

## az-500 Dumps

### Microsoft Azure Security Technologies

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



### NEW QUESTION 1

- (Exam Topic 4)

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

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

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

- An Azure Sentinel workspace
- An Azure Event Grid instance

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

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

NOTE: Each correct selection is worth one point.

Subscription1:

An Azure Log Analytics agent on a Linux virtual machine
A Data Factory pipeline
An Event Hubs namespace
An Azure Service Bus queue

Subscription2:

A new Azure Log Analytics workspace
A new Azure Sentinel data connector
A new Azure Sentinel playbook
A new Event Grid resource provider

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

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

### NEW QUESTION 2

- (Exam Topic 4)

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

Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Enabled
User2	Group1	Disabled
User3	Group1	Disabled

You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings: ➤ Assignments: Include Group1, exclude Group2

- Conditions: Sign-in risk level: Medium and above
- Access Allow access, Require multi-factor authentication

You need to identify what occurs when the users sign in to Azure AD.

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

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

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

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

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

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

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

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

References:

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

**NEW QUESTION 3**

- (Exam Topic 4)

You have an Azure 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 4**

- (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 5**

- (Exam Topic 4)

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

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

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

**Answer:** B

**Explanation:**

Reference:

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

**NEW QUESTION 6**

- (Exam Topic 4)

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

Name	Type
User1	Azure Active Directory (Azure AD) user
User2	Azure Active Directory (Azure AD) user
Group1	Azure Active Directory (Azure AD) group
Vault1	Azure key vault

User1 is a member of Group1. Group1 and User2 are assigned the Key Vault Contributor role for Vault1.  
On January 1, 2019, you create a secret in Vault1. The secret is configured as shown in the exhibit. (Click the Exhibit tab.)

### Create a secret

#### Upload options

Manual

\* Name ⓘ

Password1

\* Value

• • • • • • • • • •

Content type (optional)

Set activation date? ⓘ ☒

Activation Date

2019-03-01 12:00:00 AM

(UTC+02:00) --- Current Time Zone ---

Set expiration Date? ⓘ ☒

Expiration Date

2020-03-01 12:00:00 AM

(UTC+02:00) --- Current Time Zone ---

Enabled?

Yes

No

User2 is assigned an access policy to Vault1. The policy has the following configurations:

- > Key Management Operations: Get, List, and Restore
- > Cryptographic Operations: Decrypt and Unwrap Key
- > Secret Management Operations: Get, List, and Restore

Group1 is assigned an access to Vault1. The policy has the following configurations:

- > Key Management Operations: Get and Recover
- > Secret Management Operations: List, Backup, and Recover

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

#### Statements

Yes

No

On January 1, 2019, User1 can view the value of Password1.

☐
☐

On June 1, 2019, User2 can view the value of Password1.

☐
☐

On June 1, 2019, User1 can view the value of Password1.

☐
☐

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



Statements	Yes	No
On January 1, 2019, User1 can view the value of Password1.	<input type="radio"/>	<input checked="" type="radio"/>
On June 1, 2019, User2 can view the value of Password1.	<input checked="" type="radio"/>	<input type="radio"/>
On June 1, 2019, User1 can view the value of Password1.	<input type="radio"/>	<input checked="" type="radio"/>

#### NEW QUESTION 7

- (Exam Topic 4)

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

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

NOTE: Each correct selection is worth one point.

Configure App1 to authenticate by using a:

Key

Certificate

Passphrase

User-assigned managed identity

System-assigned managed identity

Configure a Key Vault reference for App1 from the:

Extensions blade

General settings tab

TLS/SSL settings blade

Application settings tab

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Reference:

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

#### NEW QUESTION 8

- (Exam Topic 4)

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

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

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

**Answer:** C

#### Explanation:

Reference:

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

#### NEW QUESTION 9

- (Exam Topic 4)

You have an Azure Container Registry named Registry1.

You add role assignment for Registry1 as shown in the following table.

User	Role
User1	AcrPush
User2	AcrPull
User3	AcrImageSigner
User4	Contributor

Which users can upload images to Registry1 and download images from Registry1? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

Upload images: ▼

User1 only
User1 and User4 only
User1, User3, and User4
User1, User2, User3, and User4

Download images: ▼

User2 only
User1 and User2 only
User2 ad User4 only
User1, User2, and User4
User1, User2, User3, and User4

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: User1 and User4 only  
Owner, Contributor and AcrPush can push images. Box 2: User1, User2, and User4  
All, except AcrImageSigner, can download/pull images.

Role/Permission	Access Resource Manager	Create/delete registry	Push image	Pull image	Delete image data	Change policies	Sign images
Owner	X	X	X	X	X	X	
Contributor	X	X	X	X	X	X	
Reader	X			X			
AcrPush			X	X			
AcrPull				X			
AcrDelete					X		
AcrImageSigner							X

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

**NEW QUESTION 10**

- (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 10**

- (Exam Topic 4)

You have an Azure environment.

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

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

**Answer:** C

**Explanation:**

Reference:

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

#### NEW QUESTION 14

- (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 16

- (Exam Topic 4)

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

SQL1 has the following settings:

- Auditing: On
- Audit log destination: storage1

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

**Answer Area**

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

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

#### NEW QUESTION 21

- (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 23**

- (Exam Topic 4)  
You have an Azure Sentinel workspace that has the following data connectors:

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

You need to ensure that data is being ingested from each connector.  
From the Logs query window, which table should you query for each connector? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

Azure Active Directory Identity Protection:

AzureDiagnostics

CommonSecurityLog

SecurityAlert

SecurityEvent

Syslog

Azure Firewall:

AzureDiagnostics

CommonSecurityLog

SecurityAlert

SecurityEvent

Syslog

CEF:

AzureDiagnostics

CommonSecurityLog

SecurityAlert

SecurityEvent

Syslog

- A. Mastered
- B. Not Mastered

Answer: A

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

**NEW QUESTION 28**

- (Exam Topic 4)  
You have an app that uses an Azure SQL database.  
You need to be notified if a SQL injection attack is launched against the database. What should you do?

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

Answer: C

**NEW QUESTION 33**

- (Exam Topic 4)  
You have an Azure subscription.  
You plan to create a custom role-based access control (RBAC) role that will provide permission to read the Azure Storage account.  
Which property of the RBAC role definition should you configure?

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

Answer: D



**Explanation:**

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

Reference:

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

**NEW QUESTION 34**

- (Exam Topic 4)

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

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

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

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

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

A. Yes

B. No

**Answer: B**

**NEW QUESTION 39**

- (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 40**

- (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 43**

- (Exam Topic 4)

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

You plan to assign policies that use the DeployIfNotExist, AuditIfNotExist, Append, and Deny effects.

Which effect requires a managed identity for the assignment?

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

**Answer:** C

**Explanation:**

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

References:

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

**NEW QUESTION 46**

- (Exam Topic 4)

Your company has an Azure subscription named Sub1 that is associated to an Azure Active Directory Azure (Azure AD) tenant named contoso.com. The company develops a mobile application named App1. App1 uses the OAuth 2 implicit grant type to acquire Azure AD access tokens. You need to register App1 in Azure AD.

What information should you obtain from the developer to register the application?

- A. a redirect URI
- B. a reply URL
- C. a key
- D. an application ID

**Answer:** A

**Explanation:**

For Native Applications you need to provide a Redirect URI, which Azure AD will use to return token responses. References:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/v1-protocols-oauth-code>

**NEW QUESTION 51**

- (Exam Topic 4)

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

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

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

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

**Answer:** D

**NEW QUESTION 53**

- (Exam Topic 4)

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

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

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

**Answer:** B

**Explanation:**

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

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

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

➤ Monitoring the state of your virtual machines.

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

**NEW QUESTION 55**

- (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 56**

- (Exam Topic 4)

Lab Task

Task 6

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

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

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

**NEW QUESTION 59**

- (Exam Topic 4)

You are troubleshooting a security issue for an Azure Storage account.

You enable the diagnostic logs for the storage account. What should you use to retrieve the diagnostics logs?

- A. the Security & Compliance admin center
- B. SQL query editor in Azure
- C. File Explorer in Windows
- D. AzCopy

**Answer:** D

**Explanation:**

References:

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

**NEW QUESTION 62**

- (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	Yes	No
When User1 signs in, the user is assigned the Password Administrator role automatically.	<input type="radio"/>	<input type="radio"/>
User2 can request to activate the Password Administrator role.	<input type="radio"/>	<input type="radio"/>
If User3 wants to activate the Password Administrator role, the user can approve their own request.	<input type="radio"/>	<input type="radio"/>

- 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 64**

- (Exam Topic 4)

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

Name	Operating system
VM1	Windows Server 2016
VM2	Ubuntu Server 18.04 LTS

From Azure Security Center, you turn on Auto Provisioning. You deploy the virtual machines shown in the following table.

Name	Operating system
VM3	Windows Server 2016
VM4	Ubuntu Server 18.04 LTS

On which virtual machines is the Log Analytics agent installed?

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

**Answer:** D

**Explanation:**

When automatic provisioning is On, Security Center provisions the Log Analytics Agent on all supported Azure VMs and any new ones that are created.

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

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection>

**NEW QUESTION 67**

- (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 70**

- (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 72**

- (Exam Topic 4)

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

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

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

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

**Answer:** C

**Explanation:**

Reference:

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

**NEW QUESTION 77**

- (Exam Topic 4)

You have an Azure subscription name Sub1 that contains an Azure Policy definition named Policy1. Policy1 has the following settings:

- Definition location: Tenant Root Group
- Category: Monitoring

You need to ensure that resources that are noncompliant with Policy1 are listed in the Azure Security Center dashboard.

What should you do first?

- A. Change the Category of Policy1 to Security Center.
- B. Add Policy1 to a custom initiative.
- C. Change the Definition location of Policy1 to Sub1.
- D. Assign Policy1 to Sub1.

**Answer:** D

**Explanation:**

Reference:

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

**NEW QUESTION 82**

- (Exam Topic 4)

You have an Azure subscription that contains an Azure SQL database named sql1. You plan to audit sql1.

You need to configure the audit log destination. The solution must meet the following requirements:

- Support querying events by using the Kusto query language.
- Minimize administrative effort. What should you configure?

- A. an event hub
- B. a storage account
- C. a Log Analytics workspace

**Answer:** C

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/tutorial-log-analytics-wizard>

**NEW QUESTION 87**

- (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 90**

- (Exam Topic 4)

Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD). Azure AD Connect is installed on a domain member server named Server1.

You need to ensure that a domain administrator for the adatum.com domain can modify the synchronization options. The solution must use the principle of least privilege.

Which Azure AD role should you assign to the domain administrator?

- A. Security administrator
- B. Global administrator
- C. User administrator

**Answer:** B

**Explanation:**

Reference:

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

#### NEW QUESTION 91

- (Exam Topic 4)

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

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

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

**Answer: B**

#### Explanation:

Adaptive application control is an intelligent, automated end-to-end application whitelisting solution from Azure Security Center. It helps you control which applications can run on your Azure and non-Azure VMs (Windows and Linux), which, among other benefits, helps harden your VMs against malware. Security Center uses machine learning to analyze the applications running on your VMs and helps you apply the specific whitelisting rules using this intelligence.

Reference:

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

#### NEW QUESTION 95

- (Exam Topic 4)

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

An administrator named Admin1 has access to the following identities:

- An OpenID-enabled user account
- A Hotmail account
- An account in contoso.com
- An account in an Azure AD tenant named fabrikam.com

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

- A. contoso.com only
- B. contoso.com, fabrikam.com, and Hotmail only
- C. contoso.com and fabrikam.com only
- D. contoso.com, fabrikam.com, Hotmail, and OpenID-enabled user account

**Answer: C**

#### Explanation:

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

Reference:

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

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

#### NEW QUESTION 96

- (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 101**

- (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**

The Leader of IT Certification

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

**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 106**

- (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 110**

- (Exam Topic 4)

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

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

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

Variable1:

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

Variable2:

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

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

**NEW QUESTION 113**

- (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 117

- (Exam Topic 4)

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

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 121

- (Exam Topic 4)

You are collecting events from Azure virtual machines to an Azure Log Analytics workspace. You plan to create alerts based on the collected events. You need to identify which Azure services can be used to create the alerts.

Which two services should you identify? Each correct answer presents a complete solution NOTE: Each correct selection is worth one point.

- A. Azure Monitor
- B. Azure Security Center
- C. Azure Analytics Services
- D. Azure Sentinel
- E. Azure Advisor

Answer: AD

Explanation:

<https://docs.microsoft.com/en-us/azure/analysis-services/analysis-services-overview>

NEW QUESTION 123

- (Exam Topic 4)

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



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

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

Answer Area

Monitored storage5 services:

Protected storage accounts:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Monitored storage5 services:

Protected storage accounts:

NEW QUESTION 127

- (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 130

- (Exam Topic 4)  
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.  
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 134**

- (Exam Topic 4)

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

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

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

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

**Answer:** A

**Explanation:**

Reference:

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

**NEW QUESTION 138**

- (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 139**

- (Exam Topic 4)

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

Name	Type	Region	Resource group
Sa1	Azure Storage account	East US	RG1
VM1	Azure virtual machine	East US	RG2
KV1	Azure key vault	East US 2	RG1
SQL1	Azure SQL database	East US 2	RG2

You need to ensure that you can provide VM1 with secure access to a database on SQL1 by using a contained database user. What should you do?

- A. Enable a managed service identity on VM1.
- B. Create a secret in KV1.
- C. Configure a service endpoint on SQL1.
- D. Create a key in KV1.

**Answer:** B

**Explanation:**

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

**NEW QUESTION 140**

- (Exam Topic 4)

You have a network security group (NSG) bound to an Azure subnet.

You run Get-AzureRmNetworkSecurityRuleConfig and receive the output shown in the following exhibit.

Name	:	DenyStorageAccess
Description	:	
Protocol	:	*
SourcePortRange	:	{*}
DestinationPortRange	:	{*}
SourceAddressPrefix	:	{*}
DestinationAddressPrefix	:	{Storage}
SourceApplicationSecurityGroups	:	[]
DestinationApplicationSecurityGroups	:	[]
Access	:	Deny
Priority	:	105
Direction	:	Outbound
Name	:	StorageEA2Allow
ProvisionIngState	:	Succeeded
Description	:	
Protocol	:	*
SourcePortRange	:	{*}
DestinationPortRange	:	{443}
SourceAddressPrefix	:	{*}
DestinationAddressPrefix	:	{Storage/EastUS2}
SourceApplicationSecurityGroups	:	[]
DestinationApplicationSecurityGroups	:	[]
Access	:	Allow
Priority	:	104
Direction	:	Outbound
Name	:	Contoso_FTP
Description	:	
Protocol	:	TCP
SourcePortRange	:	{*}
DestinationPortRange	:	{21}
SourceAddressPrefix	:	{1.2.3.4/32}
DestinationAddressPrefix	:	{10.0.0.5/32}
SourceApplicationSecurityGroups	:	[]
DestinationApplicationSecurityGroups	:	[]
Access	:	Allow
Priority	:	504
Direction	:	Inbound

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

Traffic destined for an Azure Storage account is [answer choice].

able to connect to East US

able to connect to East US 2

able to connect to West Europe

prevented from connecting to all regions

FTP connections from 1.2.3.4 to 10.0.0.10/32 are [answer choice].

allowed

dropped

forwarded

- A. Mastered
- B. Not Mastered

Answer: A

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

NEW QUESTION 145

- (Exam Topic 4)  
You have an Azure subscription.  
You plan to implement Azure DDoS Protection. The solution must meet the following requirement:  
\* Provide access to DDoS rapid response support during active attacks.  
\* Project Basic SKU public IP addresses.  
You need to recommend which type of DDoS projection to use for each requirement.  
What should you recommend? To answer, drag the appropriate DDoS projection types to the correct requirements. Each DDoS Projection type may be used once, or not at all. You may need to drag the split bar between panes or scroll to view connect.  
NOTE: Each correct selection is worth one point.



DDoS Protection types

DDoS infrastructure protection

DDoS IP Protection

DDoS Network Protection

Answer Area

Provide access to DDoS rapid response support during active attacks:

Protect Basic SKU public IP addresses:

A. Mastered

B. Not Mastered

**Answer:** A

**Explanation:**

DDoS Protection types

DDoS infrastructure protection

DDoS IP Protection

DDoS Network Protection

Answer Area

Provide access to DDoS rapid response support during active attacks:

DDoS Network Protection

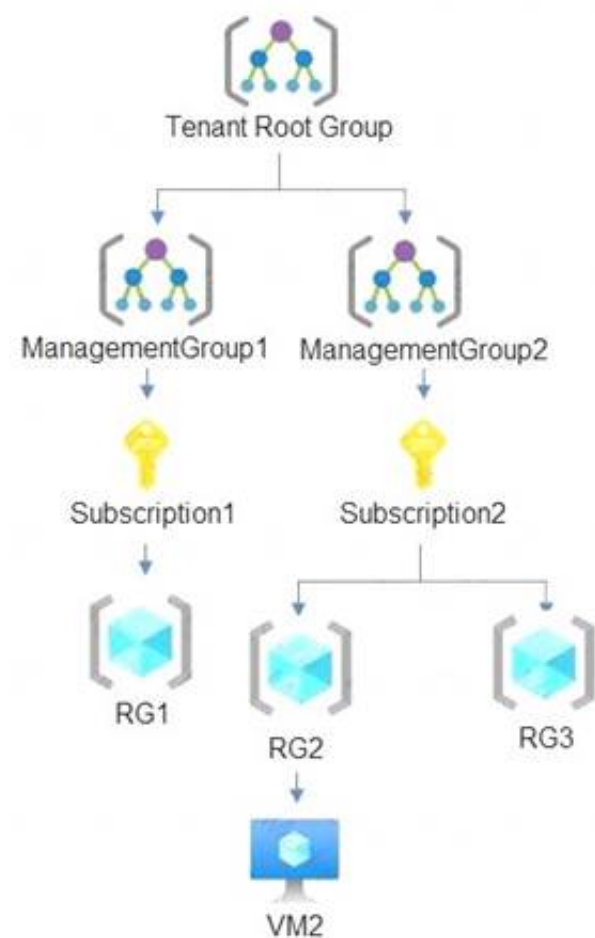
Protect Basic SKU public IP addresses:

DDoS IP Protection

#### NEW QUESTION 149

- (Exam Topic 4)

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



RG1, RG2, and RG3 are resource groups. RG2 contains a virtual machine named VM1.

You assign role-based access control (RBAC) roles to the users shown in the following table.

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

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

NOTE: Each correct selection is worth one point.



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

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 154

- (Exam Topic 4)

You have an Azure subscription that contains an Azure key vault named ContosoKey1. You create users and assign them roles as shown in the following table.

Name	Subscription role assignment	ContosoKey1 role assignment
User1	Owner	None
User2	Security Admin	None
User3	None	User Access Administrator
User4	None	Key Vault Contributor

You need to identify which users can perform the following actions:

- > Delegate permissions for ContososKey1.
- > Configure network access to ContosoKey1.

Which users should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Delegate permissions for ContosoKey1:

User1 only  
User1 and User2 only  
User1 and User3 only  
User1 and User4 only  
User1, User2, and User3 only  
User1, User2, User3, and User4

Configure network access to ContosoKey1:

User1 only  
User1 and User2 only  
User1 and User3 only  
User1 and User4 only  
User1, User2, and User3 only  
User1, User2, User3, and User4

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-gb/azure/key-vault/general/rbac-guide>

NEW QUESTION 155

- (Exam Topic 4)

You have an Azure subscription that contains the following resources:

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

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

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

NOTE: Each correct selection is worth one point.

Components	Answer Area
A data connector for Security Center	Enable alert notifications from Security Center: Component
A data connector for the firewall software	Create an incident: Component
A playbook	Initiate a script to configure the firewall rule: Component
A rule	
A Security Events connector	
A workbook	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

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

**NEW QUESTION 159**

- (Exam Topic 4)

Lab Task

use the following login credentials as needed:

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

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

Azure Password: GpOAe4@IDg

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

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

Task 7

You need to collect all the audit failure data from the security log of a virtual machine named VM1 to an Azure Storage account. To complete this task, sign in to the Azure portal.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

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

**NEW QUESTION 162**

- (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 166**

- (Exam Topic 4)

You onboard Azure Sentinel. You connect Azure Sentinel to Azure Security Center.  
You need to automate the mitigation of incidents in Azure Sentinel. The solution must minimize administrative effort.  
What should you create?

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

**Answer: B**

**NEW QUESTION 167**

- (Exam Topic 4)

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

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

Which section of the dashboard should you review?

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

**Answer: C**

**NEW QUESTION 169**

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that contains a group named Group1. You need to ensure that the members of Group1 sign in by using passwordless authentication. What should you do?

- A. Configure the Microsoft Authenticator authentication method policy.  
B. Configure the certificate-based authentication (CBA) policy.  
C. Configure the sign-in risk policy.  
D. Create a Conditional Access policy.

**Answer: A**

**NEW QUESTION 173**

- (Exam Topic 4)

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

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

User2 is the owner of Group2.  
The user and group settings for App1 are configured as shown in the following exhibit.

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

Allow users to request access to this application? ⓘ

Yes No

To which group should assigned users be added? ☐

Select group

Group2

Require approval before granting access to this application? ⓘ

Yes No

Who is allowed to approve access to this application? 

Select approvers  
1 users selected

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

User3 is configured to approve access to Appl.

You need to identify the owners of Group2 and the users of Appl.

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

NOTE: Each correct selection is worth one point.

App1 users:

- A. Mastered  
B. Not Mastered

**Answer: A**

**Explanation:**

Reference:

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

**NEW QUESTION 177**

- (Exam Topic 4)

You have an Azure subscription that has a managed identity named identity and is linked to an Azure Active Directory (Azure AD) tenant. The tenant contains the resources shown in the following table.

Which resources can be added to AU1 and AU2? To answer, select the appropriate options in the answer area.



Name	Type	Assigned object
AU1	Administrative unit	User1, Group1
AU2	Administrative unit	None
User1	User	Not applicable
Group1	Security group	Not applicable
Group2	Microsoft 365 group	Not applicable

Which resources can be added to AU1 and AU2? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

AU1:

AU2 only

Group2 only

Identity1 only

AU2 and Group2 only

Group2 and Identity1 only

AU2:

Identity1 only

AU1 and Identity1 only

Group1 and Group2 only

AU1, Group2 and Identity1 only

Group1, Group2 and User1 only

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

AU1:

AU2 only

Group2 only

Identity1 only

AU2 and Group2 only

Group2 and Identity1 only

AU2:

Identity1 only

AU1 and Identity1 only

Group1 and Group2 only

AU1, Group2 and Identity1 only

Group1, Group2 and User1 only

NEW QUESTION 182

- (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 185

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

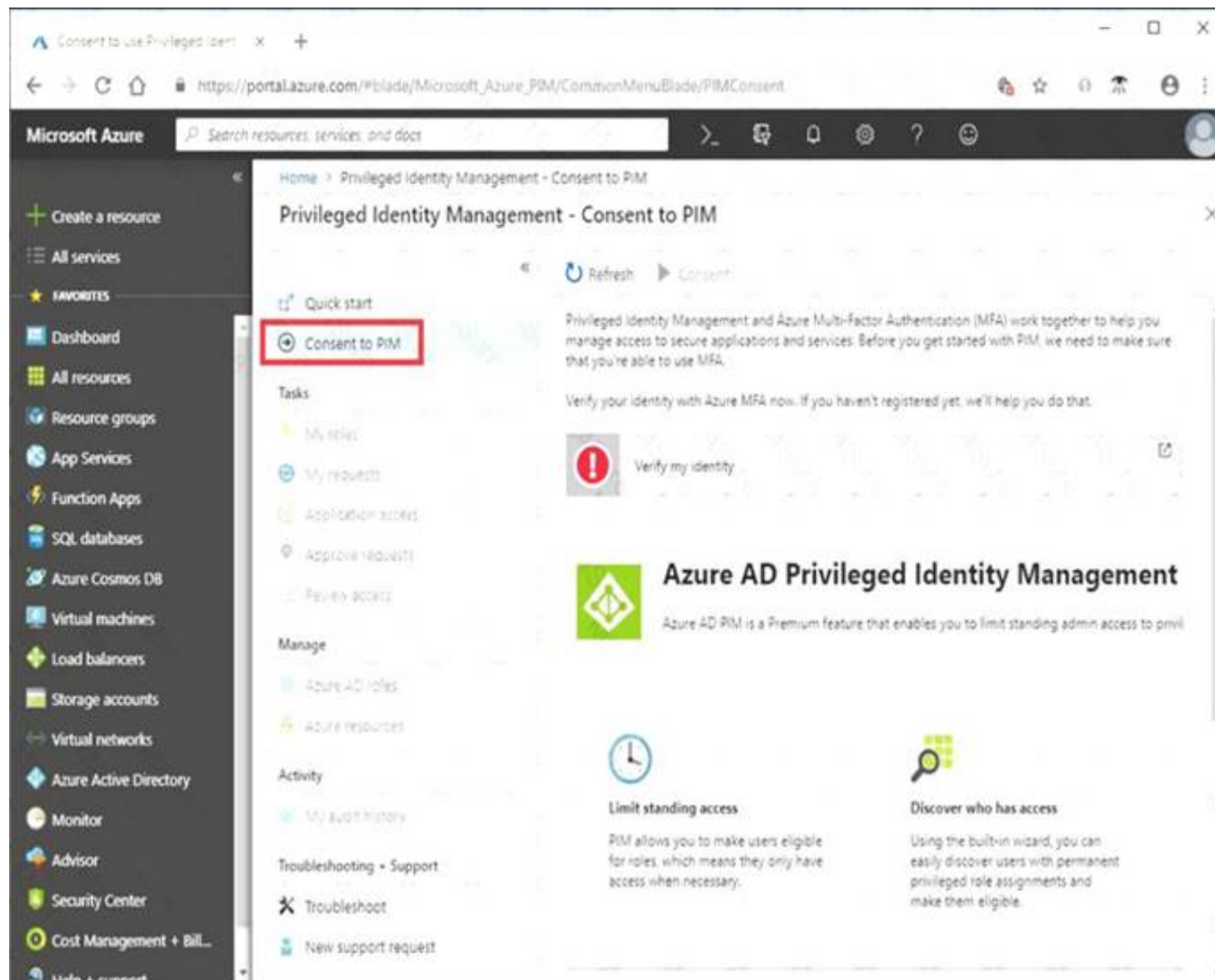
Actions	Answer Area
Verify your identity by using multi-factor authentication (MFA).	
Consent to PIM.	
Sign up PIM for Azure AD roles.	
Discover privileged roles.	
Discover resources.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Step 1: Consent to PIM



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

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

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

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

#### NEW QUESTION 190

- (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	Answer Area
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.	

- 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 195

- (Exam Topic 4)

You have Azure virtual machines that have Update Management enabled. The virtual machines are configured as shown in the following table.

Name	Operating system	Region	Resource group
VM1	Windows Server 2012	East US	RG1
VM2	Windows Server 2012 R2	West US	RG1
VM3	Windows Server 2016	West US	RG2
VM4	Ubuntu Server 18.04 LTS	West US	RG2
VM5	Red Hat Enterprise Linux 7.4	East US	RG1
VM6	CentOS 7.5	East US	RG1

You schedule two update deployments named Update1 and Update2. Update1 updates VM3. Update2 updates VM6.

Which additional virtual machines can be updated by using Update1 and Update2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Update1:

VM2 only  
VM4 only  
VM1 and VM2 only  
VM1, VM2, VM4, VM5, and VM6

Update2:

VM5 only  
VM1 and VM5 only  
VM4 and VM5 only  
VM1, VM2, and VM5 only  
VM1, VM2, VM3, VM4, and VM5

- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

Update1: VM1 and VM2 only

VM3: Windows Server 2016 West US RG2 Update2: VM4 and VM5 only

VM6: CentOS 7.5 East US RG1

For Linux, the machine must have access to an update repository. The update repository can be private or public.

References:

<https://docs.microsoft.com/en-us/azure/automation/automation-update-management>

#### NEW QUESTION 197

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that contains two administrative units named AU1 and AU2.

Users are assigned to the administrative units as shown in the following table.

User name	Member of
Admin1	AU1
Admin2	AU1
Admin3	AU2
Admin4	AU2
User1	AU1



Answer Area

Statements	Yes	No
Admin1 can reset the password of User1.	<input type="radio"/>	<input type="radio"/>
Admin2 can reset the password of User3.	<input type="radio"/>	<input type="radio"/>
Admin3 can reset the password of Admin4.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Admin1 can reset the password of User1.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can reset the password of User3.	<input checked="" type="radio"/>	<input type="radio"/>
Admin3 can reset the password of Admin4.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 198

- (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 plan to implement an application that will consist of the resources shown in the following table.

Name	Type	Description
CosmosDBAccount1	Azure Cosmos DB account	A Cosmos DB account containing a database Named CosmosDB1 that serves as a back-end tier of the application
WebApp1	Azure web app	A web app configured to serve as the middle tier of the application

Users will authenticate by using their Azure AD user account and access the Cosmos DB account by using resource tokens.

You need to identify which tasks will be implemented in CosmosDB1 and WebApp1.

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

NOTE: Each correct selection is worth one point.

CosmosDB1:

- ☒ Authenticate Azure AD users and generate resource tokens.
- ☒ Authenticate Azure AD users and relay resource tokens.
- ☐ Create database users and generate resource tokens.

WebApp1:

- ☒ Authenticate Azure AD users and generate resource tokens.
- ☒ Authenticate Azure AD users and relay resource tokens.
- ☐ Create database users and generate resource tokens.

- A. Mastered  
B. Not Mastered

Answer: A

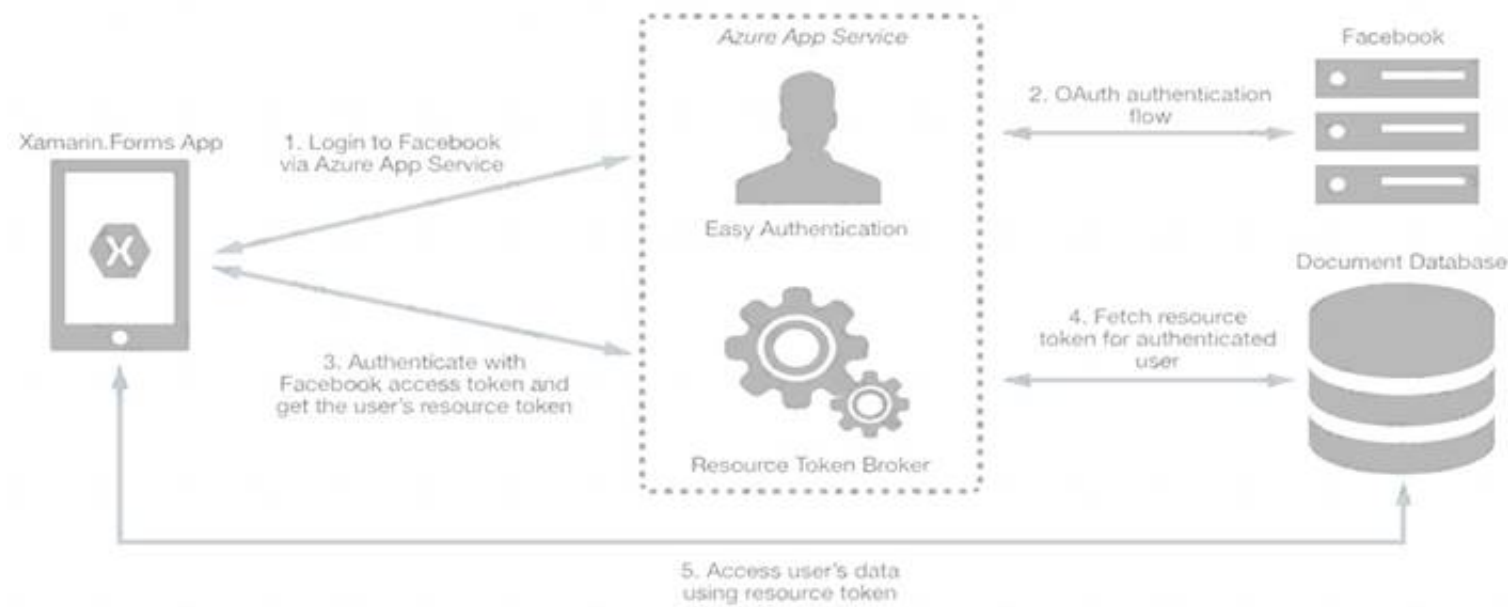
Explanation:

CosmosDB1: Create database users and generate resource tokens.

Azure Cosmos DB resource tokens provide a safe mechanism for allowing clients to read, write, and delete specific resources in an Azure Cosmos DB account according to the granted permissions.

WebApp1: Authenticate Azure AD users and relay resource tokens

A typical approach to requesting, generating, and delivering resource tokens to a mobile application is to use a resource token broker. The following diagram shows a high-level overview of how the sample application uses a resource token broker to manage access to the document database data:



References:

<https://docs.microsoft.com/en-us/xamarin/xamarin-forms/data-cloud/cosmosdb/authentication>

#### NEW QUESTION 200

- (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 203

- (Exam Topic 4)

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

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

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

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

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

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

**Answer: C**

#### Explanation:

An NSG needs to be enabled, either at the VM level or the subnet level. Reference:

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

#### NEW QUESTION 205

- (Exam Topic 4)

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

Name	Resource group
storage1	RG1
storage2	RG1
storage3	RG2

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

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

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

\* The storage3 account must be exclude from the Defender for Storage protections.  
 Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and then in the correct order.

Actions

For storage3, disable the customer-managed keys.

Disable Defender for Storage for storage3.

Enable the Defender for Storage plan for Sub1.

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

Enable the Defender for Storage plan for RG1.

>

<

Answer Area

1

2

3

>

<

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

For storage3, disable the customer-managed keys.

Disable Defender for Storage for storage3.

Enable the Defender for Storage plan for Sub1.

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

Enable the Defender for Storage plan for RG1.

>

<

Answer Area

1 Enable the Defender for Storage plan for Sub1.

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

3 Enable the Defender for Storage plan for RG1.

>

<

NEW QUESTION 206

- (Exam Topic 4)  
 You have an Azure Container Registry named ContReg1 that contains a container image named image1. You enable content trust for ContReg1. After content trust is enabled, you push two images to ContReg1 as shown in the following table.

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

Which images are trusted images?

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

Answer: B

Explanation:

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

NEW QUESTION 211

- (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 6  
 You need to email an alert to a user named admin1@contoso.com if the average CPU usage of a virtual machine named VM1 is greater than 70 percent for a period of 15 minutes.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To email an alert to a user named admin1@contoso.com if the average CPU usage of a virtual machine named VM1 is greater than 70 percent for a period of 15 minutes, you can follow these steps:

- > In the Azure portal, search for and select the virtual machine named VM1.
- >



- In the left pane, select Alerts.
- Select New alert rule.
  - In the New alert rule pane, enter the following information:
  - Name: Enter a name for the alert rule.
  - Description: Enter a description for the alert rule.
  - Condition: Select Metric measurement.
  - Resource: Select the virtual machine named VM1.
  - Metric: Select Percentage CPU.
  - Operator: Select Greater than.
  - Threshold: Enter 70.
  - Aggregation type: Select Average.
  - Period: Select 15 minutes.
  - In the Actions pane, select Add action group.
  - In the Add action group pane, enter the following information:
  - Name: Enter a name for the action group.
  - Short name: Enter a short name for the action group.
  - Email recipient: Enter the email address of the user you want to receive the alert. For example, adminl@contoso.com.
  - Select OK.

**NEW QUESTION 216**

- (Exam Topic 4)

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

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

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

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

NOTE: Each correct selection is worth one point.

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

**Answer:** AC

**Explanation:**

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

**NEW QUESTION 219**

- (Exam Topic 4)

You have an Azure web app named webapp1.

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

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

**Answer:** B

**Explanation:**

To use Azure Repos, make sure your Azure DevOps organization is linked to your Azure subscription. Reference:

<https://docs.microsoft.com/en-us/azure/app-service/deploy-continuous-deployment>

**NEW QUESTION 223**

- (Exam Topic 4)

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

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

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

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

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

**Answer:** AC



**NEW QUESTION 225**

- (Exam Topic 4)

You have an Azure environment.

You need to identify any Azure configurations and workloads that are non-compliant with ISO 27001:2013 standards.

What should you use?

- A. Azure Active Directory (Azure AD) Identity Protection
- B. Microsoft Defender for Cloud
- C. Microsoft Defender for Identity
- D. Microsoft Sentinel

**Answer:** B

**NEW QUESTION 227**

- (Exam Topic 4)

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

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

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

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

What should you do?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 228**

- (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 230**

- (Exam Topic 4)

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

Name	Pattern	Case sensitivity
Condition1	White	On
Condition2	Black	Off

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

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

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

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

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

▼

No label
Label1 only
Label2 only
Label1 and Label2

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

▼

No label
Label1 only
Label2 only
Label1 and Label2

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Label 2 only

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

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

Box 2: No Label

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

References:

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

**NEW QUESTION 235**

- (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 236**

- (Exam Topic 4)

You have an Azure subscription that contains an Azure SQL server named SQL1. SQL1 contains. You need to use Microsoft Defender for Cloud to complete a vulnerability assessment for DB1. What should you do first?

- A. From Advanced Threat Protection types, select SQL injection vulnerability.
- B. Configure the Send scan report to setting.
- C. Set Periodic recurring scans to ON.
- D. Enable the Microsoft Defender for SQL plan.

**Answer:** A

#### NEW QUESTION 240

- (Exam Topic 4)

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

Name	Virtual network	Location
Subnet11	VNet1	West US
Subnet12	VNet1	West US
Subnet21	VNet2	West US

The subscription contains Azure web app named WebApp1 that has the following configurations.

- \* Region West Us
- \* Virtual network VNet1
- \* VNet integration on: Enabled
- \* Outbound subnet: Subnet11
- \* Windows plan (West US): ASP1

You plan to deploy an Azure web app named WebApp2 that will have the following settings:

- \* Region: West US
- \* VNet integration on-Enabled
- \* Windows plan (West UAS): WebApp2?

To which subnets can you integrate WebApp2?

- A. Subnet11 only
- B. Subnet2 only
- C. Subnet11 or subnet12 only
- D. Subnet2 or Subnet21 only
- E. Subnet11, subnet2, or Subnet21

**Answer:** C

#### NEW QUESTION 244

- (Exam Topic 4)

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

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

Each user is assigned an Azure AD Premium P2 license.

You plan to onboard and configure Azure AD identity Protection.

Which users can onboard Azure AD Identity Protection, remediate users, and configure policies? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

**Answer Area**

Users who can onboard Azure AD Identity Protection:

- ☐ User1 only
- ☐ User1 and User2 only
- ☐ User1, User 2, and User3 only
- ☐ User1, User 2, User3, and User 4 only

Users who can remediate users and configure policies:

- ☐ User1 and User2 only
- ☐ User1 and User3 only
- ☐ User1, User 2, and User3 only
- ☐ User1, User 2, User3, and User 4

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area

Users who can onboard Azure AD Identity Protection:

☐ User1 only  
☐ User1 and User2 only  
☐ User1, User 2, and User3 only  
☐ User1, User 2, User3, and User 4 only

Users who can remediate users and configure policies:

☐ User1 and User2 only  
☐ User1 and User3 only  
☐ User1, User 2, and User3 only  
☐ User1, User 2, User3, and User 4

**NEW QUESTION 249**

- (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 253**

- (Exam Topic 4)

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

Name	Connected to	Private IP address	Public IP address
VM1	VNET1/Subnet1	10.1.1.5	20.224.219.170
VM2	VNET1/Subnet2	10.1.2.5	20.224.219.230
VM3	VNET2/Subnet1	10.11.1.5	40.122.155.212

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

Allow access from

☐ All networks
 ☒ Selected networks

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

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Yes, Yes, No

**NEW QUESTION 254**

- (Exam Topic 4)

You have an Azure subscription that uses Microsoft Defender for Cloud.



You have an Amazon Web Services (AWS) account.

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

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

**Answer:** A

#### NEW QUESTION 257

- (Exam Topic 4)

Lab Task

Task 1

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

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

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

- \* 1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET1. Alternatively, browse to Virtual Networks in the left navigation pane.
- \* 2. In the properties of VNET1, click on Subnets. This will display the subnets in VNET1 and the Network Security Group associated to each subnet. Note the name of the Network Security Group associated to Subnet0.
- \* 3. Type Network Security Groups into the search box and select the Network Security Group associated with Subnet0.
- \* 4. In the properties of the Network Security Group, click on Inbound Security Rules.
- \* 5. Click the Add button to add a new rule.
- \* 6. In the Source field, select Service Tag.
- \* 7. In the Source Service Tag field, select Internet.
- \* 8. Leave the Source port ranges and Destination field as the default values (\* and All).
- \* 9. In the Destination port ranges field, enter 7777.
- \* 10. Change the Protocol to TCP.
- \* 11. Leave the Action option as Allow.
- \* 12. Change the Priority to 100.
- \* 13. Change the Name from the default Port\_8080 to something more descriptive such as Allow\_TCP\_7777\_from\_Internet. The name cannot contain spaces.
- \* 14. Click the Add button to save the new rule.

#### NEW QUESTION 261

- (Exam Topic 4)

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

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

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

What should you use to construct the resource ID?

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 262

- (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 1

You need to configure Azure to allow RDP connections from the Internet to a virtual machine named VM1. The solution must minimize the attack surface of VM1.

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

To configure Azure to allow RDP connections from the Internet to a virtual machine named VM1, you can follow the steps below:

- Create a new inbound security rule in the network security group (NSG) that is associated with the virtual network subnet that contains VM1. The rule should allow RDP traffic from the Internet to the virtual network subnet. You can use the Azure portal, Azure PowerShell, or Azure CLI to create the rule.
  - Configure the network security group (NSG) to associate it with the virtual network subnet that contains VM1.
  - Configure the virtual machine to allow RDP traffic. You can use the Azure portal, Azure PowerShell, or Azure CLI to configure the virtual machine.
- To minimize the attack surface of VM1, you can use the following best practices:
- Use a strong password for the local administrator account on the virtual machine.
  - Use Network Security Groups (NSGs) to restrict traffic to only the necessary ports and protocols.
  - Use Azure Security Center to monitor and protect your virtual machines.

#### NEW QUESTION 264

- (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 266

- (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 268

- (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 270

- (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:

	▼
Analytics	
Data connectors	
Playbooks	
Workbooks	

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

	▼
Analytics	
Data connectors	
Playbooks	
Workbooks	

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

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 274

- (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 277**

- (Exam Topic 4) You have an Azure subscription. You plan to create a storage account. You need to use customer-managed keys to encrypt the tables in the storage account.

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

**Cmdlets**

**Answer Area**

New-AzStorageAccountKey		
New-AzStorageTable	➤	⬆
Register-AzProviderFeature		
New-AzStorageAccount	⬅	⬇
Register-AzResourceProvider		

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Text, table Description automatically generated with medium confidence

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-configure-key-vault?tabs=pow>

**NEW QUESTION 279**

- (Exam Topic 4)

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

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 282**

- (Exam Topic 4)

Lab Task

use the following login credentials as needed:

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

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

Azure Password: GpOAe4@IDg

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

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

Task 5

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

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

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

**NEW QUESTION 287**

- (Exam Topic 4)



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

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

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

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

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

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

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

Answer Area

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

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area

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

#### NEW QUESTION 289

- (Exam Topic 4)

You have an Azure subscription that contains a resource group named RG1 and a security group serverless RG1 contains 10 virtual machine, a virtual network VNET1, and a network security group (NSG) named NSG1. ServerAdmins can access the virtual machines by using RDP.

You need to ensure that NSG1 only RDP connections to the virtual for a maximum of 60 minutes when a member of ServerAdmins requests access.

What should you configure?

- A. an Azure Active Directory (Azure AD) Privileged identity Management (PIM) role assignment.  
B. a just in time (JIT) VM access policy in Azure Security Center  
C. an azure policy assigned to RG1.  
D. an Azure Bastion host on VNET1.

**Answer:** B

**Explanation:**

Reference:

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

#### NEW QUESTION 292

- (Exam Topic 4)

You have an Azure Sentinel workspace that has an Azure Active Directory (Azure AD) data connector. You are threat hunting suspicious traffic from a specific IP address.

You need to annotate an intermediate event stored in the workspace and be able to reference the IP address when navigating through the investigation graph.

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

Actions

Answer Area

Add the query to Favorites.

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

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

Add a bookmark and assign a tag.

Add a bookmark and map an entity.

From Azure Monitor, run an Azure Log Analytics query.

Select a query result.

<

>

↑

↓

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 293

- (Exam Topic 4)

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

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

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

NOTE: Each correct selection is worth one point.

Resource provider:

Microsoft.Authorization

Microsoft.Resources

Microsoft.Support

Assignable scope:

/

/Group1

/subscriptions/11111111-1234-1234-1111111111

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Text, application Description automatically generated

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

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

NEW QUESTION 297

- (Exam Topic 4)

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

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

You have an Azure Subscription named Sub1. Sub1 contains an Azure virtual machine named VM1 that runs Windows Server 2016.

You need to encrypt VM1 disks by using Azure Disk Encryption.

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

Actions	Answer Area
Configure secrets for the Azure key vault.	
Create an Azure key vault.	
Run Set-AzureRmStorageAccount.	
Configure access policies for the Azure key vault.	
Run Set-AzureRmVmDiskEncryptionExtension.	

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

References:

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

**NEW QUESTION 302**

- (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 304**

- (Exam Topic 4)

You have a Azure subscription.

You enable Azure Active Directory (Azure AD) Privileged identify (PIM).

Your company's security policy for administrator accounts has the following conditions:

- \* The accounts must use multi-factor authentication (MFA).

- \* The account must use 20-character complex passwords.
- \* The passwords must be changed every 180 days.
- \* The account must be managed by using PIM.

You receive alerts about administrator who have not changed their password during the last 90 days. You need to minimize the number of generated alerts. Which PIM alert should you modify?

- A. Roles don't require multi-factor authentication for activation.
- B. Administrator aren't using their privileged roles
- C. Roles are being assigned outside of Privileged identity Management
- D. Potential state accounts in a privileged role.

Answer: D

Explanation:

Reference:

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

NEW QUESTION 305

- (Exam Topic 4)

You have an Azure subscription named Sub1 that contains the resource groups shown in the following table.

Name	Location
RG1	West US
RG2	East US

You create the Azure Policy definition shown in the following exhibit.

```
{
  "mode": "All",
  "policyRule": {
    "if": {
      "anyOf": [
        {
          "field": "location",
          "notEquals": "[resourceGroup().location]"
        },
        {
          "field": "name",
          "notContains": "obj"
        }
      ]
    },
    "then": {
      "effect": "deny"
    }
  },
  "parameters": {}
}
```

You assign the policy to Sub1.

You plan to create the resources shown in the following table.

Name	Type	Location	Resource group
IPobject1	Public IP address	East US	RG2
obj1	Resource group	West US	Not applicable
OBJ3	Virtual network	West US	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.

Answer Area	Statements	Yes	No
	You can create IPobject1.	<input type="radio"/>	<input type="radio"/>
	You can create obj1.	<input type="radio"/>	<input type="radio"/>
	You can create OBJ3.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



**Answer Area**

Statements	Yes	No
You can create IPobject1.	<input type="radio"/>	<input checked="" type="radio"/>
You can create obj1.	<input type="radio"/>	<input checked="" type="radio"/>
You can create OBj3.	<input type="radio"/>	<input checked="" type="radio"/>

**NEW QUESTION 309**

- (Exam Topic 4)

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

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

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

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

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

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

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

NOTE: Each correct selection is worth one point.

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

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: No

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

Box 2: Yes

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

Box 3: No

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

**NEW QUESTION 312**

- (Exam Topic 4)

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

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

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

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

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

- A. Yes  
B. No

**Answer:** B

**Explanation:**

Instead use a management group.

Management groups in Microsoft Azure solve the problem of needing to impose governance policy on more than one Azure subscription simultaneously.

Reference:

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

**NEW QUESTION 313**

- (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 318**

- (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 323**

- (Exam Topic 4)

Lab Task

use the following login credentials as needed:

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

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

Azure Password: GpOAe4@IDg

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

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

Task 8

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

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

**NEW QUESTION 327**

- (Exam Topic 4)

You need to recommend which virtual machines to use to host App1. The solution must meet the technical requirements for KeyVault1. Which virtual machines should you use?

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

**Answer: D**

**NEW QUESTION 331**

- (Exam Topic 4)

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

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

**Answer Area**

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

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Answer Area



NEW QUESTION 332

- (Exam Topic 4)

You have an Azure subscription named Subscription1 that contains a resource group named RG1 and a user named User1. User1 is assigned the Owner role for RG1.

You create an Azure Blueprints definition named Blueprint1 that includes a resource group named RG2 as shown in the following exhibit.

Edit blueprint



You assign Blueprint1 to Subscription1 by using the following settings: ➤ Lock assignment: Read Only

➤ Managed Identity: System assigned

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
A locking mode of Read Only will be assigned to RG1.	<input type="radio"/>	<input type="radio"/>
User1 can add tags to RG2.	<input type="radio"/>	<input type="radio"/>
You can remove User1 from the Tag Contributor role for RG2.	<input type="radio"/>	<input type="radio"/>



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, text, application Description automatically generated

Reference:

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

**NEW QUESTION 336**

- (Exam Topic 4)

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

Name	Type
Key1	Key
Secret1	Secret
Cert1	Certificate

Which resources support the creation of a rotation policy?

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

**Answer:** C

**NEW QUESTION 340**

- (Exam Topic 4)

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

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

Each virtual machine has a single network interface.

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

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

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

**Answer:** D

**Explanation:**

Reference:

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

**NEW QUESTION 345**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

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

\* One year free update

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

\* Trusted by Millions

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

\* Shop Securely

All transactions are protected by VeriSign!

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

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