



# Microsoft

## Exam Questions az-500

Microsoft Azure Security Technologies

## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

- (Exam Topic 4)  
You have an Azure subscription named Subscription1.  
You deploy a Linux virtual machine named VM1 to Subscription1. You need to monitor the metrics and the logs of VM1.  
D18912E1457D5D1DDCBD40AB3BF70D5D  
What should you use?

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

Answer: A

NEW QUESTION 2

- (Exam Topic 4)  
Lab Task  
Task 3  
You need to ensure that a user named Danny-31330471 can sign in to any SQL database on a Microsoft SQL server named web31330471 by using SQL Server Management Studio (SSMS) and Azure AD credentials.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Create and register an Azure AD application. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to specify a name, such as SQLServerCTP1, and select the supported account types, such as Accounts in this organization directory only.  
Grant application permissions. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to assign the Directory.Read.All permission to the application and grant admin consent for your organization.  
Create and assign a certificate. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to create a self-signed certificate and upload it to the application. You also need to store the certificate in Azure Key Vault and grant access policies to the application and your SQL Server.  
Configure Azure AD authentication for SQL Server through Azure portal. You can use the Azure portal to do this. You need to select your SQL Server resource and enable Azure AD authentication. You also need to select your Azure AD application as the Azure AD admin for your SQL Server.  
Create logins and users. You can use SSMS or Transact-SQL to do this. You need to connect to your SQL Server as the Azure AD admin and create a login for Danny-31330471. You also need to create a user for Danny-31330471 in each database that he needs access to.  
Connect with a supported authentication method. You can use SSMS or SqlClient to do this. You need to specify the Authentication connection property in the connection string as Active Directory Password or Active Directory Integrated. You also need to provide the username and password of Danny-31330471.

NEW QUESTION 3

- (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 4**

- (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 5**

- (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 6**

- (Exam Topic 4)

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

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

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

What should you include in the recommendation?

- A. an Azure policy

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

**Answer:** D

**Explanation:**

Reference:

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

**NEW QUESTION 7**

- (Exam Topic 4)

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

What should you do?

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

**Answer:** A

**NEW QUESTION 8**

- (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 9**

- (Exam Topic 4)

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

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

Transparent Data Encryption (TDE) is disabled on SQL1.

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

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

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

NOTE: Each correct selection is worth one point.

**Answer Area**

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application Description automatically generated

#### NEW QUESTION 10

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1. You plan to publish several apps in the tenant. You need to ensure that User1 can grant admin consent for the published apps.

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

NOTE: Each correct selection is worth one point.

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

**Answer:** CE

#### Explanation:

Reference:

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

#### NEW QUESTION 10

- (Exam Topic 4)

You have an Azure SQL Database server named SQL1.

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

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

**Answer:** B

#### Explanation:

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

References:

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

#### NEW QUESTION 12

- (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 15

- (Exam Topic 4)

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

```

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

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

```

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

Password1:

	▼
Never	
Always	
Only after May 1, 2019	

Password2:

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Never Password1 is disabled.

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

```

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

```

Reference:

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

**NEW QUESTION 19**

- (Exam Topic 4)

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

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

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

You need to deploy Microsoft Antimalware to the virtual machines. Solution: You connect to each virtual machine and add a Windows feature. Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

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

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

NEW QUESTION 24

- (Exam Topic 4)

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com.

The company is developing an application named App1. App1 will run as a service on server that runs Windows Server 2016. App1 will authenticate to contoso.com and access Microsoft Graph to read directory data.

You need to delegate the minimum required permissions to App1.

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

Actions

Grant permissions

Add a delegated permission.

Configure Azure AD Application Proxy.

Add an application permission.

Create an app registration.

Answer Area

<

>

⬆

⬇

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Step 1: Create an app registration

First the application must be created/registered. Step 2: Add an application permission

Application permissions are used by apps that run without a signed-in user present. Step 3: Grant permissions

NEW QUESTION 29

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

Azure AD Privileged Identity Management (PIM) is enabled for the tenant. In PIM, the Password Administrator role has the following settings:

- > Maximum activation duration (hours): 2
- > Send email notifying admins of activation: Disable
- > Require incident/request ticket number during activation: Disable
- > Require Azure Multi-Factor Authentication for activation: Enable
- > Require approval to activate this role: Enable
- > Selected approver: Group1

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

Name	Assignment type
User1	Active
User2	Eligible
user3	Eligible

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

Statements

When User1 signs in, the user is assigned the Password Administrator role automatically.

User2 can request to activate the Password Administrator role.

If User3 wants to activate the Password Administrator role, the user can approve their own request.

Yes

No

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

YES (Already active)

YES (The user will be prompted for MFA regardless the MFA Status of the user) NO ( Even the user is included in the group, a user can't approve itself)

<https://docs.microsoft.com/es-es/azure/active-directory/privileged-identity-management/pim-deployment-plan> (Require approval section)

**NEW QUESTION 32**

- (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	<b>Not applicable</b>

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 37**

- (Exam Topic 4)

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

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

What should you use?

- A. Key Vault properties

- B. Azure Policy
- C. Azure Purview
- D. Azure Blueprints

**Answer:** B

#### NEW QUESTION 41

- (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 42

- (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	<i>Not applicable</i>
NSG2	Network security group (NSG)	Subnet1	<i>Not applicable</i>
Subnet1	Subnet	<i>Not applicable</i>	<i>Not applicable</i>
VM5	Virtual machine	Subnet1	NSG1

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

### JIT VM access configuration

VM5








+ Add     Save     Discard

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

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

You enable JIT VM access for VM5.

NSG1 has the inbound rules shown in the following exhibit.

Priority	Name	Port	Protocol	Source	Destination	Action
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 44**

- (Exam Topic 4)

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

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

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

Operating systems:

Platforms:

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Operating systems:

Platforms:

#### NEW QUESTION 48

- (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 or 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 A root "TXT" record for verification

A "CNAME" record for the www 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 50

- (Exam Topic 4)

You have an Azure subscription that contains an Azure SQL database named SQLDB1. SQLDB1 contains the columns shown in the following table.

Name	Data type	Sample value
Email	Varchar	admin@contoso.com
Birthday	Date	2010-07-07

For the Email and Birthday columns, you implement dynamic data masking by using the default masking function.

Which value will the users see in each column? To answer, drag the appropriate values to the correct columns. Each value may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

**Values**

- 1900-01-01
- 1900-01-01 00:00:00.0000
- 2010-XX-XX
- XXXX

**Answer Area**

Email:

Birthday:

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Values

1900-01-01

1900-01-01 00:00:00.0000

2010-XX-XX

XXXX

Answer Area

Email:

1900-01-01

Birthday:

2010-XX-XX

#### NEW QUESTION 55

- (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 57

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains three security groups named Group1, Group2, and Group3 and the users shown in the following table.

Name	Role	Member of
User1	Application administrator	Group1
User2	Application developer	Group2
User3	Cloud application administrator	Group3

Group3 is a member of Group2.

In contoso.com, you register an enterprise application named App1 that has the following settings:

- > Owners: User1
- > Users and groups: Group2

You configure the properties of App1 as shown in the following exhibit.

Save Discard Delete Got feedback

Enabled for users to sign-in? •

Yes No

Name \* •

App1

Homepage URL •

Logo •

AP

Select a file

Application ID •

75082794-3617-4347-ac6d-88cfa564072

Object ID •

4926ab6c-ef57-4c9f-a028-f6d635cde655

User assignment required? •

Yes No

Visible to users •

Yes No

Notes •

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 has App1 listed on his My Apps portal.	<input type="radio"/>	<input type="radio"/>
User2 has App1 listed on her My Apps portal.	<input type="radio"/>	<input type="radio"/>
User3 has App1 listed on her My Apps portal.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Text Description automatically generated

Reference:

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

NEW QUESTION 62

- (Exam Topic 4)

You have three Azure subscriptions and a user named User1.

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

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

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

Actions

Create a management group.

Add the three subscriptions to the management group.

Assign User1 the Global administrator role.

Assign User1 the Owner role for the management group.

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

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Actions

Create a management group.

Add the three subscriptions to the management group.

Assign User1 the Global administrator role.

Assign User1 the Owner role for the management group.

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

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

Assign User1 the Global administrator role.

Add the three subscriptions to the management group.

NEW QUESTION 64

- (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 65**

- (Exam Topic 4)

You have an Azure subscription that contains a storage account and an Azure web app named App1. App1 connects to an Azure Cosmos DB database named Cosmos1 that uses a private endpoint named Endpoint1. Endpoint1 has the default settings. You need to validate the name resolution to Cosmos1. Which DNS zone should you use?

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

**Answer:** D

**NEW QUESTION 69**

- (Exam Topic 4)

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

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

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

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

Save Discard Refresh

Allow access from

All networks Selected networks

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

Virtual networks


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

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

Firewall

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

Address Range

13.80.73.87 

IP address or CIDR

Exceptions

☒ Allow trusted Microsoft services to access this storage account ⓘ  
☐ Allow read access to storage logging from any network  
☐ Allow read access to storage metrics from any network

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

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

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Yes

The public IP of VM1 is allowed through the firewall.

Box 2: No

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

Box 3: No

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

Reference:

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

**NEW QUESTION 71**

- (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 74**

- (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 78**

- (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 80

- (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 83

- (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 85

- (Exam Topic 4)

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

After syncing all on-premises identities to Azure AD, you are informed that users with a givenName attribute starting with LAB should not be allowed to sync to Azure AD.

Which of the following actions should you take?

- A. You should make use of the Synchronization Rules Editor to create an attribute-based filtering rule.
- B. You should configure a DNAT rule on the Firewall.
- C. You should configure a network traffic filtering rule on the Firewall.
- D. You should make use of Active Directory Users and Computers to create an attribute-based filtering rule.

**Answer:** A

#### Explanation:

Use the Synchronization Rules Editor and write attribute-based filtering rule. Reference:

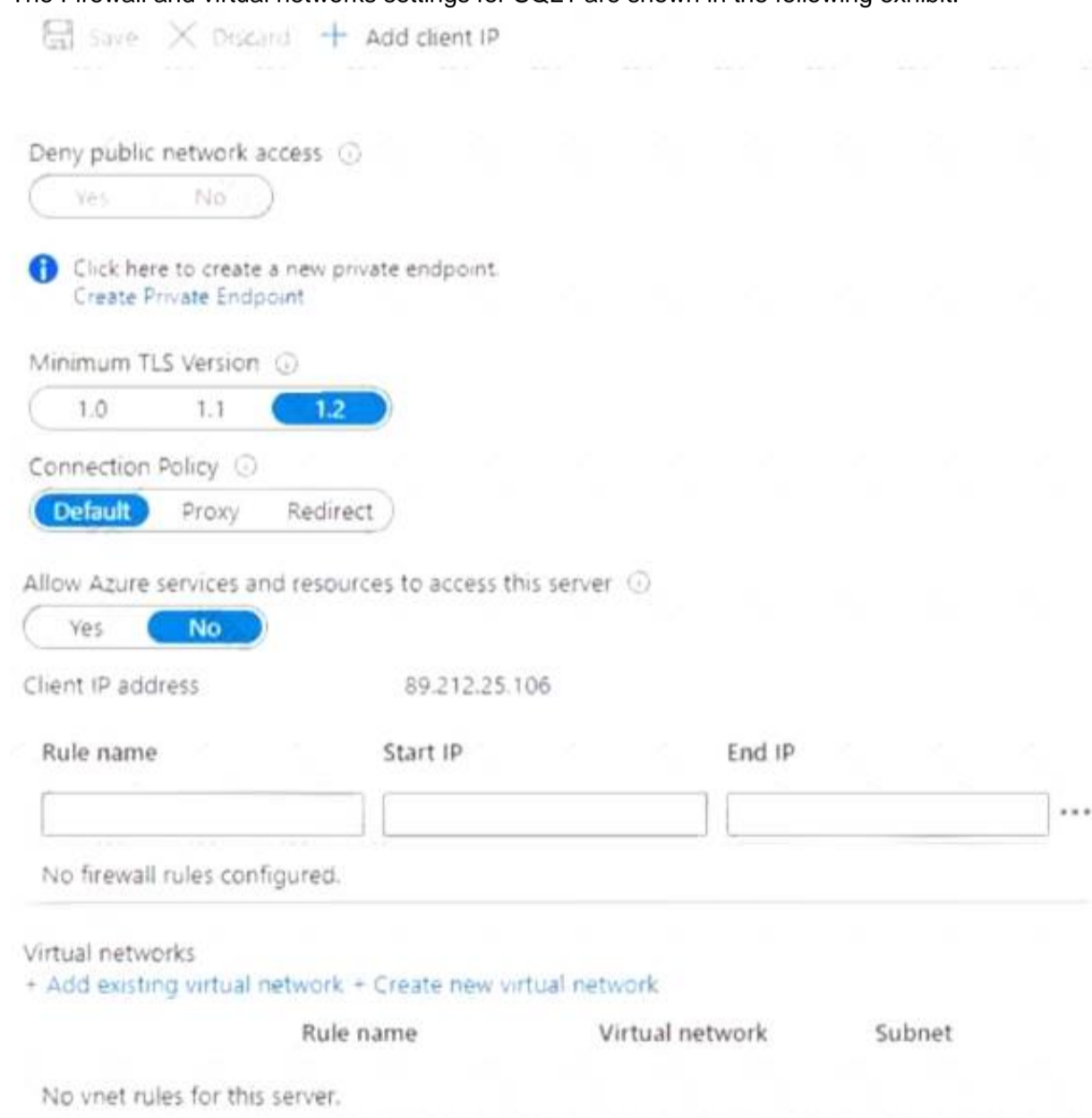
<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration>

#### NEW QUESTION 90

- (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.



The screenshot shows the Azure Firewall configuration page for a resource named SQL1. At the top, there are buttons for 'Save', 'Discard', and 'Add client IP'. Below this, the 'Deny public network access' toggle is set to 'No'. An information icon with a link 'Click here to create a new private endpoint. Create Private Endpoint' is visible. The 'Minimum TLS Version' dropdown is set to '1.2'. The 'Connection Policy' dropdown is set to 'Default'. The 'Allow Azure services and resources to access this server' toggle is set to 'No'. Under 'Client IP address', the IP '89.212.25.106' is listed. Below this is a table for firewall rules with columns 'Rule name', 'Start IP', and 'End IP'. The table is currently empty, with a message 'No firewall rules configured.' below it. At the bottom, there is a section for 'Virtual networks' with a link '+ Add existing virtual network + Create new virtual network'. Below this is a table with columns 'Rule name', 'Virtual network', and 'Subnet'. The table is empty, with a message 'No vnet rules for this server.' below it.

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 92

- (Exam Topic 4)

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

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

- A. From Azure Directory (Azure AD) Privileged Identity Management (PIM), activate the Security administrator user role.
- B. From Azure Active Directory (Azure AD) Privileged Identity Management (PIM), activate the Owner role for the virtual machine.

- C. From the Azure portal, select the virtual machine, select Connect, and then select Request access.  
D. From the Azure portal, select the virtual machine and add the Network Watcher Agent virtual machine extension.

**Answer:** C

**Explanation:**

Reference:

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

**NEW QUESTION 95**

- (Exam Topic 4)

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

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

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

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

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

- A. Yes  
B. No

**Answer:** A

**Explanation:**

References:

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

**NEW QUESTION 97**

- (Exam Topic 4)

You have an Azure subscription.

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

- \* Provide access to DDoS rapid response support during active attacks.
- \* Protect Basic SKU public IP addresses.

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

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

NOTE: Each correct selection is worth one point.



- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**



**NEW QUESTION 99**

- (Exam Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the

stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have a hybrid configuration of Azure Active Directory (AzureAD). You have an Azure HDInsight cluster on a virtual network. You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials. You need to configure the environment to support the planned authentication. Solution: You create a site-to-site VPN between the virtual network and the on-premises network. Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

**Explanation:**

You can connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway. Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions: Create Azure Virtual Network. Create a custom DNS server in the Azure Virtual Network. Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver. Configure forwarding between the custom DNS server and your on-premises DNS server. References: <https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network> <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal>

**NEW QUESTION 104**

- (Exam Topic 4)

You have an Azure Active directory tenant that syncs with an Active Directory Domain Services (AD DS) domain. You plan to create an Azure file share that will contain folders and files. Which identity store can you use to assign permissions to the Azure file share and folders within the share? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

Azure files share:

Folders in the file share:

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Azure files share:

Folders in the file share:

**NEW QUESTION 107**

- (Exam Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You use Azure Security Center for the centralized policy management of three Azure subscriptions. You use several policy definitions to manage the security of the subscriptions. You need to deploy the policy definitions as a group to all three subscriptions. Solution: You create a resource graph and an assignment that is scoped to a management group. Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

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

**NEW QUESTION 112**

- (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.

Statements	Yes	No
You can start VM1.	<input type="radio"/>	<input type="radio"/>
You can start VM2.	<input type="radio"/>	<input type="radio"/>
You can create a virtual machine in RG2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
 B. Not Mastered

**Answer: A**

**Explanation:**

NO NO NO

- 1) cannot perform write operation because following scope(s) are locked: 'subscriptions/xxxx/resourceGroups/xxx' Please remove the lock and try again.
- 2) When creating a VM in a resource group with a Read Only lock an error is shown: "The selected resource group is read only"
- 3) Because of the read only lock virtual machines cannot be started nor stopped when the lock is added after the machine started. (not part of this use case, but still good to know.

The article referenced in the answer states different because that is scoped to blueprints.

In the Lock Resources pages is states the following regarding starting VMs:

"A ReadOnly lock on a resource group that contains a virtual machine prevents all users from starting or restarting the virtual machine. These operations require a POST request."

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

#### NEW QUESTION 117

- (Exam Topic 4)

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

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

You create the Azure policies shown in the following table.

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

You create the resource locks shown in the following table.

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

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

Answer Area

Statements	Yes	No
You can start VM1.	<input type="radio"/>	<input type="radio"/>
You can start VM2.	<input type="radio"/>	<input type="radio"/>
You can create a virtual machine in RG2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 122

- (Exam Topic 4)  
You create an alert rule that has the following settings:

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

You create an action rule that has the following settings:

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

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

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

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Box 1:  
The scope for the action rule is set to VM1 and is set to suppress alerts indefinitely.  
Box 2:  
The scope for the action rule is not set to VM2. Box 3:  
Adding a tag is not an administrative operation. References:  
<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-activity-log>  
<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-action-rules>

NEW QUESTION 125

- (Exam Topic 4)  
You have an Azure subscription named Sub1 that contains an Azure Storage account named Contosostorage1 and an Azure key vault named Contosokeyvault1.

You plan to create an Azure Automation runbook that will rotate the keys of Contosostorage1 and store them in Contosokeyvault1. You need to implement prerequisites to ensure that you can implement the runbook.

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

Actions

Run Set-AzureRmKeyVaultAccessPolicy

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

Create a user-assigned managed identity.

Create a connection resource in the Azure Automation account.

Answer Area

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Step 1: Create an Azure Automation account

Runbooks live within the Azure Automation account and can execute PowerShell scripts. Step 2: Import PowerShell modules to the Azure Automation account Under 'Assets' from the Azure Automation account Resources section select 'to add in Modules to the runbook. To execute key vault cmdlets in the runbook, we need to add AzureRM.profile and AzureRM.key vault.

Step 3: Create a connection resource in the Azure Automation account

You can use the sample code below, taken from the AzureAutomationTutorialScript example runbook, to authenticate using the Run As account to manage Resource Manager resources with your runbooks. The AzureRunAsConnection is a connection asset automatically created when we created 'run as accounts' above. This can be found under Assets -> Connections. After the authentication code, run the same code above to get all the keys from the vault.

```
$connectionName = "AzureRunAsConnection" try
{
# Get the connection "AzureRunAsConnection "
$servicePrincipalConnection=Get-AutomationConnection -Name $connectionName "Logging in to Azure..."
Add-AzureRmAccount `
-ServicePrincipal `
-TenantId $servicePrincipalConnection.TenantId `
-ApplicationId $servicePrincipalConnection.ApplicationId `
-CertificateThumbprint $servicePrincipalConnection.CertificateThumbprint
}
```

References:

<https://www.rahulpnath.com/blog/accessing-azure-key-vault-from-azure-runbook/>

**NEW QUESTION 130**

- (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>

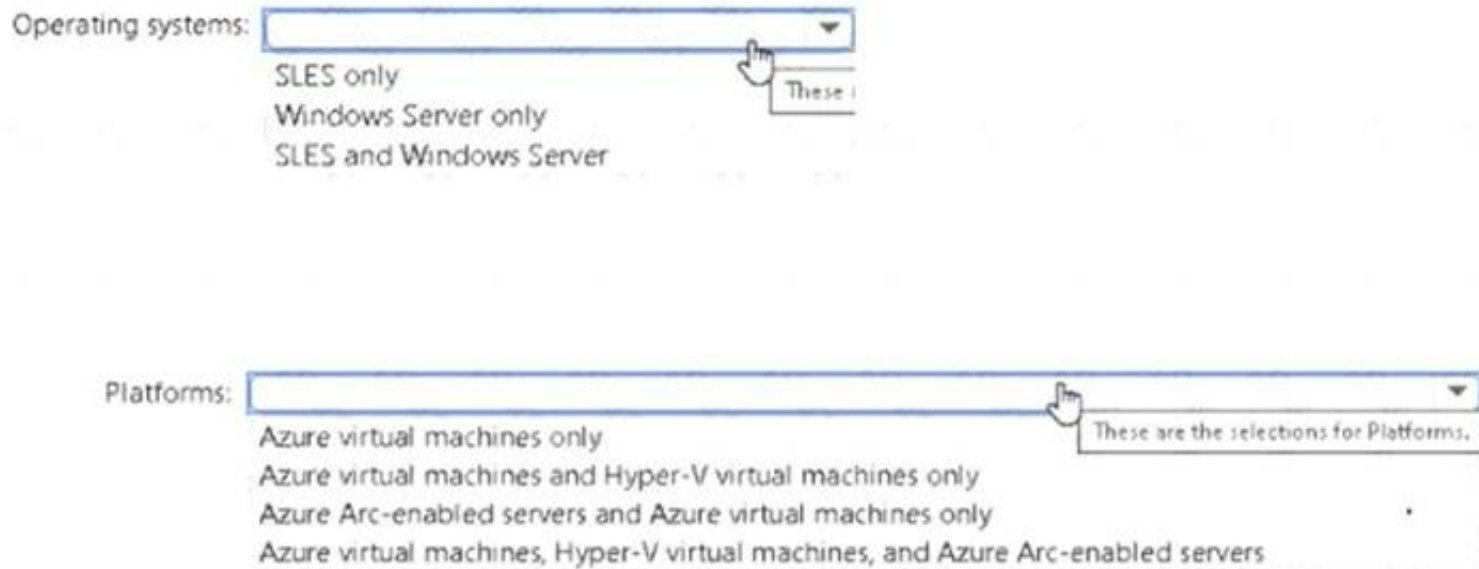
#### NEW QUESTION 134

- (Exam Topic 4)

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

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

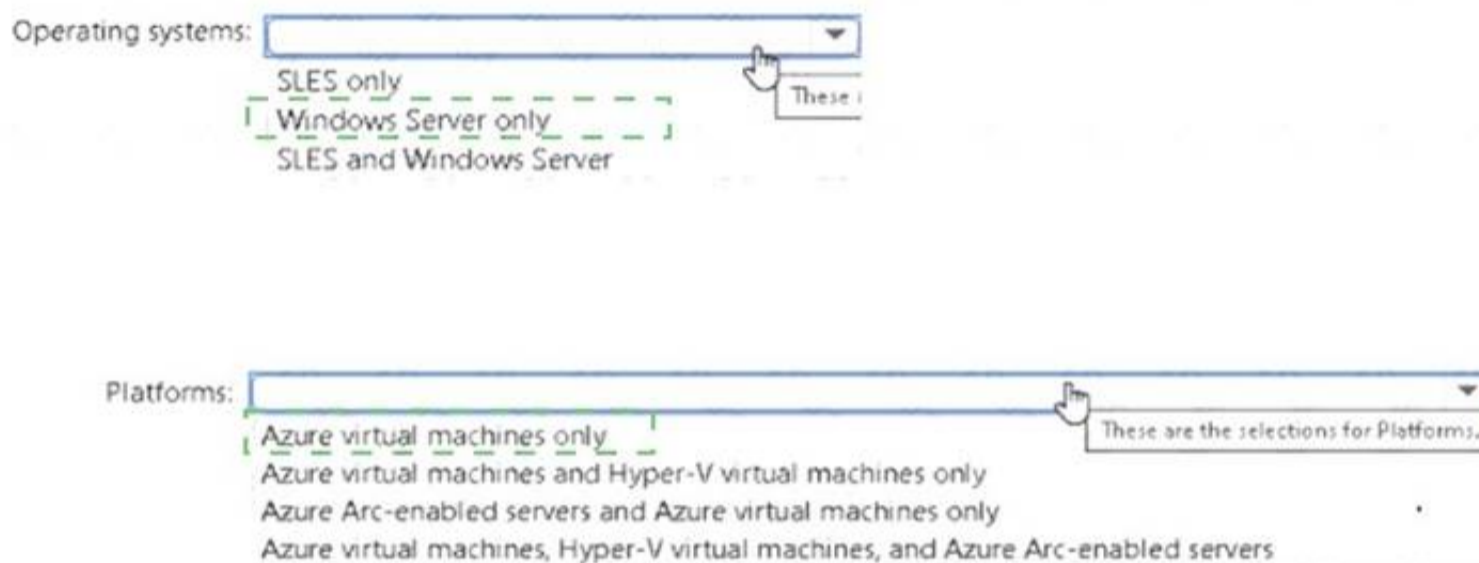
You have an Azure subscription that contains multiple virtual machines that run either Windows Server 2019 or SLES. You plan to implement adaptive application controls in Microsoft Defender for Cloud. Which operating systems and platforms can you monitor? To answer, select the appropriate options in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



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



#### NEW QUESTION 138

- (Exam Topic 4)

Your on-premises network contains a Hyper-V virtual machine named VM1. You need to use Azure Arc to onboard VM1 to Microsoft Defender for Cloud. What should you install first?

- A. the Azure Monitor agent
- B. the Azure Connected Machine agent
- C. the Log Analytics agent
- D. the guest configuration agent

**Answer:** B

#### NEW QUESTION 139

- (Exam Topic 4)

Your network contains an on-premises Active Directory domain named corp.contoso.com.

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

You sync all on-premises identities to Azure AD.

You need to prevent users who have a givenName attribute that starts with TEST from being synced to Azure AD. The solution must minimize administrative effort. What should you use?

- A. Synchronization Rules Editor
- B. Web Service Configuration Tool
- C. the Azure AD Connect wizard
- D. Active Directory Users and Computers

**Answer:** A

**Explanation:**

Use the Synchronization Rules Editor and write attribute-based filtering rule. References:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration>

#### NEW QUESTION 143

- (Exam Topic 4)

You have an Azure subscription named Sub1.

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

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

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

Actions	Answer Area
Create a JSON file.	
Run the Update-AzureRmManagementGroup cmdlet.	
Create an XML file.	
Run the New-AzureRmRoleDefinition cmdlet.	
Run the New-AzureRmRoleAssignment cmdlet.	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

References:

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

#### NEW QUESTION 145

- (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 148

- (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 150

- (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 151**

- (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 152**

- (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**

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

**Answer Area**

- 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 154**

- (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 156

- (Exam Topic 4)

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

Name	Type
container1	Container
folder1	File share
table1	Table

User1 is assigned the following roles for storage1:

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

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

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

No, Yes, No

#### NEW QUESTION 161

- (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:	<div>Robocopy.exe</div> <div>Azure Storage Explorer</div> <div>File Explorer</div>
Tools for Share1:	<div>Robocopy.exe</div> <div>Azure Storage Explorer</div> <div>File Explorer</div>

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

## Answer Area



### NEW QUESTION 166

- (Exam Topic 4)

You have an Azure subscription.

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

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

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

**Answer:** A

### NEW QUESTION 167

- (Exam Topic 4)

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

Name	Region	Subnet
VNET1	West US	Subnet11 and Subnet12
VNET2	West US 2	Subnet21
VNET3	East US	Subnet31

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

Name	Network interface	Connected to
VM1	NIC1	Subnet11
VM2	NIC2	Subnet11
VM3	NIC3	Subnet12
VM4	NIC4	Subnet21
VM5	NIC5	Subnet31

On NIC1, you configure an application security group named ASG1. On which other network interfaces can you configure ASG1?

- A. NIC2 only
- B. NIC2, NIC3, NIC4, and NIC5
- C. NIC2 and NIC3 only
- D. NIC2, NIC3, and NIC4 only

**Answer:** C

#### Explanation:

Only network interfaces in NVET1, which consists of Subnet11 and Subnet12, can be configured in ASG1, as all network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in.

Reference:

<https://azure.microsoft.com/es-es/blog/applicationsecuritygroups/>

### NEW QUESTION 171

- (Exam Topic 4)

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

Name	Type
LB1	Azure Standard Load Balancer
VM1	Virtual machine
SQL1	Azure SQL Database
VMSS1	Virtual machine scale set

You plan to deploy an Azure Private Link service named APL1. Which resource must you reference during the creation of APL1?

- A. VMSS1

- B. VM1  
C. SQL  
D. LB1

Answer: D

NEW QUESTION 176

- (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-4500-8b8b-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 180

- (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 9

You need to ensure that the rg1lod28681041n1 Azure Storage account is encrypted by using a key stored in the KeyVault28681041 Azure key vault.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

To ensure that the rg1lod28681041n1 Azure Storage account is encrypted by using a key stored in the KeyVault28681041 Azure key vault, you can follow these steps:

- In the Azure portal, search for and select the storage account named rg1lod28681041n1.
- In the left pane, select Encryption.
- In the Encryption pane, select Customer-managed key.
- In the Customer-managed key pane, select Select from Key Vault.
- In the Select from Key Vault pane, enter the following information:
- Key vault: Select the KeyVault28681041 Azure key vault.
- Key: Select the key you want to use.
- Select Save.

**NEW QUESTION 185**

- (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 189**

- (Exam Topic 4)

You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant. From the Azure portal, you register an enterprise application.

Which additional resource will be created in Azure AD?

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

**Answer:** A

**Explanation:**

Reference:

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

**NEW QUESTION 191**

- (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 193**

- (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 194**

- (Exam Topic 4)

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

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

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

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

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

NOTE: Each correct selection is worth one point.

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

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

Analytics

Data connectors

Playbooks

Workbooks

Analytics

Data connectors

Playbooks

Workbooks

- 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/tutorial-respond-threats-playbook>

NEW QUESTION 197

- (Exam Topic 4)

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

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

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

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

Solution: You create an initiative and an assignment that is scoped to the Tenant Root Group management group.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Reference:

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

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

NEW QUESTION 199

- (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

^

v

- 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>

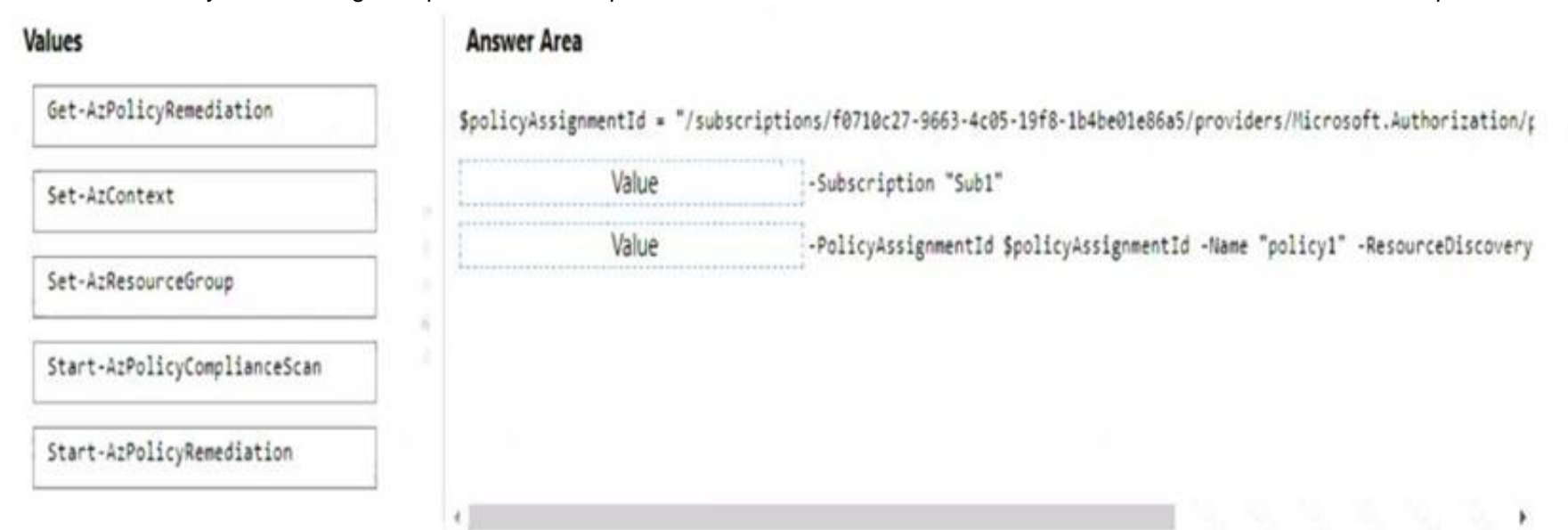
### NEW QUESTION 203

- (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.



- 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 204

- (Exam Topic 4)

You have an Azure subscription that contains an Azure Files share named share1 and a user named User1. Identity-based authentication is configured for share1.

User1 attempts to access share1 from a Windows 10 device by using SMB. Which type of token will Azure Files use to authorize the request?

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

**Answer:** C

#### Explanation:

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

### NEW QUESTION 206

- (Exam Topic 4)

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

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

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

Which Conditional Access policy settings should you configure? To answer, drag the appropriate settings to the correct requirements. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

**Policy settings**

Cloud apps or actions

Conditions

Grant

Session

**Answer Area**

Only allow access to App1 from Windows devices:

Only allow devices that are marked as compliant to access App1:

- A. Mastered  
 B. Not Mastered

**Answer: A**

**Explanation:**

**Policy settings**

Cloud apps or actions

Conditions

Grant

Session

**Answer Area**

Only allow access to App1 from Windows devices: Conditions

Only allow devices that are marked as compliant to access App1: Conditions

#### NEW QUESTION 209

- (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 3

The developers at your company plan to create a web app named App28681041 and to publish the app to <https://www.contoso.com>. You need to perform the following tasks:

- Ensure that App28681041 is registered to Azure AD.
- Generate a password for App28681041.

- A. Mastered  
 B. Not Mastered

**Answer: A**

**Explanation:**

To register App28681041 to Azure AD and generate a password for it, you can follow these steps:

- > In the Azure portal, search for and select Azure Active Directory.
- > In the left pane, select App registrations.
- > Select New registration.
- > In the Register an application pane, enter the following information:
- > Name: App28681041
- > Supported account types: Select the appropriate account types for your scenario.
- > Redirect URI: Leave this field blank.
- > Select Register.
- > In the App registrations pane, select the newly created App28681041 application.
- > In the left pane, select Certificates & secrets.
- > Select New client secret.
- > In the Add a client secret pane, enter the following information:
- > Description: Enter a description for the client secret.
- > Expires: Select an appropriate expiration date for the client secret.
- > Select Add.
- > In the Certificates & secrets pane, copy the value of the newly created client secret.

You can find more information on this topic in the following Microsoft documentation: Quickstart: Register an application with the Microsoft identity platform.

**NEW QUESTION 212**

- (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 214**

- (Exam Topic 4)

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

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

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

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

**Answer: A****Explanation:**

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

**NEW QUESTION 216**

- (Exam Topic 4)

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

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

VNET1 contains two subnets named Subnet1 and Subnet2. Subnet1 has a network ID of 10.0.0.0/24. Subnet2 has a network ID of 10.1.1.0/24.

Contoso1901 is configured as shown in the exhibit. (Click the Exhibit tab.)

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

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

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

Action IPAddressOrRange
-----
Allow  193.77.0.0/16

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

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

PS C:\> _
```

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

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

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Yes

Access from Subnet1 is allowed. Box 2: No

No access from Subnet2 is allowed. Box 3: Yes

Access from IP address 193.77.10.2 is allowed.

**NEW QUESTION 221**

- (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 224**

- (Exam Topic 4)

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

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

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

Which key vault settings should you configure?

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

**Answer:** A

**Explanation:**

References:

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

**NEW QUESTION 229**

- (Exam Topic 4)

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

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

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

What should you do first?

- A. From Azure recreate AKS1,

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

**Answer:** A

**Explanation:**

Reference:

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

**NEW QUESTION 233**

- (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 237**

- (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 242**

- (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 247

- (Exam Topic 4)

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

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

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

**Answer:** D

#### NEW QUESTION 252

- (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 253

- (Exam Topic 4)

You are configuring an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry.

You need to use the auto-generated service principal to authenticate to the Azure Container Registry. What should you create?

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

**Answer:** B

#### Explanation:

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

References:

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

#### NEW QUESTION 256

- (Exam Topic 4)

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

The company develops an application named App1. App1 is registered in Azure AD.

You need to ensure that App1 can access secrets in Azure Key Vault on behalf of the application users. What should you configure?

- A. an application permission without admin consent
- B. a delegated permission without admin consent
- C. a delegated permission that requires admin consent
- D. an application permission that requires admin consent

**Answer:** B

#### Explanation:

Delegated permissions - Your client application needs to access the web API as the signed-in user, but with access limited by the selected permission. This type of permission can be granted by a user unless the permission requires administrator consent.

## NEW QUESTION 261

- (Exam Topic 4)

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

Save Discard Upload Download

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

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

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

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

**Answer: C**

**Explanation:**

Reference:

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

## NEW QUESTION 262

- (Exam Topic 4)

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

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

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

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

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

**Answer Area**

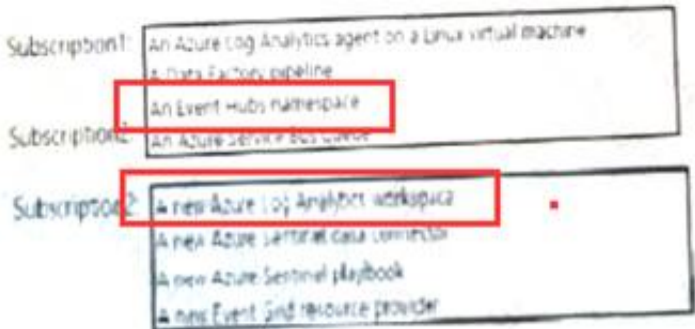
Subscription1:	<input type="checkbox"/> An Azure Log Analytics agent on a Linux virtual machine <input type="checkbox"/> A Data Factory pipeline <input type="checkbox"/> An Event Hubs namespace <input type="checkbox"/> An Azure Service Bus queue
Subscription2:	<input type="checkbox"/> A new Azure Log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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 266

- (Exam Topic 4)

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

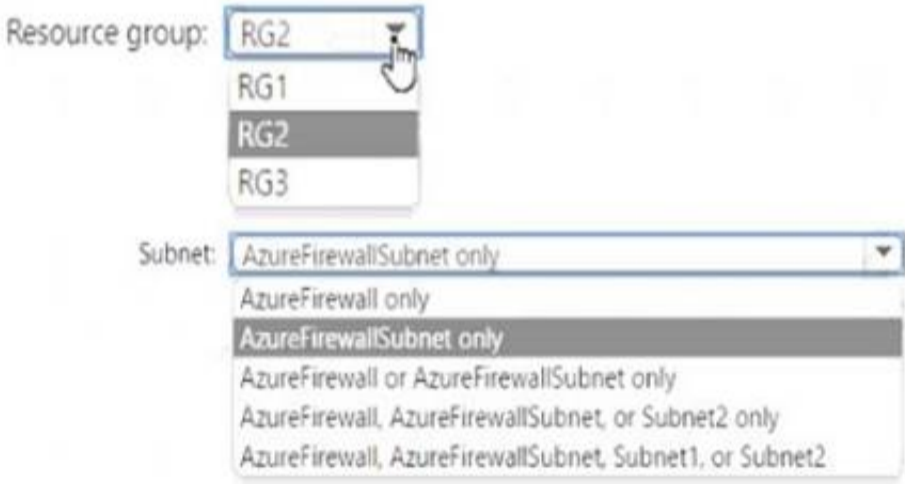
Name	Type	Location	In resource group
RG1	Resource group	East US	Not applicable
RG2	Resource group	West US	Not applicable
RG3	Resource group	Central US	Not applicable
VNet1	Virtual network	Central US	RG2

VNet1 contains the subnets shown in the following table.

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

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

Answer Area

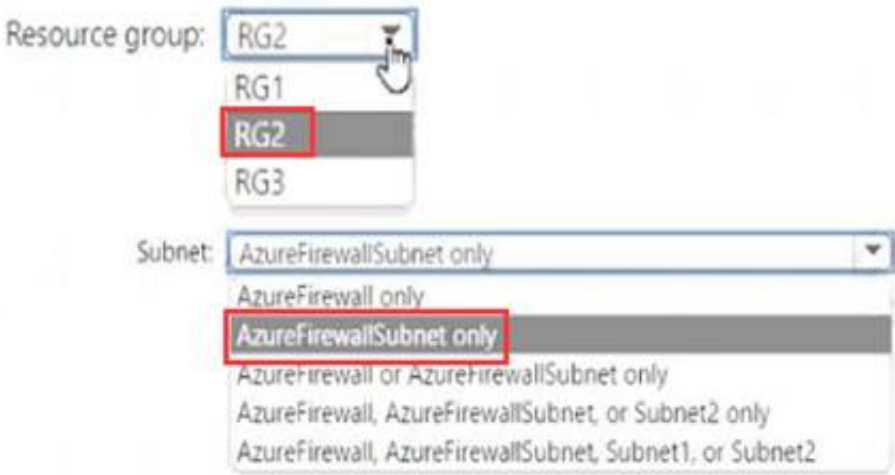


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



**NEW QUESTION 268**

- (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 271**

- (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 273**

- (Exam Topic 4)

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

Name	Operating system
Computer1	Windows 10
Computer2	Windows Server 2022
Computer3	SUSE Linux Enterprise Server (SLES)

You need to enable file integrity monitoring in Microsoft Defender for Cloud. Which computers will support file integrity monitoring?

- A. Computer1 only
- B. Computer 1 and Computer2 only
- C. Computer1 and Computer3 only
- D. Computer1, Computer2, and Computer3

Answer: B

#### NEW QUESTION 278

- (Exam Topic 4)

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

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

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

NOTE: Each correct selection is worth one point

SKUs

Basic

VpnGw1

VpnGw2

VpnGw3

Answer Area

VNET1:

SKU

VNET2:

SKU

- A. Mastered
- B. Not Mastered

Answer: A

#### Explanation:

References:

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

#### NEW QUESTION 279

- (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 284

- (Exam Topic 4)

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

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

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

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

**Answer: C**

**Explanation:**

Note: Create a workspace

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

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

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

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

**NEW QUESTION 289**

- (Exam Topic 4)

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

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

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

NOTE: Each correct selection is worth one point.

Total number of Security Center email notifications about an RDP

brute force attack on Tuesday:

▼

☐ 1
 ☐ 2
 ☐ 3
 ☐ 4

Total number of Security Center email notifications on Tuesday:

▼

☐ 3
 ☐ 4
 ☐ 6
 ☐ 9
 ☐ 11

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Reference:

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

### NEW QUESTION 292

- (Exam Topic 4)

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

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

You have an Azure subscription named Sub1.

You have an Azure Storage account named sa1 in a resource group named RG1.

Users and applications access the blob service and the file service in sa1 by using several shared access signatures (SASs) and stored access policies.

You discover that unauthorized users accessed both the file service and the blob service. You need to revoke all access to sa1.

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

A. Yes

B. No

**Answer: A**

### Explanation:

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

### NEW QUESTION 294

- (Exam Topic 4)

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

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

What should you do?

A. From Azure CLI run the Get-AzOperationalInsightsworkspace cmdlet.

B. From the Azure SQL Database query editor, create a Transact-SQL query.

C. From the Azure Sentinel workspace, create a Kusto Query Language query.

D. From Microsoft SQL Server Management Studio (SSMS), create a Transact-SQL query.

**Answer: C**

### NEW QUESTION 298

- (Exam Topic 4)

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

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

Name	Scoped to
Role1	MG1
Role2	RG1

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

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

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

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

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

Name	Role
User1	Role1
User2	Role1, Role2
User3	Role2

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

Answer Area

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

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 303

- (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 federation with Active Directory Federation Services (AD FS). Does the solution meet the goal?

- A. Yes  
B. No

Answer: B

Explanation:

A federated authentication system relies on an external trusted system to authenticate users. Some companies want to reuse their existing federated system investment with their Azure AD hybrid identity solution. The maintenance and management of the federated system falls outside the control of Azure AD. It's up to the organization by using the federated system to make sure it's deployed securely and can handle the authentication load.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta>

NEW QUESTION 305

- (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 310

- (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 312

- (Exam Topic 4)

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

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

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

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

**Answer:** C

### NEW QUESTION 316

- (Exam Topic 4)

Lab Task

Task 4

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

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

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

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

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

### NEW QUESTION 318

- (Exam Topic 4)

You have an Azure subscription named Sub1.

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

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

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

**Answer:** D

**Explanation:**

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

References:

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

**NEW QUESTION 319**

- (Exam Topic 4)

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

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

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

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

**Answer:** A

**Explanation:**

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

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

**NEW QUESTION 324**

- (Exam Topic 4)

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

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

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

**Answer:** D

**Explanation:**

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

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

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

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

Reference:

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

**NEW QUESTION 326**

- (Exam Topic 4)

You have an Azure subscription that contains an Azure SQL database named SQL1 and an Azure key vault named KeyVault1. KeyVault1 stores the keys shown in the following table.

Name	Type	RSA key size	Elliptic curve name
Key1	RSA	2048	Not applicable
Key2	RSA	3072	Not applicable
Key3	RSA	4096	Not applicable
Key4	EC	Not applicable	P-512

You need to configure Transparent Data Encryption (TDE). TDE will use a customer-managed key for SQL1?

- A. Key1. Key2 Key3. and Key4
- B. Key1 only
- C. Key2 only
- D. Key1 and key2 only
- E. Key2 and Key3 only

**Answer:** E

**NEW QUESTION 328**

- (Exam Topic 4)

You have an Azure subscription that contains an Azure Blob storage account bolb1. You need to configure attribute-based access control (ABAC) for blob1.

Which attributes can you use in access conditions?

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

Answer: A

NEW QUESTION 331

- (Exam Topic 4)

You have an Azure AD tenant that contains 500 users and an administrative unit named AU1. From the Azure Active Directory admin center, you plan to add the users to AU1 by using Bulk add members. You need to create and upload a file for the bulk add. What should you include in the file?

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

Answer: E

NEW QUESTION 334

- (Exam Topic 4)

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

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

Answer: DE

Explanation:

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

NEW QUESTION 338

- (Exam Topic 3)

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

Container registries:

0

1

2

3

Workspaces:

0

1

2

3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 341

- (Exam Topic 2)

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 346

- (Exam Topic 2)  
You need to meet the technical requirements for VNetwork1. What should you do first?

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

Answer: A

Explanation:

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

NEW QUESTION 350

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

Answer Area			
Statements		Yes	No
From VM1, you can successfully ping the public IP address of VM2.		<input type="radio"/>	<input type="radio"/>
From VM1, you can successfully ping the private IP address of VM3.		<input type="radio"/>	<input type="radio"/>
From VM1, you can successfully ping the public IP address of VM5.		<input type="radio"/>	<input type="radio"/>

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Yes, Yes No

**NEW QUESTION 353**

- (Exam Topic 2)

You are evaluating the effect of the application security groups on the network communication between the virtual machines in Sub2.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
From VM1, you can successfully ping the private IP address of VM4.	<input type="radio"/>	<input type="radio"/>
From VM2, you can successfully ping the private IP address of VM4.	<input type="radio"/>	<input type="radio"/>
From VM1, you can connect to the web server on VM4.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: No. VM4 is in Subnet13 which has NSG3 attached to it.

VM1 is in ASG1. NSG3 would only allow ICMP pings from ASG2 but not ASG1. Only TCP traffic is allowed from ASG1.

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

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

Box 2: Yes.

VM2 is in ASG2. Any protocol is allowed from ASG2 so ICMP ping would be allowed.

Box3. VM1 is in ASG1. TCP traffic is allowed from ASG1 so VM1 could connect to the web server as connections to the web server would be on ports TCP 80 or TCP 443.

**NEW QUESTION 355**

- (Exam Topic 1)

You need to configure WebApp1 to meet the data and application requirements.

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

NOTE: Each correct selection is worth one point.

- A. Upload a public certificate.  
B. Turn on the HTTPS Only protocol setting.  
C. Set the Minimum TLS Version protocol setting to 1.2.  
D. Change the pricing tier of the App Service plan.  
E. Turn on the Incoming client certificates protocol setting.

**Answer:** BE

**Explanation:**

Refer <https://docs.microsoft.com/en-us/azure/app-service/app-service-web-configure-tls-mutual-auth>

**NEW QUESTION 358**

- (Exam Topic 1)

You need to deploy Microsoft Antimalware to meet the platform protection requirements. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Create a custom policy definition that has effect set to:

▼

Append

Deny

DeployIfNotExists

Create a policy assignment and modify:

▼

The Create a Managed Identify setting

The exclusion settings

The scope

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Create a custom policy definition that has effect set to:

▼

Append

Deny

DeployIfNotExists

Create a policy assignment and modify:

▼

The Create a Managed Identify setting

The exclusion settings

The scope

**NEW QUESTION 360**

.....

## Relate Links

**100% Pass Your az-500 Exam with Examible Prep Materials**

<https://www.examible.com/az-500-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.examible.com/>