assign the Key Vault Secrets User role to the application at the scope of the key vault or individual secrets.

Enable template deployment for the key vault. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to set the `enabledForTemplateDeployment` property of the key vault to `true`.

Reference the secrets in the template by using their resource ID. You can use the `listSecrets` function to get the resource ID of a secret in the key vault. You need to specify the name of the key vault and the name of the secret as parameters.

Deploy the template by using Azure PowerShell, Azure CLI, or REST API. You can use the

`New-AzResourceGroupDeployment` cmdlet, the `az deployment group create` command, or the Deployments - Create Or Update REST API to do this. You need to provide the template file or URI and any required parameters.

NEW QUESTION 231

- (Exam Topic 4)

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	<i>Not applicable</i>

You create the virtual machines shown in the following table.

Name	Location	Operating system	Connected to
VM1	East US	Windows Server 2019	<i>None</i>
VM2	East US	Windows Server 2019	Workspace2
VM3	West US	Windows Server 2019	<i>None</i>
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

Explanation:

Reference:

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

NEW QUESTION 232

- (Exam Topic 4)

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

- A. Mastered
B. Not Mastered

Answer: A

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 237

- (Exam Topic 4)

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

- A. Mastered
B. Not Mastered

Answer: A

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 242

- (Exam Topic 4)

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

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

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

You plan to implement Microsoft Defender for SQL.

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

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

Answer: D

NEW QUESTION 243

- (Exam Topic 4)

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:

<div>▼</div> <div>Azure Active Directory User</div> <div>Managed identity</div> <div>Service Principal</div>
--

Roles:

<div>▼</div> <div>db_datawriter only</div> <div>db_datareader and db_datawriter</div> <div>db owner only</div>
--

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

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

NEW QUESTION 247

- (Exam Topic 4)

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:

<div>▼</div> <div>A key vault access policy</div> <div>Azure Information Protection</div> <div>Azure Policy</div> <div>Managed identities for Azure resources</div> <div>RBAC</div>

User2:

<div>▼</div> <div>A key vault access policy</div> <div>Azure Information Protection</div> <div>Azure Policy</div> <div>Managed identities for Azure resources</div> <div>RBAC</div>

- A. Mastered
- B. Not Mastered

Answer: A

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.

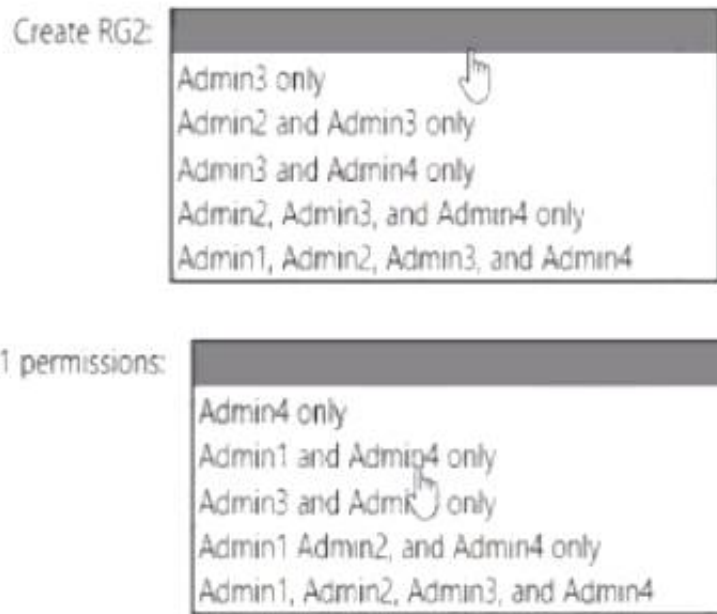
References:

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

NEW QUESTION 251

- (Exam Topic 3)

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 area. NOTE: Each correct selection is worth one point



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

Box 1: Admin3 only

The Contributor role has the necessary write permissions to create the resource group. Box 2: Admin4 only

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

NEW QUESTION 253

- (Exam Topic 3)

You need to encrypt storage1 to meet the technical requirements. Which key vaults can you use?

- A. KeyVault1 only
- B. KeyVault2 and KeyVault3 only
- C. KeyVault1 and KeyVault3 only
- D. KeyVault1 KeyVault2 and KeyVault3

Answer: B

Explanation:

The storage account and the key vault must be in the same region and in the same Azure Active Directory (Azure AD) tenant, but they can be in different subscriptions.

Storage1 is in the West US region. KeyVault1 is the only key vault in the same region. Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-overview>

NEW QUESTION 254

- (Exam Topic 2)

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box1: RG6 only as there is not option for RG5 & RG6 which it should be. Box2: RG4 & RG6

NEW QUESTION 256
- (Exam Topic 2)
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.

Answer: A

Explanation:
From scenario: Deploy Azure Firewall to VNetwork1 in Sub2.
Azure firewall needs a dedicated subnet named AzureFirewallSubnet. References:
<https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal>

NEW QUESTION 260
- (Exam Topic 2)
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.	<input type="radio"/>	<input type="radio"/>
From VM2, you can successfully ping the private IP address of VM4.	<input type="radio"/>	<input type="radio"/>
From VM1, you can connect to the web server on VM4.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:
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 263

- (Exam Topic 1)

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

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>

NEW QUESTION 265

- (Exam Topic 1)

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 269

- (Exam Topic 1)

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.	

- A. Mastered
B. Not Mastered

Answer: A

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>

NEW QUESTION 274

- (Exam Topic 1)

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/
    ],
    [
      disks/**,
      storageAccounts/**,
      virtualMachines/disks/**,
    ],
  ],
  "NotActions": [
  ],
  "AssignableScopes" : [
    [
      /*
      */
      "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4/resourceGroups Resource Group1"
      "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4
    ],
  ],
}
```

- A. Mastered
- B. Not Mastered

Answer: A

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 276

- (Exam Topic 1)
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 Assign
- E. Create two groups that have dynamic membership
- F. Add the new groups to Group1.

Answer: D

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership> Scenario:
Litware identifies the following identity and access requirements: All San Francisco users and their devices must be members of Group1.
The tenant currently contain this group:

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

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

NEW QUESTION 280

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your az-500 Exam with Our Prep Materials Via below:

<https://www.certleader.com/az-500-dumps.html>