

Exam Questions az-500

Microsoft Azure Security Technologies

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



NEW QUESTION 1

- (Exam Topic 4)

You have an Azure subscription named Subscription1.

You deploy a Linux virtual machine named VM1 to Subscription1. You need to monitor the metrics and the logs of VM1.

D18912E1457D5D1DDCBD40AB3BF70D5D

What should you use?

- A. the AzurePerformanceDiagnostics extension
- B. Azure HDInsight
- C. Linux Diagnostic Extension (LAD) 3.0
- D. Azure Analysis Services

Answer: A

NEW QUESTION 2

- (Exam Topic 4)

You have Azure Resource Manager templates that you use to deploy Azure virtual machines.

You need to disable unused Windows features automatically as instances of the virtual machines are provisioned.

What should you use?

- A. security policies in Azure Security Center
- B. Azure Logic Apps
- C. an Azure Desired State Configuration (DSC) virtual machine extension
- D. Azure Advisor

Answer: C

NEW QUESTION 3

- (Exam Topic 4)

Lab Task

Task 3

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Create and register an Azure AD application. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to specify a name, such as SQLServerCTP1, and select the supported account types, such as Accounts in this organization directory only.

Grant application permissions. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to assign the Directory.Read.All permission to the application and grant admin consent for your organization.

Create and assign a certificate. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to create a self-signed certificate and upload it to the application. You also need to store the certificate in Azure Key Vault and grant access policies to the application and your SQL Server.

Configure Azure AD authentication for SQL Server through Azure portal. You can use the Azure portal to do this. You need to select your SQL Server resource and enable Azure AD authentication. You also need to select your Azure AD application as the Azure AD admin for your SQL Server.

Create logins and users. You can use SSMS or Transact-SQL to do this. You need to connect to your SQL Server as the Azure AD admin and create a login for Danny-31330471. You also need to create a user for Danny-31330471 in each database that he needs access to.

Connect with a supported authentication method. You can use SSMS or SqlClient to do this. You need to specify the Authentication connection property in the connection string as Active Directory Password or Active Directory Integrated. You also need to provide the username and password of Danny-31330471.

NEW QUESTION 4

- (Exam Topic 4)


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

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

You need to configure authorization access.

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


NOTE: Each correct selection is worth one point.

storage1: 

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

storage2: 

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

storage3: 

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

Reference:

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

NEW QUESTION 5

- (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 6

- (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 7

- (Exam Topic 4)

You have an Azure subscription.

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

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

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

Which resource provider should you use for each role? To answer, drag the appropriate resource providers to the correct roles. Each resource provider may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content

Resource Providers

Microsoft.Compute

Microsoft.Network

Microsoft.Security

Microsoft.Solutions

Answer Area

Role1:

Role2:

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Resource Providers

Microsoft.Compute

Microsoft.Network

Microsoft.Security

Microsoft.Solutions

Answer Area

Role1:

Microsoft.Network

Role2:

Microsoft.Network

NEW QUESTION 8

- (Exam Topic 4)

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

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

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

You plan to deploy an Azure firewall to HubVNet. You create the following two routing tables:

- RT1: Includes a user-defined route that points to the private IP address of the Azure firewall as a next hop address
- RT2: Disables BGP route propagation and defines the private IP address of the Azure firewall as the default gateway

You need to ensure that traffic between SpokeVNetSubnet0 and the on-premises network flows through the Azure firewall.

To which subnet should you associate each route table? To answer, drag the appropriate subnets to the correct route tables. Each subnet may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Subnets

Azure FirewallSubnet

GatewaySubnet

HubVNetSubnet0

Answer Area

RT1:

RT2:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Subnets

Azure FirewallSubnet

GatewaySubnet

HubVNetSubnet0

Answer Area

RT1:

RT2:

GatewaySubnet

HubVNetSubnet0

NEW QUESTION 9

- (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 (AzureAD). You have an Azure HDInsight cluster on a virtual network.

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

Solution: You deploy the On-premises data gateway to the on-premises network. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

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

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

Create Azure Virtual Network.

Create a custom DNS server in the Azure Virtual Network.

Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.

Configure forwarding between the custom DNS server and your on-premises DNS server. References:

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

NEW QUESTION 10

- (Exam Topic 4)

You have an Azure SQL Database server named SQL1.

You plan to turn on Advanced Threat Protection for SQL1 to detect all threat detection types. Which action will Advanced Threat Protection detect as a threat?

- A. A user updates more than 50 percent of the records in a table.
- B. A user attempts to sign as SELECT * from table1.
- C. A user is added to the db_owner database role.
- D. A user deletes more than 100 records from the same table.

Answer: B

Explanation:

Advanced Threat Protection can detect potential SQL injections: This alert is triggered when an active exploit happens against an identified application vulnerability to SQL injection. This means the attacker is trying to inject malicious SQL statements using the vulnerable application code or stored procedures.

References:

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection-overview>

NEW QUESTION 10

- (Exam Topic 4)

On Monday, you configure an email notification in Microsoft Defender for Cloud to notify user1

@contoso.com about alerts that have a severity level of Low, Medium, or High. On Tuesday, Microsoft Defender for Cloud generates the security alerts shown in the following table.

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

How many email notifications will user1 @contoso.com receive on Tuesday? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Total number of Microsoft Defender for Cloud email notifications about an RDP brute force attack on Tuesday:

- 1
- 2
- 3
- 4

Total number of Microsoft Defender for Cloud email notifications on Tuesday:

- 3
- 4
- 7
- 9
- 11

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Total number of Microsoft Defender for Cloud email notifications about an RDP brute force attack on Tuesday:

- 1
- 2
- 3
- 4

Total number of Microsoft Defender for Cloud email notifications on Tuesday:

- 3
- 4
- 7
- 9
- 11

NEW QUESTION 11

- (Exam Topic 4)

You have an app that uses an Azure SQL database.

You need to be notified if a SQL injection attack is launched against the database. What should you do?

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

Answer: C

NEW QUESTION 15

- (Exam Topic 4)

You have an Azure subscription that contains an Azure key vault named Vault1. On January 1, 2019, Vault1 stores the following secrets.

```
Enabled      : False
Expires      :
NotBefore    : 5/1/19 12:00:00 AM
Created      : 12/20/18 2:55:00 PM
Updated      : 12/20/18 2:55:00 PM
ContentType  :
Tags         :
TagTable     :
VaultName    : vault1
Name         : Password1
Version      :
Id           : https://vault1.vault.azure.net:443/secrets/Password1
```

```
Enabled      : True
Expires      : 5/1/19 12:00:00 AM
NotBefore    : 3/1/19 12:00:00 AM
Created      : 12/20/18 3:00:00 PM
Updated      : 12/20/18 3:00:00 PM
ContentType  :
Tags         :
TagsTable    :
VaultName    : vault1
Name         : Password2
Version      :
Id           : https://vault1.vault.azure.net:443/secrets/Password2
```

Which can each secret be used by an application? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Password1:

	▼
Never	
Always	
Only after May 1, 2019	

Password2:

	▼
Never	
Always	
Only between March 1, 2019 and May 1. 2019	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Never Password1 is disabled.

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

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

Reference:

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

NEW QUESTION 20

- (Exam Topic 4)

From the Azure portal, you are configuring an Azure policy.

You plan to assign policies that use the DeployIfNotExist, AuditIfNotExist, Append, and Deny effects. Which effect requires a managed identity for the assignment?

- A. AuditIfNotExist
- B. Append
- C. DeployIfNotExist
- D. Deny

Answer: C

Explanation:

When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity.

References:

<https://docs.microsoft.com/bs-latn-ba/azure/governance/policy/how-to/remediate-resources>

NEW QUESTION 22

- (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 27

- (Exam Topic 4)

You have 15 Azure virtual machines in a resource group named RG1. All virtual machines run identical applications.

You need to prevent unauthorized applications and malware from running on the virtual machines. What should you do?

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

Answer: B

Explanation:

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

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

- Providing security recommendations for the virtual machines. Example recommendations include: app system updates, configure ACLs endpoints, enable antimalware, enable network security groups, and apply disk encryption.
- Monitoring the state of your virtual machines.

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

NEW QUESTION 30

- (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 Principles:

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 Principles:

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 34

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant and a root management group. You create 10 Azure subscriptions and add the subscriptions to the root management group.

You need to create an Azure Blueprints definition that will be stored in the root management group. What should you do first?

- A. Add an Azure Policy definition to the root management group.
- B. Modify the role-based access control (RBAC) role assignments for the root management group.
- C. Create a user-assigned identity.
- D. Create a service principal.

Answer: B

Explanation:

Reference:

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

NEW QUESTION 38

- (Exam Topic 4)

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

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

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

Answer: B

NEW QUESTION 40

- (Exam Topic 4)

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

Name	Type
Key1	Key
Secret1	Secret
Cert1	Certificate

Which resources support the creation of a rotation policy?

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

Answer: A

NEW QUESTION 41

- (Exam Topic 4)

Your on-premises network contains the servers shown in the following table.

Name	Operating system	Description
Server1	Windows Server 2019	Hyper-V host hosting four virtual machines that run Windows Server 2022
Server2	Windows Server 2019	File server that has the Azure Arc agent installed
Server3	SUSE Linux Enterprise Server (SLES)	Database server that has the Azure Arc agent installed

You have an Azure subscription That contains multiple virtual machines that run either Windows Server 2019 Of SLES.

Operating systems:

Windows Server only
SLES and Windows Server

Platforms:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Operating systems:

Windows Server only
SLES and Windows Server

Platforms:

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

NEW QUESTION 45

- (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 46

- (Exam Topic 4)

You have three Azure subscriptions and a user named User1.

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

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

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

Actions

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

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

NEW QUESTION 47

- (Exam Topic 4)

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

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

You have an Azure Subscription. The subscription contains 50 virtual machines that run Windows Server 2012 R2 or Windows Server 2016.

You need to deploy Microsoft Antimalware to the virtual machines. Solution: You add an extension to each virtual machine.

Does this meet the goal?

- A. Yes

B. No

Answer: A

Explanation:

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

References:

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

NEW QUESTION 49

- (Exam Topic 4)

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

Name	Connected to	Private IP address	Public IP address
VM1	VNET1/Subnet1	10.1.1.4	13.80.73.87
VM2	VNET2/Subnet2	10.2.1.4	213.199.133.190
VM3	VNET2/Subnet2	10.2.1.5	None

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

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

Save Discard Refresh

Allow access from

☐ All networks ☒ Selected networks

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

Virtual networks

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

[+ Add new virtual network](#)

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

Firewall

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

Address Range

13.80.73.87

IP address or CIDR

Exceptions

☒ Allow trusted Microsoft services to access this storage account ⓘ

☐ Allow read access to storage logging from any network

☐ Allow read access to storage metrics from any network

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

Statements	Yes	No
From VM1, you can upload a blob to storageacc1.	<input type="radio"/>	<input type="radio"/>
From VM2, you can upload a blob to storageacc1.	<input type="radio"/>	<input type="radio"/>
From VM3 , you can upload a blob to storageacc1.	<input type="radio"/>	<input type="radio"/>

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Box 1: Yes

The public IP of VM1 is allowed through the firewall.

Box 2: No

The allowed virtual network list is empty so VM2 cannot access storageacc1 directly. The public IP address of VM2 is not in the allowed IP list so VM2 cannot access storageacc1 over the Internet.

Box 3: No

The allowed virtual network list is empty so VM3 cannot access storageacc1 directly. VM3 does not have a public IP address so it cannot access storageacc1 over

the Internet.

Reference:

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

NEW QUESTION 51

- (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 56

- (Exam Topic 4)

You have an Azure subscription that contains virtual machines. You enable just in time (JIT) VM access to all the virtual machines.

You need to connect to a virtual machine by using Remote Desktop. What should you do first?

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 60

- (Exam Topic 4)

You have an Azure subscription that uses Azure AD Privileged Identity Management (PIM). A user named User1 is eligible for the Billing administrator role. You need to ensure that the role can only be used for a maximum of two hours. What should you do?

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

Answer: B

NEW QUESTION 62

- (Exam Topic 4)

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

Name	Type
container1	Container
folder1	File Share
table1	Table

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

Allowed services ⓘ

☐ Blob ☒ File ☐ Queue ☐ Table

Allowed resource types ⓘ

☒ Service ☒ Container ☒ Object

Allowed permissions ⓘ

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

Allowed blob index permissions ⓘ

☐ Read/Write ☐ Filter

Start and expiry date/time ⓘ

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

Allowed IP addresses ⓘ

Allowed protocols ⓘ

☒ HTTPS only ☐ HTTPS and HTTP

Preferred routing tier ⓘ

☒ Basic (default) ☐ Microsoft network routing ☐ Internet routing

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

Signing key ⓘ

Generate SAS and connection string

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

Answer Area

SAS1:

Key1:

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Answer Area

SAS1:

Key1:

NEW QUESTION 67

- (Exam Topic 4)

You have an Azure subscription that contains a

You need to grant user1 access to blob1. The solution must ensure that the access expires after six days. What should you use?

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

Answer: C

Explanation:

Depending on how you want to authorize access to blob data in the Azure portal, you'll need specific permissions. In most cases, these permissions are provided via Azure role-based access control (Azure RBAC). For more information about Azure RBAC, see [What is Azure role-based access control \(Azure RBAC\)?](https://learn.microsoft.com/en-us/azure/storage/blobs/authorize-data-operations-portal).

<https://learn.microsoft.com/en-us/azure/storage/blobs/authorize-data-operations-portal>

NEW QUESTION 70

- (Exam Topic 4)

You have an Azure subscription.

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

* Provide access to DDoS rapid response support during active attacks.

* Project Basic SKU public IP addresses.

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

What should you recommend? To answer, drag the appropriate DDoS projection types to the correct requirements. Each DDoS Projection type may be used once, or not at all. You may need to drag the split bar between panes or scroll to view connect.

NOTE: Each correct selection is worth one point.

DDoS Protection types

DDoS infrastructure protection

DDoS IP Protection

DDoS Network Protection

Answer Area

Provide access to DDoS rapid response support during active attacks:

Protect Basic SKU public IP addresses:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

DDoS Protection types

DDoS infrastructure protection

DDoS IP Protection

DDoS Network Protection

Answer Area

Provide access to DDoS rapid response support during active attacks:

DDoS Network Protection

Protect Basic SKU public IP addresses:

DDoS IP Protection

NEW QUESTION 72

- (Exam Topic 4)

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

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

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

Role settings

Assignment

☐ Allow permanent eligible assignment

Expire eligible assignments after

3 Months

☐ Allow permanent active assignment

Expire active assignments after

1 Month

☒ Require Multi-Factor Authentication on active assignment

☒ Require justification on active assignment

Activation

Activation maximum duration (hours)

8

☒ Require Multi-Factor Authentication on activation

☒ Require justification on activation

☐ Require ticket information on activation

☐ Require approval to activate

Select approver

No member or group selected

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

Name	Assignment type
User1	Eligible
User2	Active
User3	Active

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

Statements	Yes	No
On May 15, 2019, User1 can activate the Contributor role.	<input type="radio"/>	<input type="radio"/>
On May 15, 2019, User2 can use the Contributor role.	<input type="radio"/>	<input type="radio"/>
On June 15, 2019, User3 can activate the Contributor role.	<input type="radio"/>	<input type="radio"/>

A. Mastered
B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 76

- (Exam Topic 4)

Passing Certification Exams Made Easy

visit - https://www.2PassEasy.com

You have been tasked with configuring an access review, which you plan to assigned to a new collection of reviews. You also have to make sure that the reviews can be reviewed by resource owners.

You start by creating an access review program and an access review control. You now need to configure the Reviewers.

Which of the following should you set Reviewers to?

- A. Selected users.
- B. Members (Self).
- C. Group Owners.
- D. Anyone.

Answer: C

Explanation:

In the Reviewers section, select either one or more people to review all the users in scope. Or you can select to have the members review their own access. If the resource is a group, you can ask the group owners to review.

Graphical user interface, application Description automatically generated with medium confidence



Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

<https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-programs-controls>

NEW QUESTION 79

- (Exam Topic 4)

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

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

What should you create?

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

Answer: B

NEW QUESTION 80

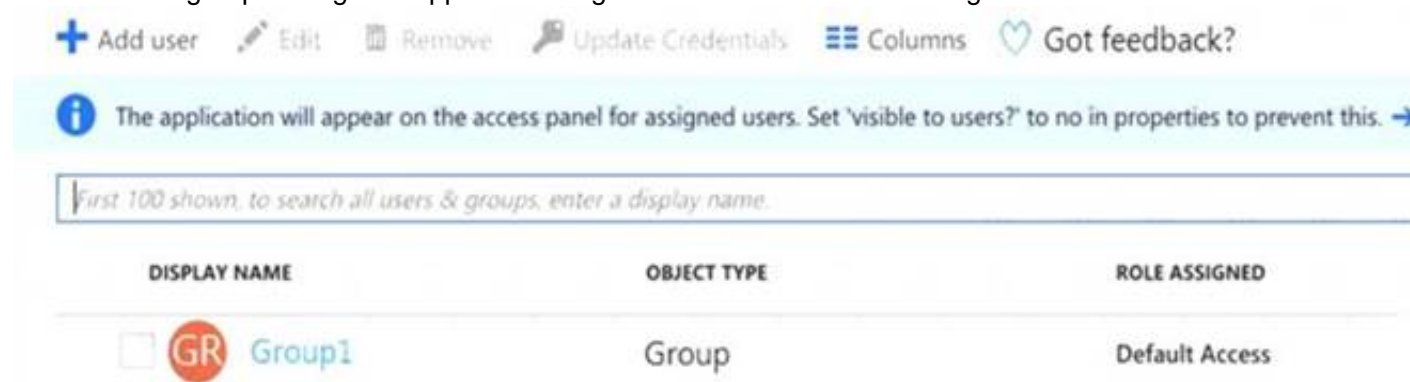
- (Exam Topic 4)

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

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

User2 is the owner of Group2.

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



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

Allow users to request access to this application? ☒ Yes ☐ No

To which group should assigned users be added?

Require approval before granting access to this application? ☒ Yes ☐ No

Who is allowed to approve access to this application?

To which role should users be assigned in this application?

User3 is configured to approve access to Appl.
 You need to identify the owners of Group2 and the users of Appl.
 What should you identify? To answer, select the appropriate options in the answer area.
 NOTE: Each correct selection is worth one point.

Group2 owners:

App1 users:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access>

NEW QUESTION 84

- (Exam Topic 4)

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

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

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

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

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

- A. Yes
- B. No

Answer: B

Explanation:

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

NEW QUESTION 88

- (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 93

- (Exam Topic 4)
DRAG DROP
You create an Azure subscription.
You need to ensure that you can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to secure Azure AD roles.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

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

Consent to PIM.

Sign up PIM for Azure AD roles.

Discover privileged roles.

Discover resources.

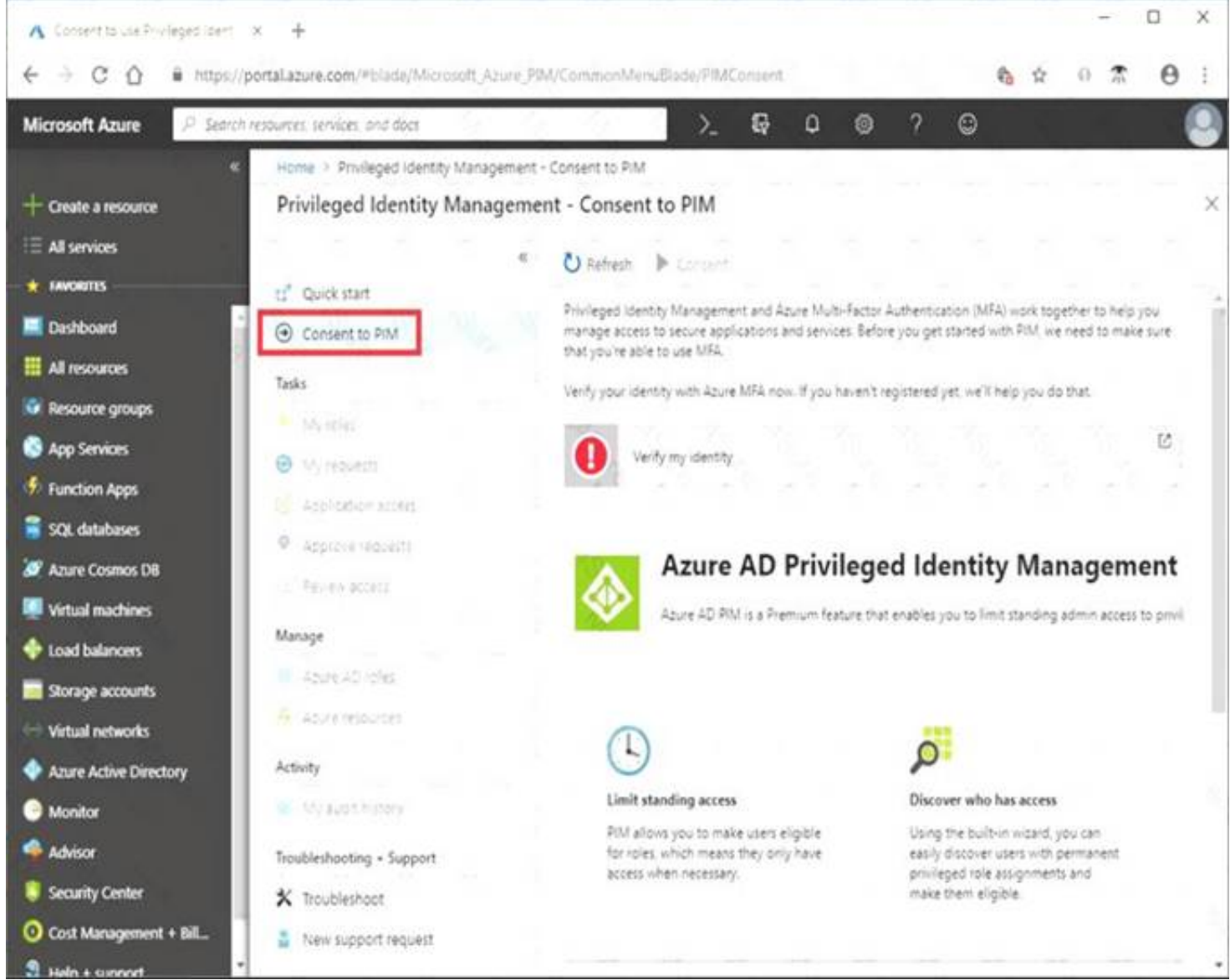
Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Step 1: Consent to PIM



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

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

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

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

NEW QUESTION 96

- (Exam Topic 4)

You have an Azure subscription that uses Microsoft Defender for Cloud. You have accounts for the following cloud services:

- Alibaba Cloud
 - Amazon Web Services (AWS)
 - Google Cloud Platform (GCP)
- What can you add to Defender for Cloud?

- A. AWS only
- B. Alibaba Cloud and AWS only
- C. Alibaba Cloud and GCP only
- D. AWS and GCP only
- E. Alibaba Cloud, AWS, and GCP
- F. AWS, GCP, and Azure

Answer: A

NEW QUESTION 98

- (Exam Topic 4)

Your on-premises network contains the servers shown in the following table.

Name	Operating system	Description
Server1	Windows Server 2019	Hyper-V host hosting four virtual machines that run Windows Server 2022
Server2	Windows Server 2019	File server that has the Azure Arc agent installed
Server3	SUSE Linux Enterprise Server (SLES)	Database server that has the Azure Arc agent installed

You have an Azure subscription that contains multiple virtual machines that run either Windows Server 2019 or SLES. You plan to implement adaptive application controls in Microsoft Defender for Cloud. Which operating systems and platforms can you monitor? To answer, select the appropriate options in the answer area.

Operating systems:

Platforms:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Operating systems:

Platforms:

NEW QUESTION 99

- (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 generate new SASs. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Instead you should create a new stored access policy.

To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it.

References:

<https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy>

NEW QUESTION 103

- (Exam Topic 4)

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

Name	Resource group
storage1	RG1
storage2	RG1
storage3	RG2

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

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

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

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

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

Actions	Answer Area
For storage3, disable the customer-managed keys.	1
Disable Defender for Storage for storage3.	2
Enable the Defender for Storage plan for Sub1.	3
For storage3, assign the AzDefenderPlanAutoEnable tag and set the value to off.	
Enable the Defender for Storage plan for RG1.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions	Answer Area
For storage3, disable the customer-managed keys.	1
Disable Defender for Storage for storage3.	2
Enable the Defender for Storage plan for Sub1.	3
For storage3, assign the AzDefenderPlanAutoEnable tag and set the value to off.	
Enable the Defender for Storage plan for RG1.	

NEW QUESTION 108

- (Exam Topic 4)

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

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

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

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

NOTE: Each correct selection is worth one point.

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

Answer: AC

Explanation:

<https://docs.microsoft.com/en-us/azure/azure-arc/servers/onboard-service-principal>

NEW QUESTION 109

- (Exam Topic 4)

You have an Azure subscription.

You plan to map an online infrastructure and perform vulnerability scanning for the following:

- ASNs
 - Hostnames
 - IP addresses
 - SSL certificates
- What should you use?

- A. Microsoft Defender for Cloud
- B. Microsoft Defender for Identity
- C. Microsoft Defender for Endpoint
- D. Microsoft Defender External Attack Surface Management (Defender EASM)

Answer: A

NEW QUESTION 112

- (Exam Topic 4)

You have an Azure web app named webapp1.

You need to configure continuous deployment for webapp1 by using an Azure Repo. What should you create first?

- A. an Azure Application Insights service
- B. an Azure DevOps organizations
- C. an Azure Storage account
- D. an Azure DevTest Labs lab

Answer: B

Explanation:

To use Azure Repos, make sure your Azure DevOps organization is linked to your Azure subscription. Reference:
<https://docs.microsoft.com/en-us/azure/app-service/deploy-continuous-deployment>

NEW QUESTION 117

- (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 121

- (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 125

- (Exam Topic 4)

You create an Azure subscription with Azure AD Premium P2.

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

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 129

- (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 130

- (Exam Topic 4)

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

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 133

- (Exam Topic 4)

You have an Azure subscription.

You need to deploy an Azure virtual WAN to meet the following requirements:

- Create three secured virtual hubs located in the East US, West US, and North Europe Azure regions.
- Ensure that security rules sync between the regions. What should you use?

- A. Azure Firewall Manager
B. Azure Virtual Network Manager
C. Azure Network Function Manager
D. Azure Front Door

Answer: A

NEW QUESTION 134

- (Exam Topic 4)

Lab Task

Task 7

You need to ensure that connections through an Azure Application Gateway named Homepage-AGW are inspected for malicious requests.

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Enable Web Application Firewall (WAF) for the application gateway. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to select a WAF policy and a WAF mode for the application gateway. You can choose a predefined policy or create a custom policy with your own rules and exclusions.

Configure WAF policy settings. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to select the managed rulesets and rule groups that you want to enable or disable for the WAF policy. You can also configure custom rules to match specific patterns or conditions and take actions such as blocking or logging requests.

Monitor WAF logs. You can use different types of logs in Azure to manage and troubleshoot the application gateway and the WAF policy. You can access some of these logs through the portal, such as metrics and health probes. You can also export the logs to Azure Storage, Event Hubs, or Log Analytics and view them in different tools, such as Azure Monitor, Excel, or Power BI.

NEW QUESTION 137

- (Exam Topic 4)

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

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

You deploy and configure an Azure Key vault.

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

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

NOTE: Each correct selection is worth one point.

VM1: ▼

The operating system version
The tier
The type

VM2: ▼

The operating system version
The tier
The type

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

VM1: The Tier

The Tier needs to be upgraded to standard.

Disk Encryption for Windows and Linux IaaS VMs is in General Availability in all Azure public regions and Azure Government regions for Standard VMs and VMs with Azure Premium Storage.

VM2: the operating system

References:

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

NEW QUESTION 139

- (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 142

- (Exam Topic 4)

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

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

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

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

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

- A. Yes
- B. No

Answer: B

NEW QUESTION 144

- (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.

Name	Resource group	TDE
SQL2	RG2	Disabled
SQL3	RG1	Disabled

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
SQL1 will have TDE enabled automatically.	<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

Reference:

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

NEW QUESTION 147

- (Exam Topic 4)

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

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

Answer: A

Explanation:

Reference:

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

NEW QUESTION 151

- (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 155

- (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

New-AzStorageAccountKey

New-AzStorageTable

Register-AzProviderFeature

New-AzStorageAccount

Register-AzResourceProvider

>

<

Answer Area

- 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 156

- (Exam Topic 4)
You have two Azure subscriptions named Sub1 and Sub2. Sub1 contains a resource group named RG1 and an Azure policy named Policy1. You need to remediate the non-compliant resources in Sub1 based on Policy1. How should you complete the PowerShell script? To answer, drag the appropriate values to the correct targets. Each value may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content. NOTE: Each correct selection is worth one point.

Values

Get-AzPolicyRemediation

Set-AzContext

Set-AzResourceGroup

Start-AzPolicyComplianceScan

Start-AzPolicyRemediation

Answer Area

\$policyAssignmentId = "/subscriptions/f0710c27-9663-4c05-19f8-1b4be01e86a5/providers/Microsoft.Authorization/f

Value

-Subscription "Sub1"

Value

-PolicyAssignmentId \$policyAssignmentId -Name "policy1" -ResourceDiscovery

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

> For the first blank, use Set-AzContext to set the current subscription context.
> For the second blank, use Start-AzPolicyRemediation policy assignment. to create and start a policy remediation for a
The final script should look like this:
\$policyAssignmentId = "/subscriptions/f0710c27-9663-4c05-1978-1bdbedle86as/providers/Microsoft.
Authorization/f Value Set-AzContext
-Subscription "Sub1" ValuSetart-AzPolicyRemediation
-PolicyAssignmentId \$policyAssignmentId -Name "policy1" -ResourceDiscovery

NEW QUESTION 158

- (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 Blueprints

- C. Azure AD Privileged Identity Management (PIM)
- D. Azure Policy

Answer: B

Explanation:

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

NEW QUESTION 161

- (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 166

- (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 do not have access



Access denied

You do not have access

You don't have permission to register applications in the sk200510outlook (Default Directory) directory. To request access, contact your administrator.

Summary	
Session ID	Resource ID
f8e55e67d10141b4bf0c7ac5115b3be7	Not available
Extension	Content
Microsoft_AAD_RegisteredApps	CreateApplicationBlade
Error code	
403	

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 169

- (Exam Topic 4)

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

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

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

NOTE: Each correct selection is worth one point.

Resource provider:

Microsoft.Authorization
 Microsoft.Resources
 Microsoft.Support

Assignable scope:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text, application Description automatically generated

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

Reference:

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

NEW QUESTION 174

- (Exam Topic 4)

You company has an Azure subscription named Sub1. Sub1 contains an Azure web app named WebApp1 that uses Azure Application Insights. WebApp1 requires users to authenticate by using OAuth 2.0 client secrets.

Developers at the company plan to create a multi-step web test app that preforms synthetic transactions emulating user traffic to Web App1.

You need to ensure that web tests can run unattended. What should you do first?

- A. In Microsoft Visual Studio, modify the .webtest file.
- B. Upload the .webtest file to Application Insights.
- C. Register the web test app in Azure AD.
- D. Add a plug-in to the web test app.

Answer: B

Explanation:

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/availability-multistep>

NEW QUESTION 179

- (Exam Topic 4)

You have an Azure subscription that contains a storage account named storage1 and several virtual machines. The storage account and virtual machines are in the same Azure region. The network configurations of the virtual machines are shown in the following table.

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

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

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

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

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

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
VM1 can connect to storage1.	<input type="radio"/>	<input type="radio"/>
VM2 can connect to storage1.	<input type="radio"/>	<input type="radio"/>
VM3 can connect to storage1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: No

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

Box 2: Yes

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

Box 3: No

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

NEW QUESTION 183

- (Exam Topic 4)

You have an Azure subscription named Subcription1 that contains an Azure Active Directory (Azure AD) tenant named contosos.com and a resource group named RG1.

You create a custom role named Role1 for contoso.com.

You need to identify where you can use Role1 for permission delegation. What should you identify?

- A. contoso.com only
- B. contoso.com and RGT only
- C. contoso.com and Subscription1 only
- D. contoso.com, RG1, and Subscription1

Answer: A

Explanation:

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

NEW QUESTION 186

- (Exam Topic 4)

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

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

VNET1 contains two subnets named Subnet1 and Subnet2. Subnet1 has a network ID of 10.0.0.0/24. Subnet2 has a network ID of 10.1.1.0/24. Contoso1901 is configured as shown in the exhibit. (Click the Exhibit tab.)

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

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

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet.
                                                    IpRules
Action  IPAddressOrRange
-----  -
Allow   193.77.0.0/16

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

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

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

Statements	Yes	No
An Azure virtual machine on Subnet1 can access data in Contoso1901.	<input type="radio"/>	<input type="radio"/>
An Azure virtual machine on Subnet2 can access data in Contoso1901.	<input type="radio"/>	<input type="radio"/>
A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Yes

Access from Subnet1 is allowed. Box 2: No

No access from Subnet2 is allowed. Box 3: Yes

Access from IP address 193.77.10.2 is allowed.

NEW QUESTION 187

- (Exam Topic 4)

You have an Azure subscription that contains a virtual machine named VM1. You create an Azure key vault that has the following configurations:

- Name: Vault5
- Region: West US
- Resource group: RG1

You need to use Vault5 to enable Azure Disk Encryption on VM1. The solution must support backing up VM1 by using Azure Backup. Which key vault settings should you configure?

- A. Access policies
- B. Secrets
- C. Keys
- D. Locks

Answer: A

Explanation:

References:

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

NEW QUESTION 188

- (Exam Topic 4)

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

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

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

What should you do first?

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

Answer: A

Explanation:

Reference:

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

NEW QUESTION 189

- (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 8

You need to prevent HTTP connections to the rg1lod28681041n1 Azure Storage account.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To prevent HTTP connections to the rg1lod28681041n1 Azure Storage account, you can follow these steps: ➤ In the Azure portal, search for and select the storage account named rg1lod28681041n1.

- In the left pane, select Firewalls and virtual networks.
- In the Firewalls and virtual networks pane, select Selected networks.
- In the Selected networks pane, select Add existing virtual network.
- In the Add existing virtual network pane, select the virtual network that does not allow HTTP connections.
- Select Add.

NEW QUESTION 194

- (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 196

- (Exam Topic 4)

You have Azure Resource Manager templates that you use to deploy Azure virtual machines.

You need to disable unused Windows features automatically as instances of the virtual machines are provisioned.

What should you use?

- A. device compliance policies in Microsoft Intune
- B. Azure Automation State Configuration
- C. application security groups
- D. Azure Advisor

Answer: B

Explanation:

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

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

References:

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

NEW QUESTION 201

- (Exam Topic 4)

You have an Azure Storage account named storage1 and an Azure virtual machine named VM1. VM1 has a premium SSD managed disk.

You need to enable Azure Disk Encryption for VM1.

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

Actions

Run the Set-AzVMDiskEncryptionExtension cmdlet.

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

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

Generate a key vault certificate.

Create an Azure key vault.

Configure storage1 to use a customer-managed key.

Answer Area

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

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

NEW QUESTION 202

- (Exam Topic 4)

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

You need to identify which inventory assets are vulnerable to the most critical web app security risks. Which Defender EASM dashboard should you use?

- A. Attack Surface Summary
- B. GDPRCompliance
- C. Security Posture
- D. OWASPTopIO

Answer: D

NEW QUESTION 206

- (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 208

- (Exam Topic 4)

Lab Task

use the following login credentials as needed:

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

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

Azure Password: GpOAe4@IDg

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

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

Task 4

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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

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

NEW QUESTION 209

- (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	<i>Not applicable</i>
RG2	Resource group	West US	<i>Not applicable</i>
RG3	Resource group	Central US	<i>Not applicable</i>
VNet1	Virtual network	Central US	RG2

VNet1 contains the subnets shown in the following table.

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

You plan to use the Azure portal to deploy an Azure firewall named AzFW1 to VNet1.

Which resource group and subnet can you use to deploy AzFW1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Resource group: RG2

Subnet: AzureFirewallSubnet only

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Resource group: RG2

Subnet: AzureFirewallSubnet only

NEW QUESTION 211

- (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 213

- (Exam Topic 4)

You have 10 virtual machines on a single subnet that has a single network security group (NSG). You need to log the network traffic to an Azure Storage account. Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

Answer: D

Explanation:

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

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

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

NEW QUESTION 217

- (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 KeyVault, the following events occur in sequence:

- Item1 is deleted
- Administrator enables soft delete
- Item2 and Policy1 are deleted.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
You can recover Policy1.	<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:

NO. Policies cannot be recovered YES, Item1 is permanently deleted

NO, You cannot use the same name cause Item2 is in Seoft-deleted status <https://docs.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview>

NEW QUESTION 218

- (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 221

- (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 224

- (Exam Topic 4)

You have the hierarchy of Azure resources shown in the following exhibit.



You create the Azure Blueprints definitions shown in the following table.

Name	Published at
Blueprint1	Tenant Root Group
Blueprint2	Subscription1

To which objects can you assign Blueprint1 and Blueprint2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Blueprint1:

ManagementGroup1 only
ManagementGroup1, Subscription1, and RG1 only
ManagementGroup1, Subscription1, RG1, and VM1
Subscription1 only
Tenant Root Group only
Tenant Root Group, ManagementGroup1, and Subscription1 only

Blueprint2:

ManagementGroup1 only
Subscription1 and RG1 only
Subscription1 only
Subscription1, RG1, and VM1

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Blueprints can only be assigned to subscriptions.

NEW QUESTION 229

- (Exam Topic 4)

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

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

You perform the following tasks:

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

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

What is the Compliance State of the policy assignments?

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

Answer: A

NEW QUESTION 233

- (Exam Topic 4)

You have an Azure subscription that contains the following resources:

- An Azure key vault
- An Azure SQL database named Database1
- Two Azure App Service web apps named AppSrv1 and AppSrv2 that are configured to use system-assigned managed identities and access Database1

You need to implement an encryption solution for Database1 that meets the following requirements:

- The data in a column named Discount in Database1 must be encrypted so that only AppSrv1 can decrypt the data.
- AppSrv1 and AppSrv2 must be authorized by using managed identities to obtain cryptographic keys. How should you configure the encryption settings for Database1 To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

To configure the encryption of Database1:

- Always Encrypted by using Azure Key Vault.
- Always Encrypted by using the Windows Certificate Store.
- Transparent Data Encryption (TDE) by using Azure Key Vault integration.
- Transparent Data Encryption (TDE) by using Bring Your Own Key (BYOK).

To obtain the cryptographic keys:

- Create an access policy in Azure Key Vault.
- Generate a key on an HSM device.
- Import App Service certificates to AppSrv1 and AppSrv2.
- Register an enterprise application in Azure AD.

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Text Description automatically generated with medium confidence

Reference:

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

NEW QUESTION 238

- (Exam Topic 4)

You have an Azure subscription that contains an Azure web app named 1 and a virtual machine named VM1. VM1 runs Microsoft SQL Server and is connected to a virtual network named VNet1. App1, VM1, and VNet are in the US Central Azure region.

You need to ensure that App1 can connect to VM1. The solution must minimize costs.

- A. NAT gateway integration
 B. Azure Front Door
 C. regional virtual network integration
 D. gateway-required virtual network integration
 E. Azure Application Gateway integration

Answer: C

NEW QUESTION 241

- (Exam Topic 4)

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

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

You set the Key Vault access policy to Enable access to Azure Disk Encryption for volume encryption. KeyVault1 is configured as shown in the following exhibit.

Save Discard

Allow access from:

☐ All networks ☒ Selected networks

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

Virtual networks:

+ Add existing virtual networks

+ Add new virtual network

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

Firewall:

IPv4 ADDRESS OR CIDR

IPv4 address or CIDR ...

Exception:

Allow trusted Microsoft services to bypass this firewall?

☒ Yes ☐ No

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

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 245

- (Exam Topic 4)

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

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

For which virtual machine can you enable Update Management?

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

Answer: C

Explanation:

References:

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

NEW QUESTION 250

- (Exam Topic 4)

You have an Azure subscription that contains several Azure SQL databases and an Azure Sentinel workspace.

You need to create a saved query in the workspace to find events reported by Advanced Threat Protection for Azure SQL Database.

What should you do?

- A. From Azure CLI run the Get-AzOperationalInsightsworkspace cmdlet.
- B. From the Azure SQL Database query editor, create a Transact-SQL query.
- C. From the Azure Sentinel workspace, create a Kusto Query Language query.
- D. From Microsoft SQL Server Management Studio (SSMS), create a Transact-SQL query.

Answer: C

NEW QUESTION 253

- (Exam Topic 4)

You have a management group named MG1 that contains an Azure subscription and a resource group named RG1. RG1 contains a virtual machine named VM1.

You have the custom Azure roles shown in the following table.

Name	Scoped to
Role1	MG1
Role2	RG1

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

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

The permissions for Role2 are shown in the following role definition file.

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

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

Name	Role
User1	Role1
User2	Role1, Role2
User3	Role2

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

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 delete VM1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 255

- (Exam Topic 4)

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

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

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

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

You plan to enable Azure Disk Encryption on VM1.

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

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

Answer: A

Explanation:

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

Reference:

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

NEW QUESTION 257

- (Exam Topic 4)

You have an Azure AD tenant named contoso.com that has Azure AD Premium P1 licenses. You need to create a group named Group1 that will be assigned the Global reader role.

Which portal should you use to create Group1 and which type of group should you create? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-create-eligible>

NEW QUESTION 258

- (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 262

- (Exam Topic 4)

You have an Azure web app named webapp1.

You need to configure continuous deployment for webapp1 by using an Azure Repo.
What should you create first?

- A. an Azure Application Insights service
- B. an Azure DevOps organization
- C. an Azure Storage account
- D. an Azure DevTest Labs lab

Answer: B

NEW QUESTION 266

- (Exam Topic 4)

You have an Azure subscription that contains a web app named Appl. App1 provides users with product images and videos. Users access App1 by using a URL of HTTPS://appl.contoso.com. You deploy two server pools named Pool1 and Pool2. Pool1 hosts product images. Pool2 hosts product videos. You need to optimize The performance of Appl. The solution must meet the following requirements:

- Minimize the performance impact of TLS connections on Pool1 and Pool2.
- Route user requests to the server pools based on the requested URL path. What should you include in the solution?

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

Answer: C

NEW QUESTION 269

- (Exam Topic 4)

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

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

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

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 274

- (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 277

- (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 280

- (Exam Topic 4)

You have an Azure subscription.

You create a new virtual network named VNet1.

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

What should you do?

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

Answer: D

NEW QUESTION 281

- (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 282

- (Exam Topic 4)

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

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

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

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

The firewalls on all the virtual machines allow ping traffic. NSG1 is configured as shown in the following exhibit. Inbound security rules

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

Outbound security rules

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

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
VM1 can ping VM3 successfully.	<input type="radio"/>	<input type="radio"/>
VM2 can ping VM4 successfully.	<input type="radio"/>	<input type="radio"/>
VM3 can be accessed by using Remote Desktop from the internet.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box 1: Yes

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

Box 2: No

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

Box 3: Yes

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

NEW QUESTION 285

- (Exam Topic 4)

You have an Azure subscription that contains a blob container named cont1. Cont1 has the access policies shown in the following exhibit.


Save

Stored access policies

Identifier	Start time	Expiry time	Permissions
Policy1			r ...


Add policy

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

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

1
2
4
7
15

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

1
2
4
7
15

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

1
2
4
7
15

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

1
2
4
7
15

NEW QUESTION 289

- (Exam Topic 4)

You have an Azure subscription that contains an Azure Blob storage account bolb1. You need to configure attribute-based access control (ABAC) for blob1. Which attributes can you use in access conditions?

- A. blob index tags only
B. blob index tags and container names only
C. file extensions and container names only
D. blob index tags, file extensions, and container names

Answer: A

NEW QUESTION 293

- (Exam Topic 4)

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

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

You create the groups shown in the following table.

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

Which resources can you add to Group5 and Group6? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Group5:

Group6:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

NEW QUESTION 298

- (Exam Topic 4)

You have an Azure subscription that uses Microsoft Sentinel.

You need to create a Microsoft Sentinel notebook that will use the Guided Investigation - Anomaly Lookup template.

What should you create first?

- A. an analytics rule
- B. a Log Analytics workspace
- C. an Azure Machine Learning workspace
- D. a hunting query

Answer: A

NEW QUESTION 303

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that contains two users named User1 and User2 and a registered app named App1.

You create an app-specific role named Role1.

You need to assign Role1 to User1 and enable User2 to request access to App1.

Which two settings should you modify? To answer select the appropriate settings in the answer area NOTE: Each correct selection is worth one pant.

Owners

Roles and administrators (Preview)

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-ins

Usage & insights

- A. Mastered

B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application Description automatically generated

NEW QUESTION 305

- (Exam Topic 4)

You have an Azure subscription that contains an Azure SQL database named SQL1. You plan to deploy a web app named App1.

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

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

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

NOTE: Each correct selection is worth one point.

Account type:

Azure Active Directory User
Managed identity
Service Principal

Roles:

db_datawriter only
db_datareader and db_datawriter
db owner only

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

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

NEW QUESTION 310

- (Exam Topic 4)

You have an Azure AD tenant that contains 500 users and an administrative unit named AU1.

From the Azure Active Directory admin center, you plan to add the users to AU1 by using Bulk add members. You need to create and upload a file for the bulk add.

What should you include in the file?

- A. only the display name of each user
- B. only the user principal name (UPN) of each user
- C. only the object identifier of each user
- D. only the user principal name (UPN) and object identifier of each user
- E. Only the user principal name (UPN) and display name of each user

Answer: E

NEW QUESTION 314

- (Exam Topic 4)

You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1. You have 500 Azure virtual machines that run Windows Server 2016 and are enrolled in LAW1.

You plan to add the System Update Assessment solution to LAW1.

You need to ensure that System Update Assessment-related logs are uploaded to LAW1 from 100 of the virtual machines only.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:
<https://docs.microsoft.com/en-us/azure/azure-monitor/insights/solution-targeting>

NEW QUESTION 318

- (Exam Topic 3)
You plan to configure Azure Disk Encryption for VM4. Which key vault can you use to store the encryption key?

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

Answer: A

Explanation:

The key vault needs to be in the same subscription and same region as the VM. VM4 is in West US. KeyVault1 is the only key vault in the same region as the VM.
Reference:
<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault>

NEW QUESTION 320

- (Exam Topic 4)
You have an Azure key vault.
You need to delegate administrative access to the key vault to meet the following requirements:

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

What should you use to assign access to each user? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

User1:	<div><div></div><div>A key vault access policy Azure Information Protection Azure Policy Managed identities for Azure resources RBAC</div></div>
User2:	<div><div></div><div>A key vault access policy Azure Information Protection Azure Policy Managed identities for Azure resources RBAC</div></div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

User1: RBAC

RBAC is used as the Key Vault access control mechanism for the management plane. It would allow a user with the proper identity to:

- > set Key Vault access policies
- > create, read, update, and delete key vaults
- > set Key Vault tags

Note: Role-based access control (RBAC) is a system that provides fine-grained access management of Azure resources. Using RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs.

User2: A key vault access policy

A key vault access policy is the access control mechanism to get access to the key vault data plane. Key Vault access policies grant permissions separately to keys, secrets, and certificates.

References:

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

NEW QUESTION 325

- (Exam Topic 3)

You need to meet the technical requirements for the finance department users. Which CAPolicy1 settings should you modify?

- A. Cloud apps or actions
- B. Conditions
- C. Grant
- D. Session

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-life>

NEW QUESTION 330

- (Exam Topic 3)

You implement the planned changes for ASG1 and ASG2.

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

Answer Area

NSGs:	NSG2 only NSG2 and NSG4 only NSG2, NSG3, and NSG4
Virtual machines:	VM3 only VM2 and VM4 only VM1, VM2, and VM4 only VM2, VM3, and VM4 only VM1, VM2, VM3, and VM4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 333

- (Exam Topic 3)

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

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 336

- (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 340

- (Exam Topic 2)
You are evaluating the security of VM1, VM2, and VM3 in Sub2.
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
From the Internet, you can connect to the web server on VM1 by using HTTP.	<input type="radio"/>	<input type="radio"/>
From the Internet, you can connect to the web server on VM2 by using HTTP.	<input type="radio"/>	<input type="radio"/>
From the Internet, you can connect to the web server on VM3 by using HTTP.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
From the Internet, you can connect to the web server on VM1 by using HTTP.	<input checked="" type="radio"/>	<input type="radio"/>
From the Internet, you can connect to the web server on VM2 by using HTTP.	<input type="radio"/>	<input checked="" type="radio"/>
From the Internet, you can connect to the web server on VM3 by using HTTP.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 343

- (Exam Topic 2)
What is the membership of Group1 and Group2? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Group1:

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

Group2:

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box 1: User1, User2, User3, User4

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

Box 2: User1, User2, User3, User4 References:

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

NEW QUESTION 347

- (Exam Topic 1)

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

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

To configure the registration settings:

	▼
Azure AD – User settings	
Azure AD – App registrations settings	
Enterprise Applications – User settings	

To configure the consent settings:

	▼
Azure AD – User settings	
Azure AD – App registrations settings	
Enterprise Applications – User settings	

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 350

- (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 353

.....

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