

# Microsoft

## Exam Questions az-500

Microsoft Azure Security Technologies



### NEW QUESTION 1

- (Exam Topic 4)

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

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

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

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

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

References:

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

### NEW QUESTION 2

- (Exam Topic 4)

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

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

You have a hybrid configuration of Azure Active Directory (Azure AD). You have an Azure HDInsight cluster on a virtual network.

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

Solution: You deploy an Azure AD Application Proxy.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

#### Explanation:

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

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

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

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

### NEW QUESTION 3

- (Exam Topic 4)

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

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

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

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

You need to ingest the CEF messages from the NVAs to Azure Sentinel.

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

NOTE: Each correct selection is worth one point.

Subscription1:

An Azure Log Analytics agent on a Linux virtual machine

A Data Factory pipeline

An Event Hubs namespace

An Azure Service Bus queue

Subscription2:

A new Azure Log Analytics workspace

A new Azure Sentinel data connector

A new Azure Sentinel playbook

A new Event Grid resource provider

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 4**

- (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 5**

- (Exam Topic 4)

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

Subnet1 and Subnet2 have a network security group {NSG}. The NSG has an outbound rule that has the following configurations:

- Port: Any
- Source: Any
- Priority: 100
- Action: Deny
- Protocol: Any
- Destination: Storage

The subscription contains a storage account named storage1.

You create a private endpoint named Private1 that has the following settings:

- Resource type: Microsoft.Storage/storageAccounts
- Resource: storage1
- Target sub-resource: blob
- Virtual network: VNet1
- Subnet: Subnet1

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

Answer Area

Statements	Yes	No
From VM2, you can create a container in storage1.	<input type="radio"/>	<input type="radio"/>
From VM1, you can upload data to the blob storage of storage1.	<input type="radio"/>	<input type="radio"/>
From VM2, you can upload data to the blob storage of storage1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
From VM2, you can create a container in storage1.	<input type="radio"/>	<input checked="" type="radio"/>
From VM1, you can upload data to the blob storage of storage1.	<input checked="" type="radio"/>	<input type="radio"/>
From VM2, you can upload data to the blob storage of storage1.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 6

- (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 7**

- (Exam Topic 4)

You have an Azure subscription that contains a web app named App1 and an Azure key vault named Vault1. You need to configure App1 to store and access the secrets in Vault1.

How should you configure App1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Configure App1 to authenticate by using a:

Key
Certificate
Passphrase
User-assigned managed identity
System-assigned managed identity

Configure a Key Vault reference for App1 from the:

Extensions blade
General settings tab
TLS/SSL settings blade
Application settings tab

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Reference:

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

**NEW QUESTION 8**

- (Exam Topic 4)

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

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

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

**Answer: C**

**Explanation:**

Reference:

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

**NEW QUESTION 9**

- (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 10**

- (Exam Topic 4)

You have an Azure environment.

You need to identify any Azure configurations and workloads that are non-compliant with ISO 27001 standards. What should you use?

- A. Azure Sentinel
- B. Azure Active Directory (Azure AD) Identity Protection
- C. Azure Security Center
- D. Azure Advanced Threat Protection (ATP)

**Answer:** C

**Explanation:**

Reference:

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

**NEW QUESTION 10**

- (Exam Topic 4)

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

SQ11 has the following settings:

- Auditing: On
- Audit tog destination: storage1

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

**Answer Area**

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

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

**NEW QUESTION 12**

- (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:

NEW QUESTION 13

- (Exam Topic 4)

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

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

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

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

NOTE: Each correct selection is worth one point.

Azure Active Directory Identity Protection:

AzureDiagnostics

CommonSecurityLog

SecurityAlert

SecurityEvent

Syslog

Azure Firewall:

AzureDiagnostics

CommonSecurityLog

SecurityAlert

SecurityEvent

Syslog

CEF:

AzureDiagnostics

CommonSecurityLog

SecurityAlert

SecurityEvent

Syslog

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
Graphical user interface, application, table Description automatically generated

NEW QUESTION 17  
- (Exam Topic 4)  
You are testing an Azure Kubernetes Service (AKS) cluster. The cluster is configured as shown in the exhibit. (Click the Exhibit tab.)

BASICS	
Subscription	Microsoft Azure Sponsorship
Resource group	AzureBackupRG_eastus2_1
Region	East US
Kubernetes cluster name	akscluster2
Kubernetes version	1.1 1.5
DNS name prefix	akscluster2
Node count	3
Node size	Standard_DS2_v2
Virtual nodes (preview)	Disabled
AUTHENTICATION	
Enable RBAC	No
NETWORKING	
HTTP application routing	Yes
Network configuration	Basic
MONITORING	
Enable container monitoring	No
TAGS	

You plan to deploy the cluster to production. You disable HTTP application routing.  
You need to implement application routing that will provide reverse proxy and TLS termination for AKS services by using a single IP address.  
What should you do?

- A. Create an AKS Ingress controller.
- B. Install the container network interface (CNI) plug-in.
- C. Create an Azure Standard Load Balancer.
- D. Create an Azure Basic Load Balancer.

Answer: A



**Explanation:**

An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services.  
 References:  
<https://docs.microsoft.com/en-us/azure/aks/ingress-tls>

**NEW QUESTION 21**

- (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:

4

1

2

3

4

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

7

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:

4

1

2

3

4

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

7

3

4

7

9

11

#### NEW QUESTION 22

- (Exam Topic 4)

You plan to deploy Azure container instances.

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

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

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

What should you include in the deployment?

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

**Answer:** D

#### Explanation:

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

Reference:

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

#### NEW QUESTION 26

- (Exam Topic 4)

You have an Azure subscription.

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

Which property of the RBAC role definition should you configure?

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

**Answer:** D

#### Explanation:

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

Reference:

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

#### NEW QUESTION 31

- (Exam Topic 4)

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

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

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

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

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

- A. Yes
- B. No

**Answer:** B

#### NEW QUESTION 33

- (Exam Topic 4)

You have an Azure subscription named Subscription1.

You need to view which security settings are assigned to Subscription1 by default. Which Azure policy or initiative definition should you review?

- A. the Audit diagnostic setting policy definition
- B. the Enable Monitoring in Azure Security Center initiative definition
- C. the Enable Azure Monitor for VMs initiative definition
- D. the Azure Monitor solution 'Security and Audit' must be deployed policy definition

**Answer:** B

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/tutorial-security-policy> <https://docs.microsoft.com/en-us/azure/security-center/policy-reference>

#### NEW QUESTION 35

- (Exam Topic 4)

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

You have two custom Azure roles named Role1 and Role2 that are scoped to RG1.  
The permissions for Role1 are shown in the following JSON code.

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

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

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

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

Name	Role
User1	Role1
User2	Role1, Role2
User3	Role1, Role2

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

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 37

- (Exam Topic 4)

Lab Task

use the following login credentials as needed:

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

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

Azure Password: GpOAe4@IDg

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

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

Task 2

You need to add the network interface of a virtual machine named VM1 to an application security group named ASG1.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

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

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

**NEW QUESTION 38**

- (Exam Topic 4)

Your network contains an Active Directory forest named contoso.com. You have an Azure Directory (Azure AD) tenant named contoso.com. You plan to configure synchronization by using the Express Settings installation option in Azure AD Connect. You need to identify which roles and groups are required to perform the planned configurations. The solution must use the principle of least privilege. Which two roles and groups should you identify? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. the Domain Admins group in Active Directory
- B. the Security administrator role in Azure AD
- C. the Global administrator role in Azure AD
- D. the User administrator role in Azure AD
- E. the Enterprise Admins group in Active Directory

**Answer:** CE

**Explanation:**

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

**NEW QUESTION 40**

- (Exam Topic 4)

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant and a user named User1. The App registrations settings for the tenant are configured as shown in the following exhibit.



You plan to deploy an app named App1. You need to ensure that User1 can register App1 in Azure AD. The solution must use the principle of least privilege. Which role should you assign to User1?

- A. App Configuration Data Owner for the subscription
- B. Managed Application Contributor for the subscription
- C. Cloud application administrator in Azure AD
- D. Application developer in Azure AD.

**Answer:** D

**Explanation:**

Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task>

**NEW QUESTION 43**

- (Exam Topic 4)

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

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

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



Settings



Assignment

☒ Allow permanent eligible assignment

Expire eligible assignments after

3 Months

☒ Allow permanent active assignment

Expire active assignments after

1 Month

☐ Require Azure Multi-Factor Authentication on active assignment

☒ Require justification on active assignment

Activation

Activation maximum duration (hours)

5

☐ Require Azure Multi-Factor Authentication on activation

☐ Require justification on activation

☐ Require ticket information on activation

☐ Require approval to activate

Select approvers

No member or group selected

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

- > Group1: Active assignment type, permanently assigned
- > Group2: Eligible assignment type, permanently eligible

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

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	<input type="radio"/>	<input type="radio"/>
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	<input type="radio"/>	<input type="radio"/>
User3 can activate the Security Administrator role.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Box 1: Yes

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

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

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

Box 2: Yes

Active Type: A role assignment that doesn't require a user to perform any action to use the role. Users assigned as active have the privileges assigned to the role

Box 3: Yes

User3 is member of Group2. Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure https://docs.microsoft.com/bs-cyrl-ba/azure/active-directory/privileged-identity-management/pim-resource-roles

#### NEW QUESTION 45

- (Exam Topic 4)

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

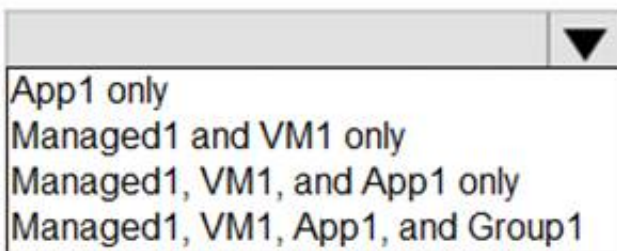
Name	Type
RG1	Resource group
VM1	Virtual machine

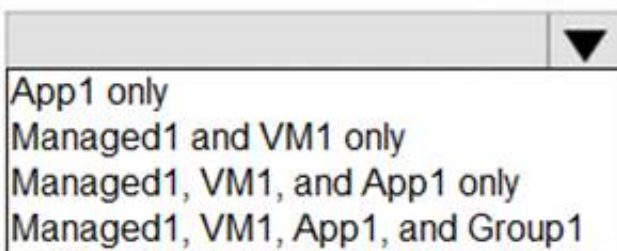
You perform the following tasks:

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: 

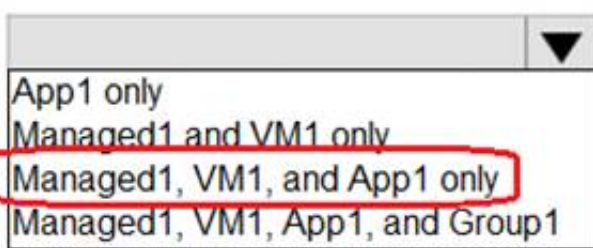
Identities: 

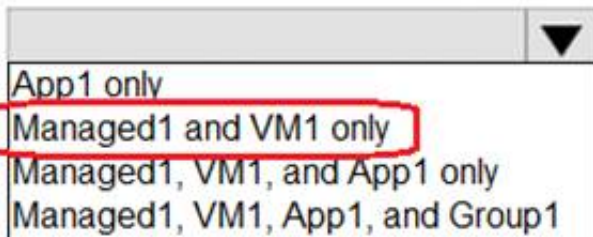
- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

#### Answer Area

Service Principles: 

Identities: 

#### NEW QUESTION 50

- (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 54

- (Exam Topic 4)  
You have five Azure subscriptions linked to a single Azure Active Directory (Azure AD) tenant. You create an Azure Policy initiative named SecurityPolicyInitiative1.  
You identify which standard role assignments must be configured on all new resource groups.  
You need to enforce SecurityPolicyInitiative1 and the role assignments when a new resource group is created. Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Publish an Azure Blueprints version

Assign an Azure blueprint.

Create a policy assignment.

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

Create a dedicated management subscription.

Create an Azure Blueprints definition.

Create an initiative assignment.

Answer Area

⏪

⏩

⏴

⏵

- A. Mastered
- B. Not Mastered

Answer: A

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

NEW QUESTION 59

- (Exam Topic 4)  
You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

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

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

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

You assign Role1 to User1 on RG1.  
For each of the following statements, select Yes if the statement is true. Otherwise, select No.  
NOTE: Each correct selection is worth one point.



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

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Text Description automatically generated

Reference:

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

**NEW QUESTION 61**

- (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 65**

- (Exam Topic 4)

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

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

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

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

Answer: C

**Explanation:**

Reference:

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

**NEW QUESTION 67**

- (Exam Topic 4)

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

Name	Type	Attached to	NSG
NSG1	Network security group (NSG)	VM5	Not applicable
NSG2	Network security group (NSG)	Subnet1	Not applicable
Subnet1	Subnet	Not applicable	Not applicable
VM5	Virtual machine	Subnet1	NSG1

An IP address of 10.1.0.4 is assigned to VM5. VM5 does not have a public IP address. VM5 has just in time (JIT) VM access configured as shown in the following



exhibit.

JIT VM access configuration

VM5

+ Add

Save

Discard

Configure the ports for which the just-in-time VM access will be applicable

Port	Protocol	Allowed source IPs	IP range	Time range (hours)	
3389	Any	Per request	N/A	3 hours	...

You enable JIT VM access for VM5.  
NSG1 has the inbound rules shown in the following exhibit.

Priority	Name	Port	Protocol	Source	Destination	Action
100	SecurityCenter-JITRule-...	3389	Any	Any	10.1.0.4	Allow
1000	SecurityCenter-JITRule_341...	3389	Any	Any	10.1.0.4	Deny
1001	RDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

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

Statements	Yes	No
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	<input type="radio"/>	<input type="radio"/>
Remote Desktop access to VM5 is blocked.	<input type="radio"/>	<input type="radio"/>
An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	<input checked="" type="radio"/>	<input type="radio"/>
Remote Desktop access to VM5 is blocked.	<input checked="" type="radio"/>	<input type="radio"/>
An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 71

- (Exam Topic 4)  
You have an Azure subscription.  
You create an Azure web app named Contoso1812 that uses an S1 App service plan.  
You create a DNS record for www.contoso.com that points to the IP address of Contoso1812.  
You need to ensure that users can access Contoso1812 by using the https://www.contoso.com URL. Which two actions should you perform? Each correct answer presents part of the solution.  
NOTE: Each correct selection is worth one point.

- A. Turn on the system-assigned managed identity for Contoso1812.

- B. Add a hostname to Contoso1812.
- C. Scale out the App Service plan of Contoso1812.
- D. Add a deployment slot to Contoso1812.
- E. Scale up the App Service plan of Contoso1812.
- F. Upload a PFX file to Contoso1812

**Answer:** BF

**Explanation:**

B: You can configure Azure DNS to host a custom domain for your web apps. For example, you can create an Azure web app and have your users access it using either [www.contoso.com](http://www.contoso.com) or [contoso.com](http://contoso.com) as a fully qualified domain name (FQDN). To do this, you have to create three records:

A root "A" record pointing to [contoso.com](http://contoso.com) A root "TXT" record for verification

A "CNAME" record for the [www](http://www.contoso.com) name that points to the A record

F: To use HTTPS, you need to upload a PFX file to the Azure Web App. The PFX file will contain the SSL certificate required for HTTPS.

References: <https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom-Domain>

**NEW QUESTION 75**

- (Exam Topic 4)

You have an Azure subscription that contains an instance of Azure Firewall Standard named AzFWL. You need to identify whether you can use the following features with AzFW1:

- TLS inspection
- Threat intelligence
- The network intrusion detection and prevention systems (IDPS) What can you use?

- A. TLS inspection only
- B. threat intelligence only
- C. TLS inspection and the IDPS only
- D. threat intelligence and the IDPS only
- E. TLS inspection, threat intelligence, and the IDPS

**Answer:** E

**NEW QUESTION 80**

- (Exam Topic 4)

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

An administrator named Admin1 has access to the following identities:

- An OpenID-enabled user account
- A Hotmail account
- An account in [contoso.com](http://contoso.com)
- An account in an Azure AD tenant named [fabrikam.com](http://fabrikam.com)

You plan to use Azure Account Center to transfer the ownership of Sub1 to Admin1. To which accounts can you transfer the ownership of Sub1?

- A. [contoso.com](http://contoso.com) only
- B. [contoso.com](http://contoso.com), [fabrikam.com](http://fabrikam.com), and Hotmail only
- C. [contoso.com](http://contoso.com) and [fabrikam.com](http://fabrikam.com) only
- D. [contoso.com](http://contoso.com), [fabrikam.com](http://fabrikam.com), Hotmail, and OpenID-enabled user account

**Answer:** C

**Explanation:**

When you transfer billing ownership of your subscription to an account in another Azure AD tenant, you can move the subscription to the new account's tenant. If you do so, all users, groups, or service principals who had role based access (RBAC) to manage subscriptions and its resources lose their access. Only the user in the new account who accepts your transfer request will have access to manage the resources.

Reference:

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

<https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transferring-subscription-to-anaccou>

**NEW QUESTION 85**

- (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 89

- (Exam Topic 4)

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

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

The subscription contains the users shown in the following table.

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

On June 1, you perform the following actions:

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

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

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

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

- Yes  
Yes No

NEW QUESTION 94

- (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 97  
- (Exam Topic 4)  
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

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

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

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

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

Statements	Yes	No
If User1 signs in from an unfamiliar location, he must change his password.	<input type="radio"/>	<input type="radio"/>
If User2 signs in from an anonymous IP address, she must change her password.	<input type="radio"/>	<input type="radio"/>
If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
Box 1: Yes  
User1 is member of Group1. Sign in from unfamiliar location is risk level Medium. Box 2: Yes  
User2 is member of Group1. Sign in from anonymous IP address is risk level Medium. Box 3: No  
Sign-ins from IP addresses with suspicious activity is low. Note:



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

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

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

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

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

#### NEW QUESTION 100

- (Exam Topic 4)

You network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant. The tenant contains the users shown in the following table.

Name	Source
User1	Azure AD
User2	Azure AD
User3	On-premises Active Directory

The tenant contains the groups shown in the following table.

Name	Members
Group1	User1, User2, User3
Group2	User2

You configure a multi-factor authentication (MFA) registration policy that and the following settings:

- Assignments:
- Include: Group1
- Exclude Group2

Controls: Require Azure MFA registration Enforce Policy: On

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

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>
User2 must configure MFA during the user's next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>
User3 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user’s next Azure AD authentication.	<input checked="" type="radio"/>	<input type="radio"/>
User2 must configure MFA during the user’s next Azure AD authentication.	<input type="radio"/>	<input checked="" type="radio"/>
User3 will be prompted to configure MFA registration during the user’s next Azure AD authentication.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 102

- (Exam Topic 4)

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

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

You enable Microsoft Defender for Storage.

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

Answer Area

Monitored storage5 services:

Protected storage accounts:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Monitored storage5 services:

Protected storage accounts:

NEW QUESTION 105

- (Exam Topic 4)

Your company has two offices in Seattle and New York. Each office connects to the Internet by using a NAT device. The offices use the IP addresses shown in the following table.

Location	IP address space	Public NAT segment
Seattle	10.10.0.0/16	190.15.1.0/24
New York	172.16.0.0/16	194.25.2.0/24

The company has an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

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

The MFA service settings are configured as shown in the exhibit. (Click the Exhibit tab.)

trusted ips [learn more](#)

☒ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

10.10.0.0/16

194.25.2.0/24

verification options [learn more](#)

Methods available to users:

☒ Call to phone

☒ Text message to phone

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

	Yes	No
If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.	<input type="radio"/>	<input type="radio"/>
If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app.	<input type="radio"/>	<input type="radio"/>
If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**  
Box 2: No  
Use of Microsoft Authenticator is not required.  
Note: Microsoft Authenticator is a multifactor app for mobile devices that generates time-based codes used during the Two-Step Verification process.  
Box 3: No  
The New York IP address subnet is included in the "skip multi-factor authentication for request. References:  
<https://www.cayosoft.com/difference-enabling-enforcing-mfa/>

**NEW QUESTION 106**  
- (Exam Topic 4)  
You have an Azure Storage account that contains a blob container named container1 and a client application named App1. You need to enable App1 access to container1 by using Azure Active Directory (Azure AD) authentication. What should you do? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

From Azure AD:

Register App1.

Create an access package.

Implement an application proxy.

Modify the authentication methods.

From the storage account:

Add a private endpoint.

Regenerate the access key.

Configure Access control (IAM).

Generate a shared access signature (SAS).

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



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

**NEW QUESTION 110**

- (Exam Topic 4)

You plan to implement an Azure function named Function1 that will create new storage accounts for containerized application instances. You need to grant Function1 the minimum required privileges to create the storage accounts. The solution must minimize administrative effort. What should you do? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

Assign role to:

A group account

A system-assigned managed identity

A user account

A user-assigned managed identity

Role assignment to create:

Built-in role assignment

Classic administrator role assignment

Custom role-based access control (RBAC) role assignment

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 112**

- (Exam Topic 4)

You have an Azure subscription that contains a resource group named RG1 and a security group named ServerAdmins. RG1 contains 10 virtual machines, a virtual network named VNET1, and a network security group (NSG) named NSG1. ServerAdmins can access the virtual machines by using RDP. You need to ensure that NSG1 only allows RDP connections to the virtual machines for a maximum of 60 minutes when a member of ServerAdmins requests access. What should you configure?

- A. an Azure policy assigned to RG1
- B. a just in time (JIT) VM access policy in Microsoft Defender for Cloud
- C. an Azure AD Privileged Identity Management (PIM) role assignment
- D. an Azure Bastion host on VNET1




**Answer:** B

**NEW QUESTION 113**

- (Exam Topic 4)


You have an Azure subscription that contains an Azure SQL Database logic server named SQL1 and an Azure virtual machine named VM1. VM1 uses a private IP address only. The Firewall and virtual networks settings for SQL1 are shown in the following exhibit.



 Save
  Discard
  Add client IP

Deny public network access ⓘ
 

Yes
 No

 Click here to create a new private endpoint.  
[Create Private Endpoint](#)

Minimum TLS Version ⓘ
 

1.0
 1.1
 1.2

Connection Policy ⓘ
 

Default
 Proxy
 Redirect

Allow Azure services and resources to access this server ⓘ
 

Yes
 No

Client IP address 89.212.25.106

Rule name	Start IP	End IP

No firewall rules configured.

Virtual networks  
[+ Add existing virtual network](#) [+ Create new virtual network](#)

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

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

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

**Answer: C**

#### NEW QUESTION 116

- (Exam Topic 4)

You have an Azure subscription that contains an app named App1. App1 has the app registration shown in the following table.

API	Permission	Type	Admin consent required	Status
Microsoft.Graph	User.Read	Delegated	No	None
Microsoft.Graph	Calendars.Read	Delegated	No	None

You need to ensure that App1 can read all user calendars and create appointments. The solution must use the principle of least privilege. What should you do?

- A. Add a new Delegated API permission for Microsoft.Graph Calendars.ReadWrite.
- B. Add a new Application API permission for Microsoft.Graph Calendars.ReadWrite.
- C. Select Grant admin consent.
- D. Add a new Delegated API permission for Microsoft.Graph Calendars.ReadWrite.Shared.

**Answer: A**

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/graph/permissions-reference#calendars-permissions>

#### NEW QUESTION 121

- (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 124**

- (Exam Topic 4)

You have an Azure subscription that contains the following resources:

- > A network virtual appliance (NVA) that runs non-Microsoft firewall software and routes all outbound traffic from the virtual machines to the internet
- > An Azure function that contains a script to manage the firewall rules of the NVA
- > Azure Security Center standard tier enabled for all virtual machines
- > An Azure Sentinel workspace
- > 30 virtual machines

You need to ensure that when a high-priority alert is generated in Security Center for a virtual machine, an incident is created in Azure Sentinel and then a script is initiated to configure a firewall rule for the NVA.

How should you configure Azure Sentinel to meet the requirements? To answer, drag the appropriate components to the correct requirements. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

**Components**

A data connector for Security Center

A data connector for the firewall software

A playbook

A rule

A Security Events connector

A workbook

**Answer Area**

Enable alert notifications from Security Center:

Component

Create an incident:

Component

Initiate a script to configure the firewall rule:

Component

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 126**

- (Exam Topic 4)

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

Name	Resource group	Status
VM1	RG1	Stopped (Deallocated)
VM2	RG2	Stopped (Deallocated)

You create the Azure policies shown in the following table.

Policy definition	Resource type	Scope
Not allowed resource types	virtualMachines	RG1
Allowed resource types	virtualMachines	RG2

You create the resource locks shown in the following table.

Name	Type	Created on
Lock1	Read-only	VM1
Lock2	Read-only	RG2

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



Allow users to request access to this application? ⓘ

Yes

No

To which group should assigned users be added? ⓘ

Select group

Group2

Require approval before granting access to this application? ⓘ

Yes

No

Who is allowed to approve access to this application? ⓘ

Select approvers

1 users selected

To which role should users be assigned in this application? ⓘ

Select role

Default Access

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

Group2 owners:

User2 only

User3 only

User1 and User2 only

User2 and User3 only

User1, User2, and User3

App1 users:

Group1 members only

Group2 members only

Group1 and Group2 members only

Group1 and Group2 members and User1 only

Group1 and Group2 members, User1, and User3 only

- 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 136**  
- (Exam Topic 4)  
You need to create an Azure key vault. The solution must ensure that any object deleted from the key vault be retained for 90 days.  
How should you complete the command? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

New-AzureRmKeyVault -VaultName 'KeyVault1' -ResourceGroupName 'RG1'

-Location 'East US'

-EnabledForDeployment

-EnablePurgeProtection

-Tag

-Confirm

-DefaultProfile

-EnableSoftDelete

-SKU

- A. Mastered
- B. Not Mastered

**Answer:** A



**Explanation:**

Box 1: -EnablePurgeProtection  
If specified, protection against immediate deletion is enabled for this vault; requires soft delete to be enabled as well.  
Box 2: -EnableSoftDelete  
Specifies that the soft-delete functionality is enabled for this key vault. When soft-delete is enabled, for a grace period, you can recover this key vault and its contents after it is deleted.  
References:  
<https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/new-azurermkeyvault>

**NEW QUESTION 141**

- (Exam Topic 4)  
You have an Azure subscription that contains the resources shown in the following table.

Name	Type
SQL1	Azure SQL Database server
DB1	Azure SQL database on SQL1
DB2	Azure SQL database on SQL1
storage1	Storage account
storage2	Storage account
Workspace1	Log Analytics workspace

SQL1 has the following configurations:

- Auditing: Enabled
- Audit log destination: storage1, Workspace1

DB1 has the following configurations:

- Auditing: Enabled
- Audit log destination: storage2

DB2 has auditing disabled.

Where are the audit logs for DB1 and DB2 stored? To answer, select the appropriate options in the answer area  
NOTE: Each correct selection is worth one point.

**Answer Area**

DB1:

storage1, storage2, and Workspace1

storage2 only

storage1 and Workspace1 only

storage2 and Workspace1 only

storage1, storage2, and Workspace1

DB2:

Workspace1 only

No audit logs created

storage1 only

Workspace1 only

storage1 and Workspace1

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

DB1:

storage1, storage2, and Workspace1

storage2 only

storage1 and Workspace1 only

storage2 and Workspace1 only

storage1, storage2, and Workspace1

DB2:

Workspace1 only

No audit logs created

storage1 only

Workspace1 only

storage1 and Workspace1

**NEW QUESTION 146**

- (Exam Topic 4)  
Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD).  
The Azure AD tenant contains the users shown in the following table.

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

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

Custom smart lockout

Lockout threshold ⓘ

Lockout duration in seconds ⓘ

Custom banned passwords

Enforce custom list ⓘ 

Yes

No

Custom banned password list ⓘ 

Adatum

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ 

Yes

No

Mode ⓘ 

Enforced

Audit

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

Statements	Yes	No
User1 will be prompted to change the password on the next sign-in.	<input type="radio"/>	<input type="radio"/>
User2 can change the password to @d@tum_C0mpleX123.	<input type="radio"/>	<input type="radio"/>
User3 can change the password to Adatum123!.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text Description automatically generated

Reference:

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

NEW QUESTION 150

- (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 Good and GCP only
- D. AWS and GCP only
- E. Alibaba Cloud, AW
- F. and GCP

Answer: A

NEW QUESTION 152

- (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 154

- (Exam Topic 4)

You have an Azure subscription named Sub1.

You have an Azure Active Directory (Azure AD) group named Group1 that contains all the members of your IT team.

You need to ensure that the members of Group1 can stop, start, and restart the Azure virtual machines in Sub1. The solution must use the principle of least privilege.

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

Actions

Create a JSON file.

Run the Update-AzureRmManagementGroup cmdlet.

Create an XML file.

Run the New-AzureRmRoleDefinition cmdlet.

Run the New-AzureRmRoleAssignment cmdlet.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

References:

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

NEW QUESTION 155

- (Exam Topic 4)

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

Name	Resource group
storage1	RG1
storage2	RG1
storage3	RG2

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

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

- \* The storage1 and storage2 account must be include in the defender for storage requirement.
- \* The storage3 account must be exclude from the Defender for Storage protections.

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

Actions

For storage3, disable the customer-managed keys.

Disable Defender for Storage for storage3.

Enable the Defender for Storage plan for Sub1.

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

Enable the Defender for Storage plan for RG1.

Answer Area

1

2

3



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

For storage3, disable the customer-managed keys.

Disable Defender for Storage for storage3.

Enable the Defender for Storage plan for Sub1.

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

Enable the Defender for Storage plan for RG1.

Answer Area

1 Enable the Defender for Storage plan for Sub1.

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

3 Enable the Defender for Storage plan for RG1.

NEW QUESTION 157

- (Exam Topic 4)

You have an Azure Container Registry named ContReg1 that contains a container image named image1. You enable content trust for ContReg1. After content trust is enabled, you push two images to ContReg1 as shown in the following table.

Name	Details
image2	Image was pushed with client content trust enabled.
image3	Image was pushed with client content trust disabled.

Which images are trusted images?

- A. image1 and image2 only
- B. image2 only
- C. image1, image2, and image3

Answer: B

Explanation:

Azure Container Registry implements Docker's content trust model, enabling pushing and pulling of signed images. To push a trusted image tag to your container registry, enable content trust and push the image with docker push. To work with trusted images, both image publishers and consumers need to enable content trust for their Docker clients. As a publisher, you can sign the images you push to a content trust-enabled registry.  
Reference:  
<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust>

NEW QUESTION 159

- (Exam Topic 4)

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

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

Answer: D

Explanation:

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

NEW QUESTION 161

- (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 164

- (Exam Topic 4)

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

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

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

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

**Answer:** A

#### NEW QUESTION 165

- (Exam Topic 4)

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

Name	Type
storage1	Storage account
KeyVault1	Azure key vault

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

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

**Answer:** D

#### NEW QUESTION 170

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant. You have the deleted objects shown in the following table.

Name	Type	Deleted on
Group1	Security group	April 5, 2020
Group2	Office 365 group	April 5, 2020
User1	User	March 25, 2020
User2	User	April 30, 2020

On May 4, 2020, you attempt to restore the deleted objects by using the Azure Active Directory admin center. Which two objects can you restore? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

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

**Answer:** BC

#### Explanation:

Deleted users and deleted Office 365 groups are available for restore for 30 days. You cannot restore a deleted security group.

Reference:

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

#### NEW QUESTION 173

- (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 177

- (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 179

- (Exam Topic 4)

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

Each subscription contains a resource group named RG1.

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

- > The members of Group1 are assigned the Owner role.
- > The modification of permissions to RG1 is prevented.

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

NOTE: Each correct selection is worth one point.

Configure role-based access control (RBAC) role assignments by using:	<div><div></div><div>Azure Blueprints</div><div>Azure Policy</div><div>Azure Security Center</div></div>
Prevent the modification of permissions to RG1 by using:	<div><div></div><div>A resource lock</div><div>A role-based access control (RBAC) role assignment at the resource group level</div><div>Azure Blueprint assignments in locking mode</div></div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

▼

Azure Blueprints |

Azure Policy

Azure Security Center

Prevent the modification of permissions to RG1 by using:

▼

A resource lock

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

Azure Blueprint assignments in locking mode

#### NEW QUESTION 181

- (Exam Topic 4)

You have an Azure subscription that contains a user named User1. You need to ensure that User1 can perform the following tasks:

- Create groups.
- Create access reviews for role-assignable groups.
- Assign Azure AD roles to groups.

The solution must use the principle of least privilege. Which role should you assign to User1?

- A. Groups administrator
- B. Authentication administrator
- C. Identity Governance Administrator
- D. Privileged role administrator

Answer: C

#### NEW QUESTION 186

- (Exam Topic 4)

HOTSPOT

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

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

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

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

▼

ActivityID

DataType

EventID

QuantityUnit

==4625

```
| Summarize failed_login_attempts=
```

▼

Count(),

Countif(),

Makeset(),

Split(),

```
latest_failed_login=arg_max(TimeGenerated by Account
| where failed_login_attempts > 5
```

- A. Mastered
- B. Not Mastered

Answer: A

#### Explanation:

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

```
let timeframe = 1d; SecurityEvent
| where TimeGenerated > ago(1d)
| where AccountType == 'User' and EventID == 4625 // 4625 - failed log in
| summarize failed_login_attempts=count(), latest_failed_login=arg_max(TimeGenerated, Account) by Account
| where failed_login_attempts > 5
| project-away Account1 References:
https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/examples
```

#### NEW QUESTION 191

- (Exam Topic 4)

You have an Azure subscription named Sub 1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the

users shown in the following table.

Name	Role
User1	Global administrator
User2	Security administrator
User3	Security reader
User4	License administrator

Each user is assigned an Azure AD Premium P2 license.  
You plan to onboard and configure Azure AD Identity Protection.  
Which users can onboard Azure AD Identity Protection, remediate users, and configure policies? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point

Answer Area

Users who can onboard Azure AD Identity Protection:

User1 only

User1 and User2 only

User1, User 2, and User3 only

User1, User 2, User3, and User 4 only

Users who can remediate users and configure policies:

User1 and User2 only

User1 and User3 only

User1, User 2, and User3 only

User1, User 2, User3, and User 4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
Answer Area

Users who can onboard Azure AD Identity Protection:

User1 only

User1 and User2 only

User1, User 2, and User3 only

User1, User 2, User3, and User 4 only

Users who can remediate users and configure policies:

User1 and User2 only

User1 and User3 only

User1, User 2, and User3 only

User1, User 2, User3, and User 4

NEW QUESTION 194

- (Exam Topic 4)  
You have an Azure subscription named Sub1. Sub1 has an Azure Storage account named Storage1 that contains the resources shown in the following table.

Name	Type
Container1	Blob container
Share1	File share

You generate a shared access signature (SAS) to connect to the blob service and the file service.  
Which tool can you use to access the contents in Container1 and Share1 by using the SAS? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

Answer Area

Tools for Container1:

Robocopy.exe

Azure Storage Explorer

File Explorer

Tools for Share1:

Robocopy.exe

Azure Storage Explorer

File Explorer

- A. Mastered
- B. Not Mastered

Answer: A



Explanation:  
Answer Area



NEW QUESTION 198

- (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	10.1.1.5	20.224.219.170
VM2	VNET1/Subnet2	10.1.2.5	20.224.219.230
VM3	VNET2/Subnet1	10.11.1.5	40.122.155.212

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

Allow access from

☐ All networks ☒ Selected networks

Configure network security for your Azure Cosmos DB account. Learn more

Statements	Yes	No
VM1 can access cosmos1 over the internet.	<input type="radio"/>	<input type="radio"/>
VM2 can access cosmos1 over the internet.	<input type="radio"/>	<input type="radio"/>
VM3 can access cosmos1 over the internet.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
Yes, Yes, No

NEW QUESTION 203

- (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 207

- (Exam Topic 4)  
You have an Azure subscription that uses Microsoft Defender for Cloud.  
You have an Amazon Web Services (AWS) account.

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

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

**Answer:** A

#### NEW QUESTION 212

- (Exam Topic 4)

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

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 216

- (Exam Topic 4)

You have an Azure subscription that contains an Azure key vault. The role assignments for the key vault are shown in the following exhibit.

```
[
  {
    "RoleAssignmentId": "3336fcfb-33d8-4c8a-85b6-d8edd964762b",
    "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa",
    "DisplayName": "User1",
    "SignInName": "User1@contoso.com",
    "RoleDefinitionName": "Owner",
    ...
  },
  {
    "RoleAssignmentId": "9d080a14-246e-4580-8b8b-077bfec22f7c",
    "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG1/providers/Microsoft.KeyVault/vaults/KeyVault1",
    "DisplayName": "User2",
    "SignInName": "User2@contoso.com",
    "RoleDefinitionName": "Key Vault Crypto Officer",
    "RoleAssignmentId": "i",
    "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG1/providers/Microsoft.KeyVault/vaults/KeyVault1",
    "DisplayName": "User3",
    "SignInName": "User3@contoso.com",
    "RoleDefinitionName": "Key Vault Secrets Officer",
    ...
  },
  {
    "RoleAssignmentId": "f1e46302-c5d0-4519-9ee7-128594eea97c",
    "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG3/providers/Microsoft.KeyVault/vaults/KeyVault1/keys/Key1",
    "DisplayName": "User4",
    "SignInName": "User4@contoso.com",
    "RoleDefinitionName": "Key Vault Administrator",
    ...
  }
]
```

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 Area

[Answer choice] can create keys in the key vault.

[Answer choice] can create secrets in the key vault.

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

#### Answer Area

[Answer choice] can create keys in the key vault. Only User1 and User4

[Answer choice] can create secrets in the key vault. Only User1 and User3

#### NEW QUESTION 219

- (Exam Topic 4)

You plan to use Azure Resource Manager templates to perform multiple deployments of identically configured Azure virtual machines. The password for the administrator account of each deployment is stored as a secret in different Azure key vaults. You need to identify a method to dynamically construct a resource ID that will designate the key vault containing the appropriate secret during each deployment. The name of the key vault and the name of the secret will be provided as inline parameters. What should you use to construct the resource ID?

- A. a key vault access policy
- B. a linked template
- C. a parameters file
- D. an automation account

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 223

- (Exam Topic 4)

You have an Azure subscription that contains a storage account named storage1 and a virtual machine named VM1. VM1 is connected to a virtual network named VNet1 that contains one subnet and uses Azure DNS. You need to ensure that VM1 connects to storage1 by using a private IP address. The solution must minimize administrative effort. What should you do?

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

**Answer:** D

#### NEW QUESTION 226

- (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 230

- (Exam Topic 4)

You have an Azure subscription that contains a user named User1 and an Azure Container Registry named ConReg1. You enable content trust for ContReg1. You need to ensure that User1 can create trusted images in ContReg1. The solution must use the principle of least privilege. Which two roles should you assign to User1? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. AcrQuarantineReader
- B. Contributor
- C. AcrPush
- D. AcrImageSigner
- E. AcrQuarantineWriter

**Answer:** CD

**Explanation:**

References:

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust> <https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles>

**NEW QUESTION 233**

- (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 234**

- (Exam Topic 4)

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

Name	Type
storage1	Storage account
Vault1	Azure Key vault
Vault2	Azure Key vault

You plan to deploy the virtual machines shown in the following table.

Name	Role
VM1	<ul style="list-style-type: none"><li>Storage Blob Data Reader for storage1</li><li>Key Vault Reader for Vault1</li></ul>
VM2	<ul style="list-style-type: none"><li>Storage Blob Data Reader for storage1</li><li>Key Vault Reader for Vault1</li></ul>
VM3	<ul style="list-style-type: none"><li>Storage Blob Data Reader for storage1</li><li>Key Vault Reader for Vault1</li><li>Key Vault Reader for Vault2</li></ul>
VM4	<ul style="list-style-type: none"><li>Storage Blob Data Reader for storage1</li><li>Key Vault Reader for Vault1</li><li>Key Vault Reader for Vault2</li></ul>

You need to assign managed identities to the virtual machines. The solution must meet the following requirements:

- Assign each virtual machine the required roles.
- Use the principle of least privilege.

What is the minimum number of managed identities required?

- A. 1
- B. 2
- C. 3
- D. 4

**Answer: B**

**Explanation:**

We have two different sets of required permissions. VM1 and VM2 have the same permission requirements. VM3 and VM4 have the same permission requirements.

A user-assigned managed identity can be assigned to one or many resources. By using user-assigned managed identities, we can create just two managed identities: one with the permission requirements for VM1 and VM2 and the other with the permission requirements for VM3 and VM4.

Reference:

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

**NEW QUESTION 236**

- (Exam Topic 4)



You have an Azure Active Directory (Azure AD) tenant named contoso.com  
You need to configure diagnostic settings for contoso.com. The solution must meet the following requirements:

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

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

**Answer:** A

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

**NEW QUESTION 239**

- (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 243**

- (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/p

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 247**

- (Exam Topic 4)

From Azure Security Center, you enable Azure Container Registry vulnerability scanning of the images in Registry1. You perform the following actions:

- > Push a Windows image named Image1 to Registry1.
- > Push a Linux image named Image2 to Registry1.
- > Push a Windows image named Image3 to Registry1.
- > Modify Image1 and push the new image as Image4 to Registry1.
- > Modify Image2 and push the new image as Image5 to Registry1.

Which two images will be scanned for vulnerabilities? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Image4
- B. Image2
- C. Image1
- D. Image3
- E. Image5

**Answer:** BC

**NEW QUESTION 251**

- (Exam Topic 4)

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

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

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

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

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

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

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

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area

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

NEW QUESTION 255

- (Exam Topic 4)

You have an Azure Sentinel workspace that has an Azure Active Directory (Azure AD) data connector. You are threat hunting suspicious traffic from a specific IP address. You need to annotate an intermediate event stored in the workspace and be able to reference the IP address when navigating through the investigation graph. Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Add the query to Favorites.

From the Azure Sentinel workspace, run an Azure Log Analytics query.

In a Jupyter notebook, create a reference to the IP address.

Add a bookmark and assign a tag.

Add a bookmark and map an entity.

From Azure Monitor, run an Azure Log Analytics query.

Select a query result.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 257

- (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. Sub1 contains an Azure virtual machine named VM1 that runs Windows Server 2016. You need to encrypt VM1 disks by using Azure Disk Encryption. Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Configure secrets for the Azure key vault.

Create an Azure key vault.

Run Set-AzureRmStorageAccount.

Configure access policies for the Azure key vault.

Run Set-AzureRmVmDiskEncryptionExtension.

Answer Area

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

References:

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

**NEW QUESTION 260**

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that contains a user named Admin1. Admin1 is assigned the Application developer role.

You purchase a cloud app named App1 and register App1 in Azure AD.

Admin1 reports that the option to enable token encryption for App1 is unavailable.

You need to ensure that Admin1 can enable token encryption for App1 in the Azure portal. What should you do?

- A. Upload a certificate for App1.
- B. Modify the API permissions of App1.
- C. Add App1 as an enterprise application.
- D. Assign Admin1 the Cloud application administrator role.

**Answer:** C

**Explanation:**

This is a tricky one because uploading a certificate is also required. However, the question states that the Token Encryption option is unavailable. This is because the app is not added as an enterprise application. When the app is added as an enterprise application, the Token Encryption option will be available. Then you can upload the certificate.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/howto-saml-token-encryption>

**NEW QUESTION 265**

- (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 10

You need to create a new Azure AD directory named 28681041.onmicrosoft.com. The new directory must contain a new user named user1@28681041.onmicrosoft.com.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

To create a new Azure AD directory named 28681041.onmicrosoft.com that contains a new user named user1@28681041.onmicrosoft.com, you can follow these steps:

- In the Azure portal, search for and select Azure Active Directory.
- In the left pane, select Domains.
- Select Add domain.
- In the Add a custom domain pane, enter the following information:
- Domain name: Enter the domain name you want to use. For example, 28681041.onmicrosoft.com.
- Add domain: Select Add domain.
- In the left pane, select Users.
- Select New user.
- In the New user pane, enter the following information:
- User name: Enter the user name you want to use. For example, user1@28681041.onmicrosoft.com.
- Name: Enter the name of the user.
- Password: Enter a password for the user.
- Groups: Select the groups you want the user to be a member of.
- Select Create.

You can find more information on these topics in the following Microsoft documentation:

- Add a custom domain name to Azure Active Directory
- Create a new user in your organization - Azure Active Directory

**NEW QUESTION 267**

- (Exam Topic 4)

Your 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 performs 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 270**

- (Exam Topic 4)

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

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

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

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

NOTE: Each correct selection is worth one point.

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

**Answer:** AC

**Explanation:**

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

**NEW QUESTION 273**

- (Exam Topic 4)

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

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

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

What should you do first?

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

**Answer:** A

**Explanation:**

Reference:

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

**NEW QUESTION 275**

- (Exam Topic 4)

You have an Azure subscription that contains a user named User1. User1 is assigned the Reader role for the subscription.

You plan to create a custom role named Role1 and assign Role1 to User1.

You need to ensure that User1 can create and manage application security groups by using the Azure portal. Which two permissions should you add to Role1? To answer, select the appropriate permission in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

**Add permissions**

<b>Microsoft Monitoring Insights</b> Microsoft.SecurityGraph	<b>Microsoft Monitoring Insights</b> Enable your workforce to be productive on all their devices, while keeping your organization's information protected.	<b>Microsoft Monitoring Insights</b> Microsoft.DynamicsTelemetry	<b>Microsoft Network</b> Connect cloud and on-premises infrastructure and services to provide your customers and users the best.
<b>Microsoft Operations Management</b> A simplified management solution for any enterprise	<b>Microsoft Policy Insights</b> Summarize policy states for the subscription level policy definition.	<b>Microsoft Portal</b> Build, manage, and monitor all Azure products in a single, unified console.	<b>Microsoft Power BI Dedicated</b> Manage Power BI Premium dedicated capacities for exclusive use by an organization.
<b>Microsoft Power Platform</b> Microsoft.PowerPlatform	<b>Microsoft Project Babylon</b> Microsoft.ProjectBabylon	<b>Microsoft Purview</b> Microsoft.Purview	<b>Microsoft Resource Graph</b> Powerful tool to query, explore, and analyze your cloud resources at scale.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

\* 1. Microsoft Portal 2. Microsoft Network

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/azure-services-resource-providers>

**NEW QUESTION 276**

- (Exam Topic 4)

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

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

You have an Azure subscription named Sub1.

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

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

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

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

- A. Yes
- B. No

**Answer:** A

**Explanation:**

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 effects 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 278**

- (Exam Topic 4)

You have an Azure subscription named Sub1. Sub1 contains a virtual network named VNet1 that contains one subnet named Subnet1.

You create a service endpoint for Subnet1.

Subnet1 contains an Azure virtual machine named VM1 that runs Ubuntu Server 18.04.

You need to deploy Docker containers to VM1. The containers must be able to access Azure Storage resources and Azure SQL databases by using the service endpoint.

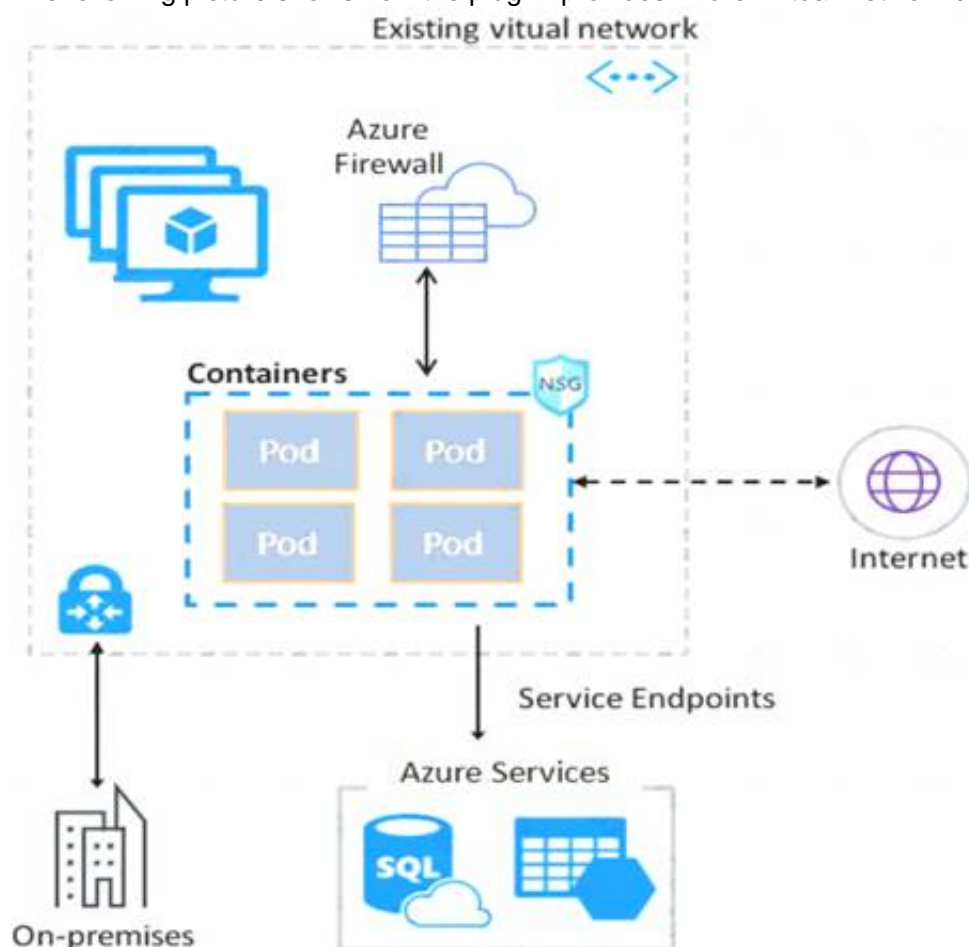
- A. Create an application security group and a network security group (NSG).
- B. Edit the docker-compose.yml file.
- C. Install the container network interface (CNI) plug-in.

**Answer:** C

**Explanation:**

The Azure Virtual Network container network interface (CNI) plug-in installs in an Azure Virtual Machine. The plug-in supports both Linux and Windows platform. The plug-in assigns IP addresses from a virtual network to containers brought up in the virtual machine, attaching them to the virtual network, and connecting them directly to other containers and virtual network resources. The plug-in doesn't rely on overlay networks, or routes, for connectivity, and provides the same performance as virtual machines.

The following picture shows how the plug-in provides Azure Virtual Network capabilities to Pods:



References:

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

**NEW QUESTION 282**

- (Exam Topic 4)

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

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

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 286**

- (Exam Topic 4)

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

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

You need to ensure that ServerAdmins can perform the following tasks: Create virtual machine to the existing virtual network in RG2 only. The solution must use the principle of least privilege. Which two role-based access control (RBAC) roles should you assign to ServerAdmins? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

**Answer:** DF

**NEW QUESTION 288**

- (Exam Topic 4)

You are implementing conditional access policies.

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

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

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

Which level should you identify for each risk event? To answer, drag the appropriate levels to the correct risk events. Each level may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content. NOTE: Each correct selection is worth one point.

Levels

Answer Area

High

Impossible travel to atypical locations:

Low

Users with leaked credentials:

Medium

Sign ins from IP addresses with suspicious activity:

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Medium High Medium Refer

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

**NEW QUESTION 292**

- (Exam Topic 4)

You have an Azure virtual machine named VM1.

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

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

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

**Answer:** A

**Explanation:**

Reference:

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

**NEW QUESTION 295**

- (Exam Topic 4)

You are configuring and securing a network environment.

You deploy an Azure virtual machine named VM1 that is configured to analyze network traffic. You need to ensure that all network traffic is routed through VM1.

What should you configure?

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

**Answer:** C

**Explanation:**

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

Note: User Defined Routes

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

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

Reference:

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

**NEW QUESTION 297**

- (Exam Topic 4)

You have an Azure Sentinel workspace that contains an Azure Active Directory (Azure AD) connector, an Azure Log Analytics query named Query1 and a playbook named Playbook1.

Query1 returns a subset of security events generated by Azure AD.

You plan to create an Azure Sentinel analytic rule based on Query1 that will trigger Playbook1. You need to ensure that you can add Playbook1 to the new rule.

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

NOTE: Each correct selection is worth one point.

Create the rule and set the type to:

Fusion
Microsoft Security incident creation
Scheduled

Configure the playbook to include:

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

- A. Mastered
- B. Not Mastered



Answer: A

Explanation:

Reference:

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

NEW QUESTION 301

- (Exam Topic 4)

You have an Azure subscription mat contains a resource group named RG1. RG1 contains a storage account named storage1.

You have two custom Azure rotes named Role1 and Role2 that are scoped to RG1. The permissions for Role1 are shown in the following JSON code.

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

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

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 305

- (Exam Topic 4)

You have a Azure subscription that contains an Azure Container Registry named Registry1. The subscription uses the Standard use tier of Azure Security Center.

You upload several container images to Register1.

You discover that vulnerability security scans were not performed

You need to ensured that the images are scanned for vulnerabilities when they are uploaded to Registry1. What should you do?

- A. From the Azure portal modify the Pricing tier settings.
- B. From Azure CLI, lock the container images.
- C. Upload the container images by using AzCopy
- D. Push the container images to Registry1 by using Docker

Answer: A

Explanation:

Reference:

<https://charbelnemnom.com/scan-container-images-in-azure-container-registry-with-azure-security-center/>

#### NEW QUESTION 310

- (Exam Topic 4)

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

Name	Role
Admin1	Global administrator
Admin2	Group administrator
Admin3	User administrator

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

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

NOTE: Each correct selection is worth one point.

Users who can create a security group named Contoso Sales:

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

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

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

- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

Reference:

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

#### NEW QUESTION 314

- (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 316

- (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 318**

- (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 322**

- (Exam Topic 4)

From Azure Security, you create a custom alert rule.

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

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

**Answer:** A

**Explanation:**

References:

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

NEW QUESTION 325

- (Exam Topic 4)

You need to configure an access review. The review will be assigned to a new collection of reviews and reviewed by resource owners. Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Create an access review program.

Set Reviewers to Selected users.

Create an access review audit.

Create an access review control.

Set Reviewers to Group owners.

Set Reviewers to Members.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Step 1: Create an access review program Step 2: Create an access review control Step 3: Set Reviewers to Group owners  
In the Reviewers section, select either one or more people to review all the users in scope. Or you can select to have the members review their own access. If the resource is a group, you can ask the group owners to review.

Reviewers

Reviewers

Programs

Link to program

Group owners

Group owners

Selected users

Members (self)

References:  
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-programs-controls

NEW QUESTION 327

- (Exam Topic 4)

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

All Alerts

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

Don't see a subscription? Open Directory + Subscription settings

Subscription Azure Pass - Sponsorship

Resource group Type to start filtering

Resource type 0 selected

Resource Type to start filtering

Time range Past hour

Monitor service 15 selected

Monitor condition 2 selected

Severity Sev 4

Alert state 3 selected

Smart group id Smart group id

All Alerts Alerts By Smart Group (Preview)

Search by name (case-insensitive)

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

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



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

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

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

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

- A. Mastered
- B. Not Mastered

Answer: A

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

NEW QUESTION 332  
- (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 334

- (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 338

- (Exam Topic 4)  
You have an Azure subscription that contains a Microsoft Sentinel workspace.  
Microsoft Sentinel is configured to ingest logs from several Azure workloads. A third-party service management platform is used to manage incidents.  
You need to identify which Microsoft Sentinel components to configure to meet the following requirements:  
• When Microsoft Sentinel identifies a threat an incident must be created.  
• A ticket must be logged in the service management platform when an incident is created in Microsoft Sentinel.  
Which component should you identify for each requirement? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

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

Analytics

Data connectors

Playbooks

Workbooks

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

Analytics

Data connectors

Playbooks

Workbooks

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

When an incident is created, a ticket must be created in the service management platform:

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



NEW QUESTION 339

- (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 Vent 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 343

- (Exam Topic 4)

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

Name	Subscription role	Azure Active Directory (Azure AD) user role	Multi-factor authentication (MFA) status
User1	Owner	Authentication administrator	Enabled
User2	None	Global administrator	Enforced
User3	None	Global administrator	Disabled

Which users can enable Azure AD Privileged Identity Management (PIM)?

- A. User2 and User3 only
- B. User1 and User2 only
- C. User2 only
- D. User1 only

Answer: B

Explanation:

Reference:

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

NEW QUESTION 346

- (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 2012R2	Running
VM3	Windows Server 2016	Stopped
VM4	Ubuntu Server 18.04 LTS	Running

For which virtual machine can you enable Update Management?

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

E. VM1, VM2, and VM3 only

Answer: C

Explanation:

References:

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

NEW QUESTION 347

- (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": []
  }
]
```

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 351

- (Exam Topic 4)

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



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

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

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

**Answer: C**

#### NEW QUESTION 352

- (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 354

- (Exam Topic 4)

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

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

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

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

The solution must use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

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

**Answer: AF**

**Explanation:**

Reference:

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

**NEW QUESTION 359**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### 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

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The az-500 Practice Test Here](#)**