

## Exam Questions az-500

Microsoft Azure Security Technologies

<https://www.2passeasy.com/dumps/az-500/>



NEW QUESTION 1

- (Exam Topic 4)

You plan to use Azure Log Analytics to collect logs from 200 servers that run Windows Server 2016. You need to automate the deployment of the Microsoft Monitoring Agent to all the servers by using an Azure Resource Manager template. How should you complete the template? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

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

AzureADApplicationID

WorkspaceID

WorkspaceName

WorkspaceURL

AzureADApplicationSecret

StorageAccountKey

WorkspaceID

WorkspaceKey

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:  
https://blogs.technet.microsoft.com/manageabilityguys/2015/11/19/enabling-the-microsoft-monitoring-agent-in

NEW QUESTION 2

- (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	Enabled
User2	Group1	Disabled
User3	Group1	Disabled

You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings: ➤ Assignments: Include Group1, exclude Group2  
➤ Conditions: Sign-in risk level: Medium and above  
➤ Access Allow access, Require multi-factor authentication  
You need to identify what occurs when the users sign in to Azure AD. What should you identify for each user? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

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

	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

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

	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

When User3 signs in from an infected device, the user will:

	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

References:

<http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/> <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies> <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

**NEW QUESTION 3**

- (Exam Topic 4)

You have an Azure web app named WebApp1. You upload a certificate to WebApp1.

You need to make the certificate accessible to the app code of WebApp1. What should you do?

- A. Add a user-assigned managed identity to WebApp1.
- B. Add an app setting to the WebApp1 configuration.
- C. Enable system-assigned managed identity for the WebApp1.
- D. Configure the TLS/SSL binding for WebApp1.

**Answer:** B

**Explanation:**

Reference:

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

**NEW QUESTION 4**

- (Exam Topic 4)

Lab Task

Task 5

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

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Create an Azure Resource Manager service principal. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to specify a name and a role for the service principal, such as Contributor.

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

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

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

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

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

**NEW QUESTION 5**

- (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 6

- (Exam Topic 4)

You have an Azure subscription that contains four Azure SQL managed instances.

You need to evaluate the vulnerability of the managed instances to SQL injection attacks. What should you do first?

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

**Answer:** B

#### NEW QUESTION 7

- (Exam Topic 4)

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

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

Transparent Data Encryption (TDE) is disabled on SQL1.

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

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

You plan to deploy Azure SQL databases by using an Azure Resource Manager (ARM) template. The databases will be configured as shown in the following table.

NOTE: Each correct selection is worth one point.

**Answer Area**

Statements	Yes	No
SQL1 will have TDE enabled automatically.	<input type="radio"/>	<input type="radio"/>
The deployment of SQL2 will fail.	<input type="radio"/>	<input type="radio"/>
SQL3 will be deployed and marked as noncompliant.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application Description automatically generated

#### NEW QUESTION 8

- (Exam Topic 4)

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

SQL1 has the following settings:

- Auditing: On
- Audit log destination: storage1

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



## Answer Area

Statements	Yes	No
Audit events for DB1 are written to storage1.	<input type="radio"/>	<input type="radio"/>
Audit events for DB2 are written to storage1 and storage2.	<input type="radio"/>	<input type="radio"/>
Storage3 can be used as an audit log destination for DB3.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

### Explanation:

Reference:

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

## NEW QUESTION 9

- (Exam Topic 4)

You have an Azure subscription.

You plan to create a custom role-based access control (RBAC) role that will provide permission to read the Azure Storage account.

Which property of the RBAC role definition should you configure?

- A. NotActions []
- B. DataActions []
- C. AssignableScopes []
- D. Actions []

**Answer:** D

### Explanation:

To 'Read a storage account', ie. list the blobs in the storage account, you need an 'Action' permission. To read the data in a storage account, ie. open a blob, you need a 'DataAction' permission.

Reference:

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

## NEW QUESTION 10

- (Exam Topic 4)

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

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

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

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

Solution: You recommend the use of password hash synchronization and seamless SSO. Does the solution meet the goal?

- A. Yes
- B. No

**Answer:** B

## NEW QUESTION 10

- (Exam Topic 4)

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

All users have computers that run Windows 10 and are hybrid Azure AD joined.

You have an Azure SQL database that is configured to support Azure AD authentication.

Database developers must connect to the SQL database by using Microsoft SQL Server Management Studio (SSMS) and authenticate by using their on-premises Active Directory account.

You need to tell the developers which authentication method to use to connect to the SQL database from SSMS. The solution must minimize authentication prompts.

Which authentication method should you instruct the developers to use?

- A. SQL Login
- B. Active Directory – Universal with MFA support
- C. Active Directory – Integrated
- D. Active Directory – Password

**Answer:** C

### Explanation:

Azure AD can be the initial Azure AD managed domain. Azure AD can also be an on-premises Active Directory Domain Services that is federated with the Azure AD.

Using an Azure AD identity to connect using SSMS or SSDT

The following procedures show you how to connect to a SQL database with an Azure AD identity using SQL Server Management Studio or SQL Server Database Tools.

Active Directory integrated authentication

Use this method if you are logged in to Windows using your Azure Active Directory credentials from a federated domain.

\* 1. Start Management Studio or Data Tools and in the Connect to Server (or Connect to Database Engine) dialog box, in the Authentication box, select Active Directory - Integrated. No password is needed or can be entered because your existing credentials will be presented for the connection.

\* 2. Select the Options button, and on the Connection Properties page, in the Connect to database box, type the name of the user database you want to connect to. (The AD domain name or tenant ID" option is only supported for Universal with MFA connection options, otherwise it is greyed out.)

References:

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/sql-database/sql-database-aad-authentication>

### NEW QUESTION 13

- (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 15

- (Exam Topic 4)

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

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

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

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

Answer: D

NEW QUESTION 20

- (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 connect to each virtual machine and add a Windows feature. Does this meet the goal?

- A. Yes  
B. No

Answer: B

Explanation:

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

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

NEW QUESTION 23

- (Exam Topic 4)

Lab Task

Task 6

You need to configure a Microsoft SQL server named Web3l 330471 only to accept connections from the Subnet0 subnet on the VNET01 virtual network.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

Configure the network settings for the SQL server. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to enable service endpoints for SQL Server on the Subnet0 subnet. You also need to add a virtual network rule that links the SQL server to the Subnet0 subnet.

Configure the connection settings for the SQL server. You can use SQL Server Management Studio or Transact-SQL to do this. You need to enable remote server connections and specify a TCP port for listening. You also need to configure SQL Server Authentication or Azure Active Directory Authentication for connecting to the SQL server.

**NEW QUESTION 24**

- (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 26**

- (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 29**

- (Exam Topic 4) You have an Azure SQL database. You implement Always Encrypted.

You need to ensure that application developers can retrieve and decrypt data in the database.

Nantes's of information should you provide to the developers? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a stored access policy
- B. a shared access signature (SAS)
- C. the column encryption key
- D. user credentials
- E. the column master key

**Answer:** CE



Explanation:

Always Encrypted uses two types of keys: column encryption keys and column master keys. A column encryption key is used to encrypt data in an encrypted column. A column master key is a key-protecting key that encrypts one or more column encryption keys.

References:

<https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine>

NEW QUESTION 32

- (Exam Topic 4)

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

Name	Type
RG1	Resource group
VM1	Virtual machine

You perform the following tasks:

Create a managed identity named Managed1. Create a Microsoft 365 group named Group1.

You need to identify which service principals were created and which identities can be assigned the Reader role for RG1. What should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Service Principals:

▼

App1 only  
Managed1 and VM1 only  
Managed1, VM1, and App1 only  
Managed1, VM1, App1, and Group1

Identities:

▼

App1 only  
Managed1 and VM1 only  
Managed1, VM1, and App1 only  
Managed1, VM1, App1, and Group1

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Service Principals:

▼

App1 only  
Managed1 and VM1 only  
Managed1, VM1, and App1 only  
Managed1, VM1, App1, and Group1

Identities:

▼

App1 only  
Managed1 and VM1 only  
Managed1, VM1, and App1 only  
Managed1, VM1, App1, and Group1

NEW QUESTION 36

- (Exam Topic 4)

You have five Azure subscriptions linked to a single Azure Active Directory (Azure AD) tenant. You create an Azure Policy initiative named SecurityPolicyInitiative1.

You identify which standard role assignments must be configured on all new resource groups.

You need to enforce SecurityPolicyInitiative1 and the role assignments when a new resource group is created. 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

Publish an Azure Blueprints version

Assign an Azure blueprint.

Create a policy assignment.

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

Create a dedicated management subscription.

Create an Azure Blueprints definition.

Create an initiative assignment.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 41

- (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 44**

- (Exam Topic 4)

You have three on-premises servers named Server1, Server2, and Server3 that run Windows Server1 and Server2 and located on the Internal network. Server3 is located on the premises network. All servers have access to Azure.

From Azure Sentinel, you install a Windows firewall data connector.

You need to collect Microsoft Defender Firewall data from the servers for Azure Sentinel. What should you do?

- A. Create an event subscription from Server1, Server2 and Server3
- B. Install the On-premises data gateway on each server.
- C. Install the Microsoft Agent on each server.
- D. Install the Microsoft Agent on Server1 and Server2 install the on-premises data gateway on Server3.

**Answer:** C

**Explanation:**

Reference:

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

**NEW QUESTION 49**

- (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 Azure Active Directory Domain Services (Azure AD DS) to the Azure subscription. Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

**Explanation:**

References:

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

**NEW QUESTION 52**

- (Exam Topic 4)

You have an Azure subscription that contains a storage account and an Azure web app named App1. App1 connects to an Azure Cosmos DB database named Cosmos1 that uses a private endpoint named

Endpoint1. Endpoint1 has the default settings.

You need to validate the name resolution to Cosmos1. Which DNS zone should you use?

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

**Answer:** D

#### NEW QUESTION 55

- (Exam Topic 4)

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

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

You create an Azure container instance named container1 by using File1.yaml. You need to identify where you can access the values of Variable1 and Variable2. What should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Variable1:

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

Variable2:

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

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Reference:

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

#### NEW QUESTION 59

- (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 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 64

- (Exam Topic 4)  
You have an Azure Storage account that contains a blob container named container1 and a client application named App1.  
You need to enable App1 access to container1 by using Azure Active Directory (Azure AD) authentication.  
What should you do? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

From Azure AD:

Register App1.

Create an access package.

Implement an application proxy.

Modify the authentication methods.

From the storage account:

Add a private endpoint.

Regenerate the access key.

Configure Access control (IAM).

Generate a shared access signature (SAS).

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 68

- (Exam Topic 4)  
You have an Azure subscription that contains an Azure SQL Database logic server named SQL! and an Azure virtual machine named VM1. VM1 uses a private IP

address only.

The Firewall and virtual networks settings for SQL1 are shown in the following exhibit.

Save Discard Add client IP

Deny public network access

Yes No

Click here to create a new private endpoint.  
Create Private Endpoint

Minimum TLS Version

1.0 1.1 1.2

Connection Policy

Default Proxy Redirect

Allow Azure services and resources to access this server

Yes No

Client IP address 89.212.25.106

Rule name	Start IP	End IP

No firewall rules configured.

Virtual networks  
+ Add existing virtual network + Create new virtual network

Rule name	Virtual network	Subnet
No vnet rules for this server.		

You need to ensure that VM1 can connect to SQL1. The solution must use the principle of least privilege. What should you do?

- A. Add an existing virtual network.
- B. Set Connection Policy to Proxy.
- C. Create a new firewall rule.
- D. Set Allow Azure services and resources to access this server to Yes.

Answer: C

### NEW QUESTION 73

- (Exam Topic 4)

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

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

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

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

The subscription contains the subnets shown in the following table.

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

The subscription contains the routes shown in the following table.

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

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

Answer Area

Statements	Yes	No
Traffic from Subnet1-1 to Subnet 1-2 is routed through Fw1.	<input type="radio"/>	<input type="radio"/>
Traffic from Subnet2-1 to Subnet 1-1 is routed through Fw1.	<input type="radio"/>	<input type="radio"/>
Traffic from Subnet3-1 to the internet is routed through Fw1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

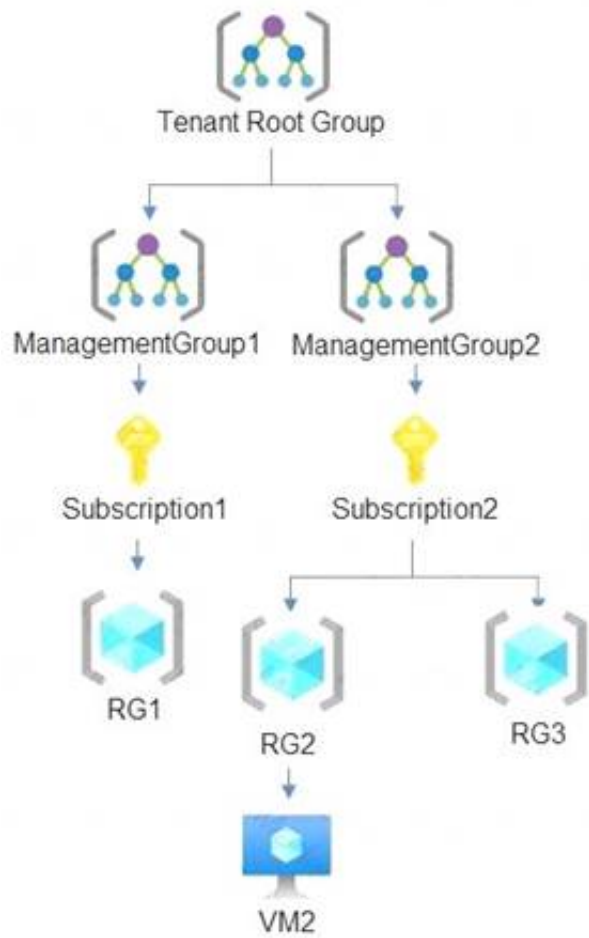
Explanation:

Answer Area

Statements	Yes	No
Traffic from Subnet1-1 to Subnet 1-2 is routed through Fw1.	<input checked="" type="radio"/>	<input type="radio"/>
Traffic from Subnet2-1 to Subnet 1-1 is routed through Fw1.	<input type="radio"/>	<input checked="" type="radio"/>
Traffic from Subnet3-1 to the internet is routed through Fw1.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 77

- (Exam Topic 4)  
You have the hierarchy of Azure resources shown in the following exhibit.



RG1, RG2, and RG3 are resource groups. RG2 contains a virtual machine named VM1.  
You assign role-based access control (RBAC) roles to the users shown in the following table.



Name	Role	Added to resource
User1	Contributor	Tenant Root Group
User2	Virtual Machine Contributor	Subscription2
User3	Virtual Machine Administrator Login	RG2

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

Statements	Yes	No
User1 can deploy virtual machines to RG1.	<input type="radio"/>	<input type="radio"/>
User2 can delete VM2.	<input type="radio"/>	<input type="radio"/>
User3 can reset the password of the built-in Administrator account of VM2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Statements	Yes	No
User1 can deploy virtual machines to RG1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can delete VM2.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can reset the password of the built-in Administrator account of VM2.	<input type="radio"/>	<input checked="" type="radio"/>

#### NEW QUESTION 80

- (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 82

- (Exam Topic 4)

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

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

Which section of the dashboard should you review?

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

**Answer:** C

#### NEW QUESTION 83

- (Exam Topic 4)



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

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

**Answer:** A

#### NEW QUESTION 86

- (Exam Topic 4)

You create an alert rule that has the following settings:

- > Resource: RG1
- > Condition: All Administrative operations
- > Actions: Action groups configured for this alert rule: ActionGroup1
- > Alert rule name: Alert1

You create an action rule that has the following settings:

- > Scope: VM1
- > Filter criteria: Resource Type = "Virtual Machines"
- > Define on this scope: Suppression
- > Suppression config: From now (always)
- > Name: ActionRule1

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

Statements	Yes	No
If you start VM1, an alert is triggered.	<input type="radio"/>	<input type="radio"/>
If you start VM2, an alert is triggered.	<input type="radio"/>	<input type="radio"/>
If you add a tag to RG1, an alert is triggered.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Box 1:

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

Box 2:

The scope for the action rule is not set to VM2. Box 3:

Adding a tag is not an administrative operation. References:

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

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

#### NEW QUESTION 90

- (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 93**

- (Exam Topic 4)

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains a user named User1.

You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains an Azure Storage account named storage1. Storage1 contains an Azure file share named share1.

Currently, the domain and the tenant are not integrated.

You need to ensure that User1 can access share1 by using his domain credentials.

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

**Actions**

**Answer Area**

Create a private link to storage1.

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

Implement Azure AD Connect.

Create a service endpoint to storage1.

Assign share-level permissions for share1.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 98**

- (Exam Topic 4)

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

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

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

Which two values should you specify in the code to automate the deployment of the extension to the virtual machines? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

**Answer:** AC

**NEW QUESTION 101**

- (Exam Topic 4)

You have the role assignments shown in the following exhibit.

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

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.  
NOTE: Each correct selection is worth one point.

[answer choice] can delete VM1.

Only Admin1

Only Admin1 and Admin2

Only Admin1 and Admin3

Only Admin1 and Admin4

Admin1, Admin2, Admin3, and Admin4

[answer choice] can create new resource groups.

Admin1 only

Admin2 only

Admin3 only

Admin1 and Admin3 only

Admin1, Admin2, Admin3, and Admin4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

[answer choice] can delete VM1.

Only Admin1

Only Admin1 and Admin2

Only Admin1 and Admin3

Only Admin1 and Admin4

Admin1, Admin2, Admin3, and Admin4

[answer choice] can create new resource groups.

Admin1 only

Admin2 only

Admin3 only

Admin1 and Admin3 only

Admin1, Admin2, Admin3, and Admin4

NEW QUESTION 102

- (Exam Topic 4)

You have an Azure subscription that contains two virtual machines named VM1 and VM2 that run Windows Server 2019. You are implementing Update Management in Azure Automation. You plan to create a new update deployment named Update1. You need to ensure that Update1 meets the following requirements:

- Automatically applies updates to VM1 and VM2.
- Automatically adds any new Windows Server 2019 virtual machines to Update1. What should you include in Update1?

- A. a security group that has a Membership type of Dynamic Device
- B. a security group that has a Membership type of Assigned
- C. a Kusto query language query
- D. a dynamic group query

Answer: D

NEW QUESTION 103

- (Exam Topic 4)

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



Name	Pattern	Case sensitivity
Condition1	White	On
Condition2	Black	Off

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

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

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

What should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

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

▼

No label

Label1 only

Label2 only

Label1 and Label2

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

▼

No label

Label1 only

Label2 only

Label1 and Label2

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Label 2 only

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

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

➤ The most sensitive label is applied.

➤ The last sublabel is applied.

Box 2: No Label

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

References:

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

**NEW QUESTION 107**

- (Exam Topic 4)

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

Each subscription contains a resource group named RG1.

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

➤ The members of Group1 are assigned the Owner role.

➤ The modification of permissions to RG1 is prevented.

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

NOTE: Each correct selection is worth one point.

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

▼

Azure Blueprints

Azure Policy

Azure Security Center

Prevent the modification of permissions to RG1 by using:

▼

A resource lock

A role-based access control (RBAC) role assignment at the resource group level

Azure Blueprint assignments in locking mode

- A. Mastered  
B. Not Mastered



Answer: A

**Explanation:**

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

▼

Azure Blueprints |

Azure Policy

Azure Security Center

Prevent the modification of permissions to RG1 by using:

▼

A resource lock

A role-based access control (RBAC) role assignment at the resource group level

Azure Blueprint assignments in locking mode

**NEW QUESTION 108**

- (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 110**

- (Exam Topic 4)

You have an Azure subscription that contains a user named User1 and a storage account named storage 1. The storage1 account contains the resources shown in the following table:

Name	Type
container1	Container
folder1	File share
table1	Table

User1 is assigned the following roles for storage1:

- Storage Blob Data Reader
- Storage Table Data Contributor
- Storage File Data SMB Share Reader

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

A. Mastered

B. Not Mastered

**Answer:** A

**Explanation:**

No, Yes, No

#### NEW QUESTION 111

- (Exam Topic 4)

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

Name	Type
Container1	Blob container
Share1	File share

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

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

NOTE: Each correct selection is worth one point.

**Answer Area**

Tools for Container1: ☐ Robocopy.exe ☐ Azure Storage Explorer ☐ File Explorer

Tools for Share1: ☐ Robocopy.exe ☐ Azure Storage Explorer ☐ File Explorer

A. Mastered

B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Tools for Container1: ☒ Robocopy.exe ☒ Azure Storage Explorer ☐ File Explorer

Tools for Share1: ☒ Robocopy.exe ☒ Azure Storage Explorer ☐ File Explorer

#### NEW QUESTION 112

- (Exam Topic 4)

You plan to use Azure Resource Manager templates to perform multiple deployments of identically configured Azure virtual machines. The password for the administrator account of each deployment is stored as a secret in different Azure key vaults.

You need to identify a method to dynamically construct a resource ID that will designate the key vault containing the appropriate secret during each deployment.

The name of the key vault and the name of the secret will be provided as inline parameters.

What should you use to construct the resource ID?

A. a key vault access policy

B. a linked template

C. a parameters file

D. an automation account

**Answer:** C

**Explanation:**

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-cli#r>

#### NEW QUESTION 113

- (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 114**

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant named contoso.com

You need to configure diagnostic settings for contoso.com. The solution must meet the following requirements:

- Retain logs for two years.
- Query logs by using the Kusto query language
- Minimize administrative effort. Where should you store the logs?

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

**Answer:** A

**Explanation:**

<https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/get-started-queries>

**NEW QUESTION 115**

- (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 117**

- (Exam Topic 4)

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

You need to ensure that User1 can create and manage administrative units. The solution must use the principle of least privilege.

Which role should you assign to User1?

- A. Privileged role administrator
- B. Helpdesk administrator
- C. Global administrator
- D. Security administrator

**Answer:** A

**NEW QUESTION 121**

- (Exam Topic 4) You have an Azure subscription. You plan to create a storage account.

You need to use customer-managed keys to encrypt the tables in the storage account.

From Azure Cloud Shell, which three cmdlets should you run in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the correct order.

**Cmdlets**

**Answer Area**

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



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Text, table Description automatically generated with medium confidence  
Reference:  
https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-configure-key-vault?tabs=pow

NEW QUESTION 125

- (Exam Topic 4)  
You have an Azure subscription named Sub1.  
You create a virtual network that contains one subnet. On the subnet, you provision the virtual machines shown in the following table.

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

Currently, you have not provisioned any network security groups (NSGs). You need to implement network security to meet the following requirements:

- > Allow traffic to VM4 from VM3 only.
- > Allow traffic from the Internet to VM1 and VM2 only.
- > Minimize the number of NSGs and network security rules.

How many NSGs and network security rules should you create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

NSGs:

▼

1

2

3

4

Network security rules:

▼

1

2

3

4

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

NSGs: 1  
Network security rules: 3  
Not 2: You cannot specify multiple service tags or application groups) in a security rule. References:  
https://docs.microsoft.com/en-us/azure/virtual-network/security-overview

NEW QUESTION 127

- (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 5  
You need to ensure that only devices connected to a 131-107.0.0/16 subnet can access data in the rg1lod28681041 Azure Storage account.

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

To ensure that only devices connected to a 131-107.0.0/16 subnet can access data in the rg1lod28681041 Azure Storage account, you can follow these steps:

- > In the Azure portal, search for and select the storage account named rg1lod28681041.
- > In the left pane, select Firewalls and virtual networks.
- > In the Firewalls and virtual networks pane, select Selected networks.
- > In the Selected networks pane, select Add existing virtual network.
- > In the Add existing virtual network pane, select the virtual network that contains the 131-107.0.0/16 subnet.



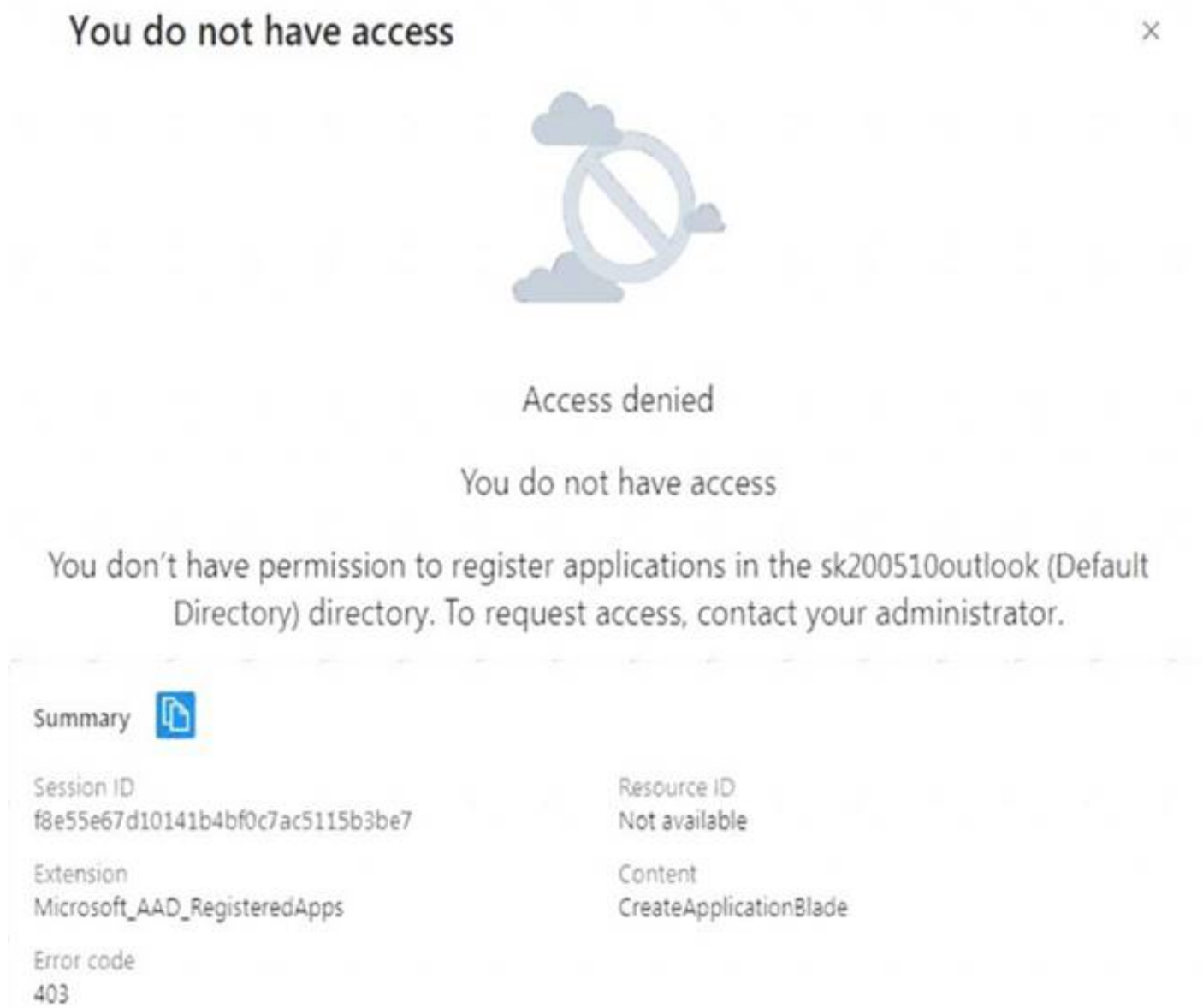
> Select Add.  
<https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security>

### NEW QUESTION 130

- (Exam Topic 4)

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

When a developer attempts to register an app named App1 in the tenant, the developer receives the error message shown in the following exhibit.



You need to ensure that the developer can register App1 in the tenant. What should you do for the tenant?

- A. Modify the User settings
- B. Set Enable Security default to Yes.
- C. Modify the Directory properties.
- D. Configure the Consent and permissions settings for enterprise applications.

**Answer:** A

#### Explanation:

Reference:

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

### NEW QUESTION 132

- (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.



- 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 137**

- (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 138**

- (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 142**

- (Exam Topic 4)

You plan to deploy a custom policy initiative for Microsoft Defender for Cloud. You need to identify all the resource groups that have a Delete lock.

How should you complete the policy definition? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 147

- (Exam Topic 4)

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

Name	Location	Virtual network name
VM1	East US	VNET1
VM2	West US	VNET2
VM3	East US	VNET1
VM4	West US	VNET3

All the virtual networks are peered. You deploy Azure Bastion to VNET2. Which virtual machines can be protected by the bastion host?

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

**Answer:** A

**Explanation:**

<https://docs.microsoft.com/en-us/azure/bastion/vnet-peering>

#### NEW QUESTION 149

- (Exam Topic 4)

You have an Azure subscription.

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

- When a new virtual machine is deployed, automatically install a custom security extension.
- Trigger an autogenerated remediation task for non-compliant virtual machines to install the extension.

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

NOTE: Each correct selection is worth one point.

Definition effect:

▼

Append

DeployIfNotExists

EnforceOPAConstraint

EnforceRegoPolicy

Modify

Assignment remediation task:

▼

A managed identity that has the Contributor role

A managed identity that has the User Access Administrator role

A service principal that has the Contributor role

A service principal that has the User Access Administrator role

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

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

#### NEW QUESTION 154

- (Exam Topic 4)

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

Name	Type	Description
RG1	Resource group	Used to store virtual machines
RG2	Resource group	Used to store virtual networks
ServerAdmins	Security group	Used to manage virtual machines

You need to ensure that ServerAdmins can perform the following tasks: Create virtual machine to the existing virtual network in RG2 only. The solution must use the principle of least privilege.

Which two role-based access control (RBAC) roles should you assign to ServerAdmins? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. the Contributor role for the subscription
- B. the Network Contributor role for RG2
- C. A custom RBAC role for the subscription
- D. a custom RBAC role for RG2
- E. the Network Contributor role for RG1.
- F. the Virtual Machine Contributor role for RG1.



Answer: DF

#### NEW QUESTION 159

- (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 162

- (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	None
User2	Contributor	None
User3	Security Admin	None
User4	None	Service administrator

You create a resource group named RG1.

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

NOTE: Each correct selection is worth one point.

Users who can modify the permissions for RG1:

User1 only

User1 and User2 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

Users who can create virtual networks in RG1:

User1 only

User1 and User2 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

- 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 165

- (Exam Topic 4)

You have an Azure virtual machine named VM1.

From Azure Security Center, you get the following high-severity recommendation: "Install endpoint protection solutions on virtual machine".

You need to resolve the issue causing the high-severity recommendation. What should you do?

- A. Add the Microsoft Antimalware extension to VM1.
- B. Install Microsoft System Center Security Management Pack for Endpoint Protection on VM1.
- C. Add the Network Watcher Agent for Windows extension to VM1.
- D. Onboard VM1 to Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).

Answer: A

**Explanation:**

Reference:

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

**NEW QUESTION 170**

- (Exam Topic 4)

You have an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry. You need to use automatically generated service principal for the AKS cluster to authenticate to the Azure Container Registry.  
What should you create?

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

**Answer:** B

**Explanation:**

References:

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

**NEW QUESTION 172**

- (Exam Topic 4)

You have an Azure subscription mat contains a resource group named RG1. RG1 contains a storage account named storage1.  
You have two custom Azure roles named Role1 and Role2 that are scoped to RG1. The permissions for Role1 are shown in the following JSON code.

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

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

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

Answer Area	Statements	Yes	No
	User1 can read data in storage1.	<input type="radio"/>	<input type="radio"/>
	User2 can read data in storage1.	<input type="radio"/>	<input type="radio"/>
	User3 can restore storage1 from a backup in Azure Backup.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area	Statements	Yes	No
	User1 can read data in storage1.	<input checked="" type="radio"/>	<input type="radio"/>
	User2 can read data in storage1.	<input checked="" type="radio"/>	<input type="radio"/>
	User3 can restore storage1 from a backup in Azure Backup.	<input type="radio"/>	<input checked="" type="radio"/>

# NEW QUESTION 174

- (Exam Topic 4)

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

Save Discard Upload Download

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

```
1 {
2   "id": "d6b00db3-7ef4-4f3c-ble7-8346f0a59546",
3   "acceptMappedClaims": null,
4   "accessTokenAcceptedVersion": null,
5   "addIns": [],
6   "allowPublicClient": null,
7   "appId": "88137405-6a75-4c20-903a-f7b18ff7d496",
8   "appRoles": [],
9   "oauth2AllowUrlPathMatching": false,
10  "createdDateTime": "2019-07-15T21:09:20Z",
11  "groupMembershipClaims": null,
12  "identifierUris": [],
13  "informationalUrls": {
14    "termsOfService": null,
15    "support": null,
16    "privacy": null,
17    "marketing": null
18  },
19  "keyCredentials": [],
20  "knownClientApplications": [],
21  "logoUrl": null,
22  "logoutUrl": null,
23  "name": "AKSAzureADServer",
24  "oauth2AllowIdTokenImplicitFlow": false,
25  "oauth2AllowImplicitFlow": false,
26  "oauth2Permissions": [],
27  "oauth2RequirePostResponse": false,
28  "optionalClaims": null,
29  "orgRestrictions": [],
30  "parentalControlSettings": {
```

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

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

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli> <https://www.codeproject.com/Articles/3211864/Operation-and-Maintenance-of-AKS-Applications>

# NEW QUESTION 179

- (Exam Topic 4)

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

Name	Type	Description
EventHub1	Azure Event Hubs	Not applicable
Adf1	Azure Data Factory	Not applicable
NVA1	Network virtual appliance (NVA)	The NVA sends security event messages in the Common Event Format (CEF).

You have an Azure subscription named Subscription2 that contains the following resources:

- > An Azure Sentinel workspace
- > An Azure Event Grid instance

You need to ingest the CEF messages from the NVAs to Azure Sentinel. NOTE: Each correct selection is worth one point.

Answer Area

Subscription1:	<input type="checkbox"/> An Azure Log Analytics agent on a Linux virtual machine <input type="checkbox"/> A Data Factory pipeline <input type="checkbox"/> An Event Hubs namespace <input type="checkbox"/> An Azure Service Bus queue
Subscription2:	<input type="checkbox"/> A new Azure Log Analytics workspace <input type="checkbox"/> A new Azure Sentinel data connector <input type="checkbox"/> A new Azure Sentinel playbook <input type="checkbox"/> A new Event Grid resource provider

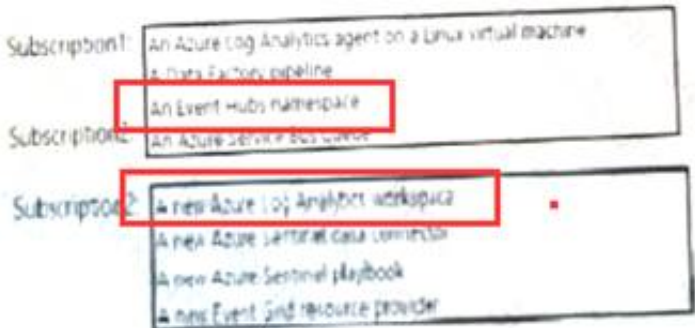


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 184

- (Exam Topic 4)

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

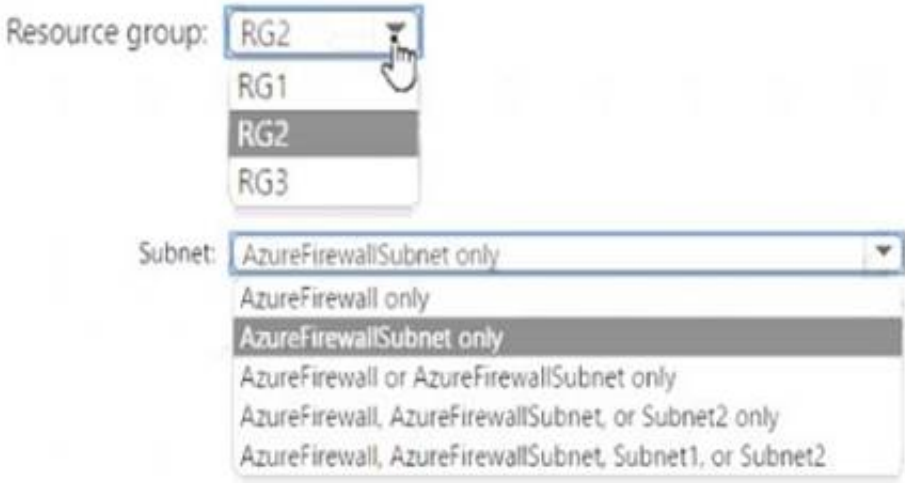
Name	Type	Location	In resource group
RG1	Resource group	East US	Not applicable
RG2	Resource group	West US	Not applicable
RG3	Resource group	Central US	Not applicable
VNet1	Virtual network	Central US	RG2

VNet1 contains the subnets shown in the following table.

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

You plan to use the Azure portal to deploy an Azure firewall named AzFW1 to VNet1.  
Which resource group and subnet can you use to deploy AzFW1? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

Answer Area

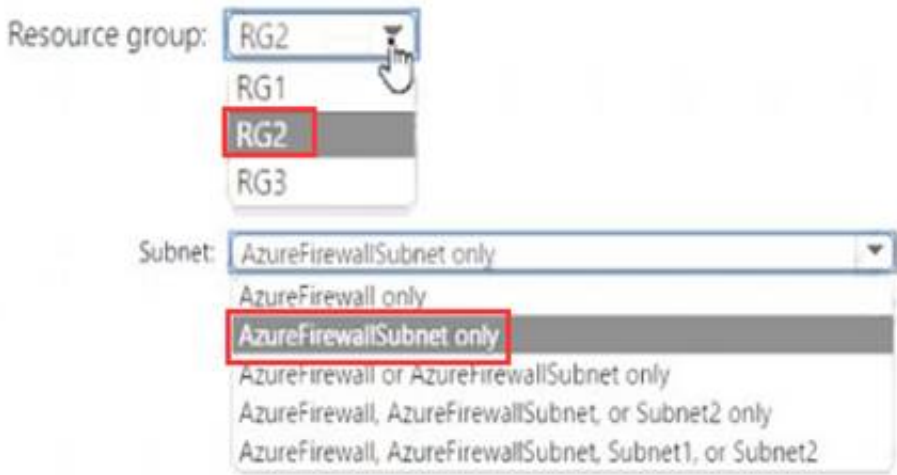


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area





### NEW QUESTION 188

- (Exam Topic 4)

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

Name	Resource group
VM1	RG1
VM2	RG2
VM3	RG1
VM4	RG2

You need to ensure that the virtual machines in RG1 have the Remote Desktop port closed until an authorized user requests access. What should you configure?

- A. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
- B. an application security group
- C. Azure Active Directory (Azure AD) conditional access
- D. just in time (JIT) VM access

**Answer:** D

#### Explanation:

Just-in-time (JIT) virtual machine (VM) access can be used to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.

Note: When just-in-time is enabled, Security Center locks down inbound traffic to your Azure VMs by creating an NSG rule. You select the ports on the VM to which inbound traffic will be locked down. These ports are controlled by the just-in-time solution.

When a user requests access to a VM, Security Center checks that the user has Role-Based Access Control (RBAC) permissions that permit them to successfully request access to a VM. If the request is approved, Security Center automatically configures the Network Security Groups (NSGs) and Azure Firewall to allow inbound traffic to the selected ports and requested source IP addresses or ranges, for the amount of time that was specified. After the time has expired, Security Center restores the NSGs to their previous states. Those connections that are already established are not being interrupted, however.

Reference:

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

### NEW QUESTION 192

- (Exam Topic 4)

From Azure Security, you create a custom alert rule.

You need to configure which users will receive an email message when the alert is triggered. What should you do?

- A. From Azure Monitor, create an action group.
- B. From Security Center, modify the Security policy settings of the Azure subscription.
- C. From Azure Active Directory (Azure AD), modify the members of the Security Reader role group.
- D. From Security Center, modify the alert rule.

**Answer:** A

#### Explanation:

References:

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

### NEW QUESTION 193

- (Exam Topic 4)

You have an Azure key vault named KeyVault1 that contains the items shown in the following table.

Name	Type
Item1	Key
Item2	Secret
Policy1	Access policy

In KeyVault1 the following events occur in sequence:

- item is deleted.
- Item2 and Policy1 are deleted.

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

Statements	Yes	No
You can recover Policy1.	<input type="radio"/>	<input type="radio"/>
You can add a new key named Item1.	<input type="radio"/>	<input type="radio"/>
You can add a new secret named Item2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
You can recover Policy1.	<input type="radio"/>	<input checked="" type="radio"/>
You can add a new key named Item1.	<input type="radio"/>	<input checked="" type="radio"/>
You can add a new secret named Item2.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 198

- (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 that contains a Microsoft Sentinel workspace.

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

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

- When Microsoft Sentinel identifies a threat an incident must be created.
- A ticket must be logged in the service management platform when an incident is created in Microsoft Sentinel.

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

NOTE: Each correct selection is worth one point.

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

▼

Analytics

Data connectors

Playbooks

Workbooks

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

▼

Analytics

Data connectors

Playbooks

Workbooks

- A. Mastered  
 B. Not Mastered

Answer: A

Explanation:

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

▼

Analytics

Data connectors

Playbooks

Workbooks

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

▼

Analytics

Data connectors

Playbooks

Workbooks

#### NEW QUESTION 204

- (Exam Topic 4)

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

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

You plan to enable Azure Defender for the subscription. Which resources can be protected by using Azure Defender?

- A. VM1, VNET1, storage1, and Vault1  
 B. VM1, VNET1, and storage1 only  
 C. VM1, storage1, and Vault1 only  
 D. VM1 and VNET1 only  
 E. VM1 and storage1 only

Answer: A

Explanation:

Reference:

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

#### NEW QUESTION 209

- (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

...

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 210

- (Exam Topic 4)

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



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

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

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

**Answer: C**

**Explanation:**

Note: Create a workspace

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

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

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

Select a Subscription to link to by selecting from the drop-down list if the default selected is not appropriate. For Resource Group, select an existing resource group that contains one or more Azure virtual machines. Select the Location your VMs are deployed to. For additional information, see which regions Log Analytics is available in.

**NEW QUESTION 212**

- (Exam Topic 4)

On Monday, you configure an email notification in Azure Security Center to notify user user1@contoso.com. On Tuesday, Security Center generates the security alerts shown in the following table.

Time	Description	Severity
01:00	Failed RDP brute force attack	Medium
01:01	Successful RDP brute force attack	High
06:10	Suspicious process executed	High
09:00	Malicious SQL activity	High
11:15	Network communication with a malicious machine detected	Low
13:30	Suspicious process executed	High
14:00	Failed RDP brute force attack	Medium
16:01	Successful RDP brute force attack	High
23:20	Possible outgoing spam activity detected	Low
23:25	Modified system binary discovered in dump file	High
23:30	Malicious SQL activity	High

How many email notifications will user1@contoso.com receive on Tuesday? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Total number of Security Center email notifications about an RDP

brute force attack on Tuesday:

▼

1

2

3

4

Total number of Security Center email notifications on Tuesday:

▼

3

4

6

9

11

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details>

#### NEW QUESTION 215

- (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 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 216

- (Exam Topic 4)

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

You need to prevent nonprivileged Azure AD users from creating service principals in Azure AD. What should you do in the Azure Active Directory admin center of the tenant?

A. From the Properties blade, set Enable Security defaults to Yes.

B. From the Properties blade, set Access management for Azure resources to No

C. From the User settings blade, set Users can register applications to No

D. From the User settings blade, set Restrict access to Azure AD administration portal to Yes.

**Answer: C**

#### NEW QUESTION 221

- (Exam Topic 4)

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

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

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

A. Assign User1 the Authentication Policy Administrator role.

B. Enable Azure AD Password Protection.

C. Configure a multi-factor authentication (MFA) registration policy.

D. Create a new app registration.

**Answer: C**

#### NEW QUESTION 224

- (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 226

- (Exam Topic 4)

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

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

You create the Azure policy shown in the following exhibit.

Basics	Parameters	Remediation	Non-compliance messages	Review + create
<b>Basics</b>				
Scope	Azure Pass - Sponsorship/RG1			
Exclusions	Azure Pass - Sponsorship/RG1/NSG1			
Policy definition	Flow logs should be enabled for every network security group			
Assignment name	Flow logs should be enabled for every network security group			
Description	Description1			
Policy enforcement	Enabled			
Assigned by	Admin1			
<b>Parameters</b>				
effect	Audit			
<b>Remediation</b>				
Create managed identity	Yes			
Managed identity location	westeurope			
Create a remediation task	No			
<b>Non-compliance messages</b>				
Default non-compliance message	Message1			

You assign the policy to RG1.

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

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

**Answer:** B

#### NEW QUESTION 229

- (Exam Topic 4)

HOTSPOT

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

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

The company is sold to a new owner.

The company needs to transfer ownership of Subscription1.

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

NOTE: Each correct selection is worth one point.

User:

	▼
User1	
User2	
User3	
User4	

Tool:

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1; User2

Billing Administrator

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

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

Box 2: Azure Account Center Azure Account Center can be used. Reference:

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

**NEW QUESTION 234**

- (Exam Topic 4)

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

Name	Type	Description
RG1	Resource group	Used to store virtual machines
RG2	Resource group	Used to store virtual networks
ServerAdmins	Security group	Used to manage virtual machines

You need to ensure that ServerAdmins can perform the following tasks:

- > Create virtual machines in RG1 only.
- > Connect the virtual machines to the existing virtual networks in RG2 only.

The solution must use the principle of least privilege.

Which two role-based access control (RBAC) roles should you assign to ServerAdmins? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a custom RBAC role for RG2
- B. the Network Contributor role for RG2
- C. the Contributor role for the subscription
- D. a custom RBAC role for the subscription
- E. the Network Contributor role for RG1
- F. the Virtual Machine Contributor role for RG1

**Answer:** AF

**Explanation:**

Reference:

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

**NEW QUESTION 236**

- (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 237

- (Exam Topic 4)

You have an Azure subscription named Sub1.

In Azure Security Center, you have a security playbook named Play1. Play1 is configured to send an email message to a user named User1.

You need to modify Play1 to send email messages to a distribution group named Alerts. What should you use to modify Play1?

- A. Azure DevOps
- B. Azure Application Insights
- C. Azure Monitor
- D. Azure Logic Apps Designer

**Answer:** D

#### Explanation:

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

References:

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

#### NEW QUESTION 240

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

**Answer:** A

#### Explanation:

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

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

References:

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

#### NEW QUESTION 245

- (Exam Topic 4)

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

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

You need to create a custom sensitivity label. What should you do first?

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

**Answer:** A

#### Explanation:

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

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

#### NEW QUESTION 247

- (Exam Topic 4)

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

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

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

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

NOTE: Each correct selection is worth one point.

You can restore the Secret1 backup to:

▼

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

You can restore the Key1 backup to:

▼

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

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

The backups can only be restored to key vaults in the same subscription and same geography. You can restore to a different region in the same geography.

<https://docs.microsoft.com/en-us/azure/key-vault/general/backup?tabs=azure-cli>

#### NEW QUESTION 250

- (Exam Topic 4)

Your company plans to create separate subscriptions for each department. Each subscription will be associated to the same Azure Active Directory (Azure AD) tenant.

You need to configure each subscription to have the same role assignments. What should you use?

- A. Azure Security Center
- B. Azure Policy
- C. Azure AD Privileged Identity Management (PIM)
- D. Azure Blueprints

**Answer:** D

#### Explanation:

Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of

Azure resources that implements and adheres to an organization's standards, patterns, and requirements.

Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

- Role Assignments
- Policy Assignments
- Azure Resource Manager templates
- Resource Groups

Reference:

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

#### NEW QUESTION 254

- (Exam Topic 4)

You create a new Azure subscription.

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

- A. Onboard Azure Active Directory (Azure AD) Identity Protection.
- B. Create an Azure Storage account.
- C. Implement Azure Advisor recommendations.
- D. Create an Azure Log Analytics workspace.

E. Upgrade the pricing tier of Security Center to Standard.

**Answer:** DE

**Explanation:**

D: You need write permission in the workspace that you select to store your custom alert. References:  
<https://docs.microsoft.com/en-us/azure/security-center/security-center-custom-alert>

**NEW QUESTION 257**

- (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 261**

- (Exam Topic 3)

You need to configure support for Azure Sentinel notebooks to meet the technical requirements. What is the minimum number of Azure container registries and Azure Machine Learning workspaces required?

Container registries:

	▼
0	
1	
2	
3	

Workspaces:

	▼
0	
1	
2	
3	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Table Description automatically generated with medium confidence  
Reference:  
<https://docs.microsoft.com/en-us/azure/sentinel/notebooks>

**NEW QUESTION 263**

- (Exam Topic 2)

You need to ensure that User2 can implement PIM. What should you do first?

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

**Answer:** D

**Explanation:**

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

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

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

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

References:

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

#### NEW QUESTION 264

- (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 268

- (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 273

- (Exam Topic 1)

You need to ensure that users can access VM0. The solution must meet the platform protection requirements. What should you do?

- A. Move VM0 to Subnet1.
- B. On Firewall, configure a network traffic filtering rule.
- C. Assign RT1 to AzureFirewallSubnet.
- D. On Firewall, configure a DNAT rule.

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 278

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual az-500 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the az-500 Product From:

<https://www.2passeasy.com/dumps/az-500/>

## Money Back Guarantee

### **az-500 Practice Exam Features:**

- \* az-500 Questions and Answers Updated Frequently
- \* az-500 Practice Questions Verified by Expert Senior Certified Staff
- \* az-500 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* az-500 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year