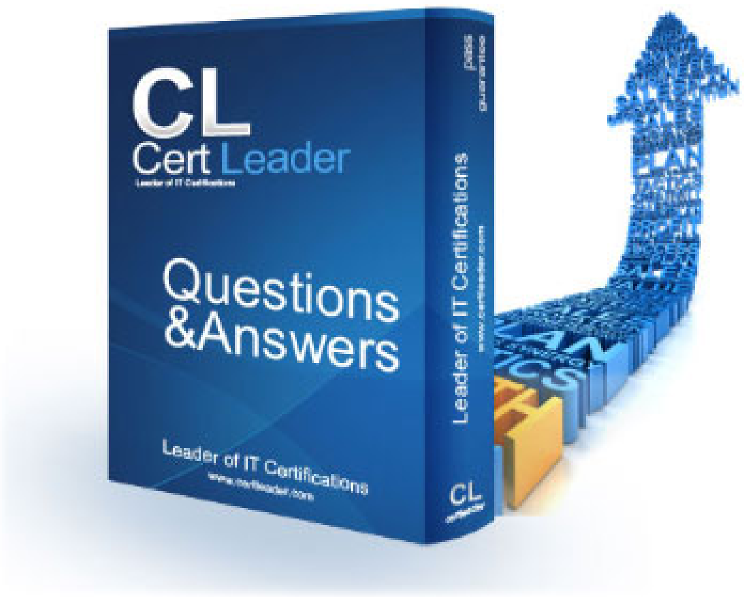
az-500 Dumps

Microsoft Azure Security Technologies

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



NEW QUESTION 1
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a hybrid configuration of Azure Active Directory (Azure AD). You have an Azure HDInsight cluster on a virtual network.
You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials. You need to configure the environment to support the planned authentication.
Solution: You deploy an Azure AD Application Proxy.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.
Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:

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

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

NEW QUESTION 2
- (Exam Topic 4)
You have Azure Resource Manager templates that you use to deploy Azure virtual machines.
You need to disable unused Windows features automatically as instances of the virtual machines are provisioned.
What should you use?

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

Answer: C

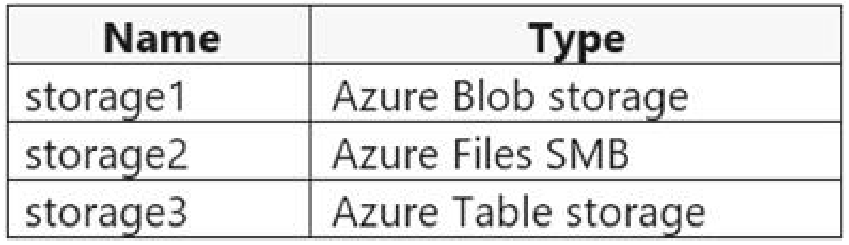
NEW QUESTION 3
- (Exam Topic 4)
Lab Task
Task 3
You need to ensure that a user named Danny-31330471 can sign in to any SQL database on a Microsoft SQL server named web31330471 by using SQL Server Management Studio (SSMS) and Azure AD credentials.

A. Mastered
B. Not Mastered

Answer: A

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

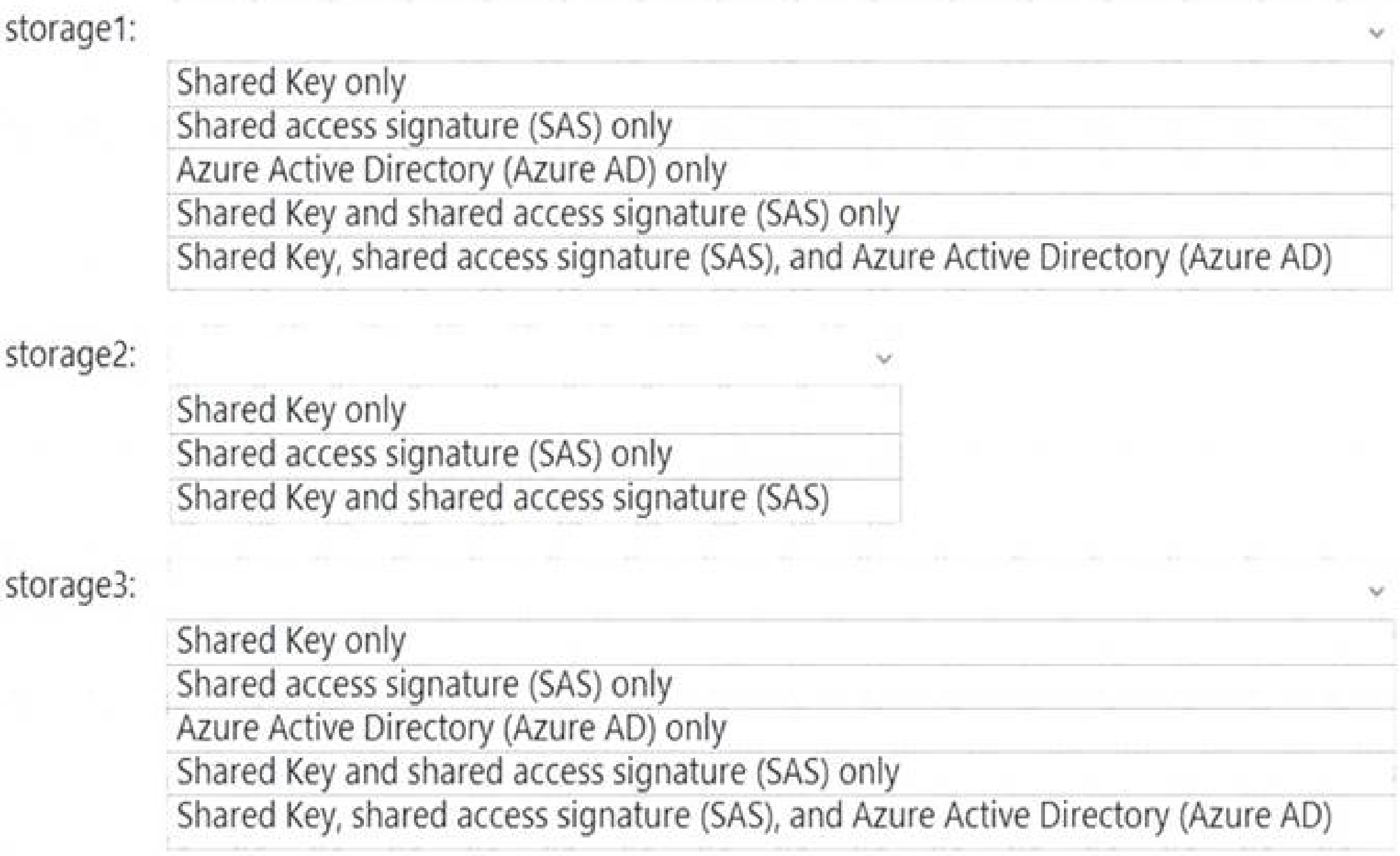
NEW QUESTION 4
- (Exam Topic 4)
You have an Azure subscription that contains the storage accounts shown in the following table.



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

You need to configure authorization access.

Which authorization types can you use for each storage account? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



storage1:
- Shared Key only
- Shared access signature (SAS) only
- Azure Active Directory (Azure AD) only
- Shared Key and shared access signature (SAS) only
- Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

storage2:
- Shared Key only
- Shared access signature (SAS) only
- Shared Key and shared access signature (SAS)

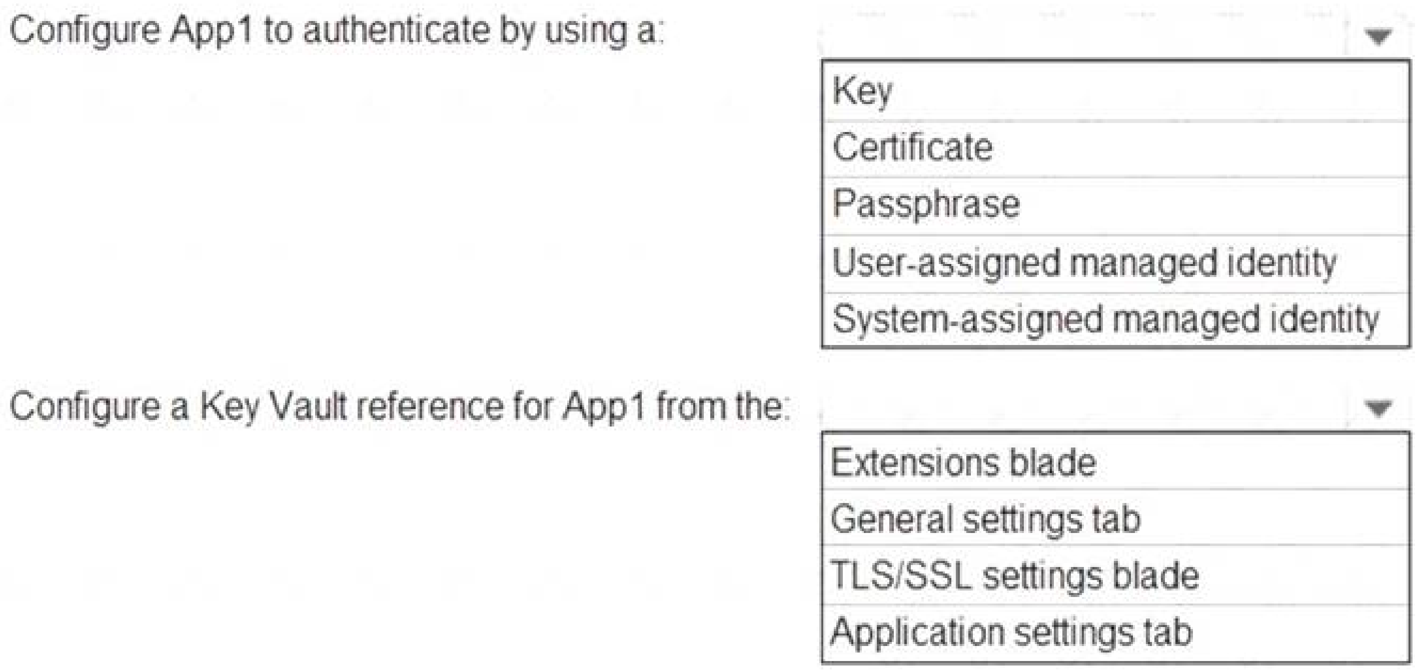
storage3:
- Shared Key only
- Shared access signature (SAS) only
- Azure Active Directory (Azure AD) only
- Shared Key and shared access signature (SAS) only
- Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application, email Description automatically generated
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/authorize-data-access

NEW QUESTION 5
- (Exam Topic 4)
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

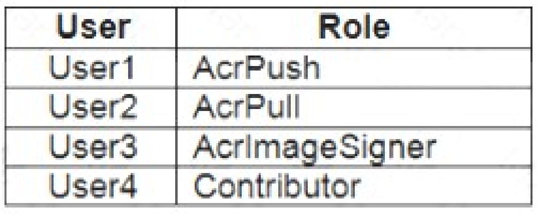
NEW QUESTION 6
- (Exam Topic 4)
You have 10 on-premises servers that run Windows Server 2019.
You plan to implement Azure Security Center vulnerability scanning for the servers. What should you install on the servers first?

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

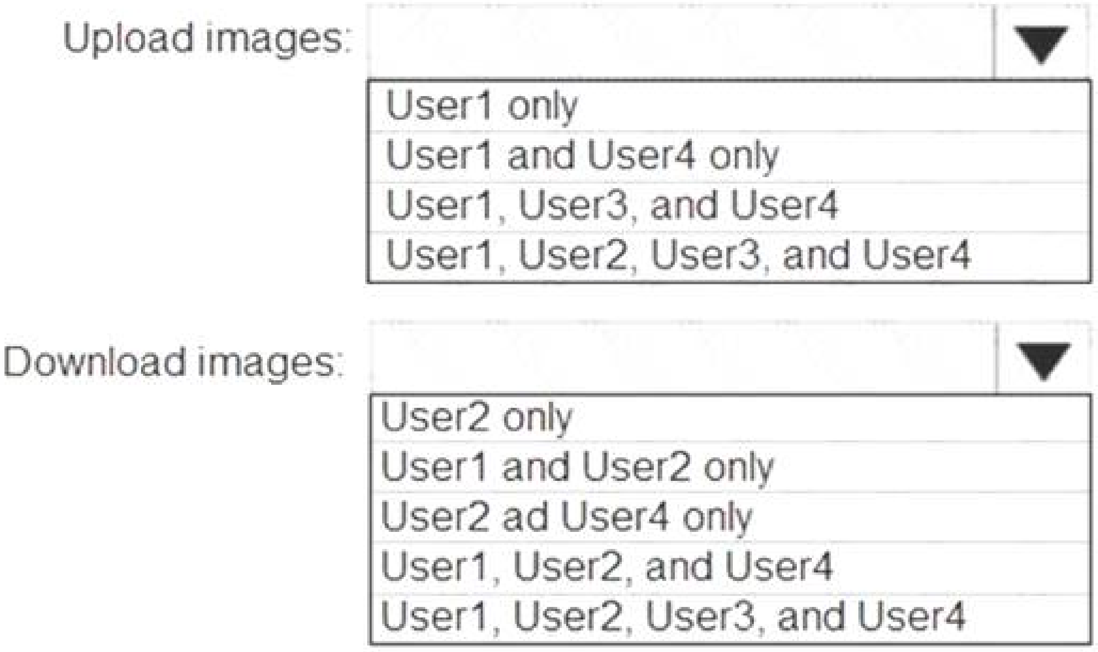
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/azure-arc/servers/agent-overview https://docs.microsoft.com/en-us/azure/security-center/deploy-vulnerability-assessment-vm

NEW QUESTION 7
- (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.



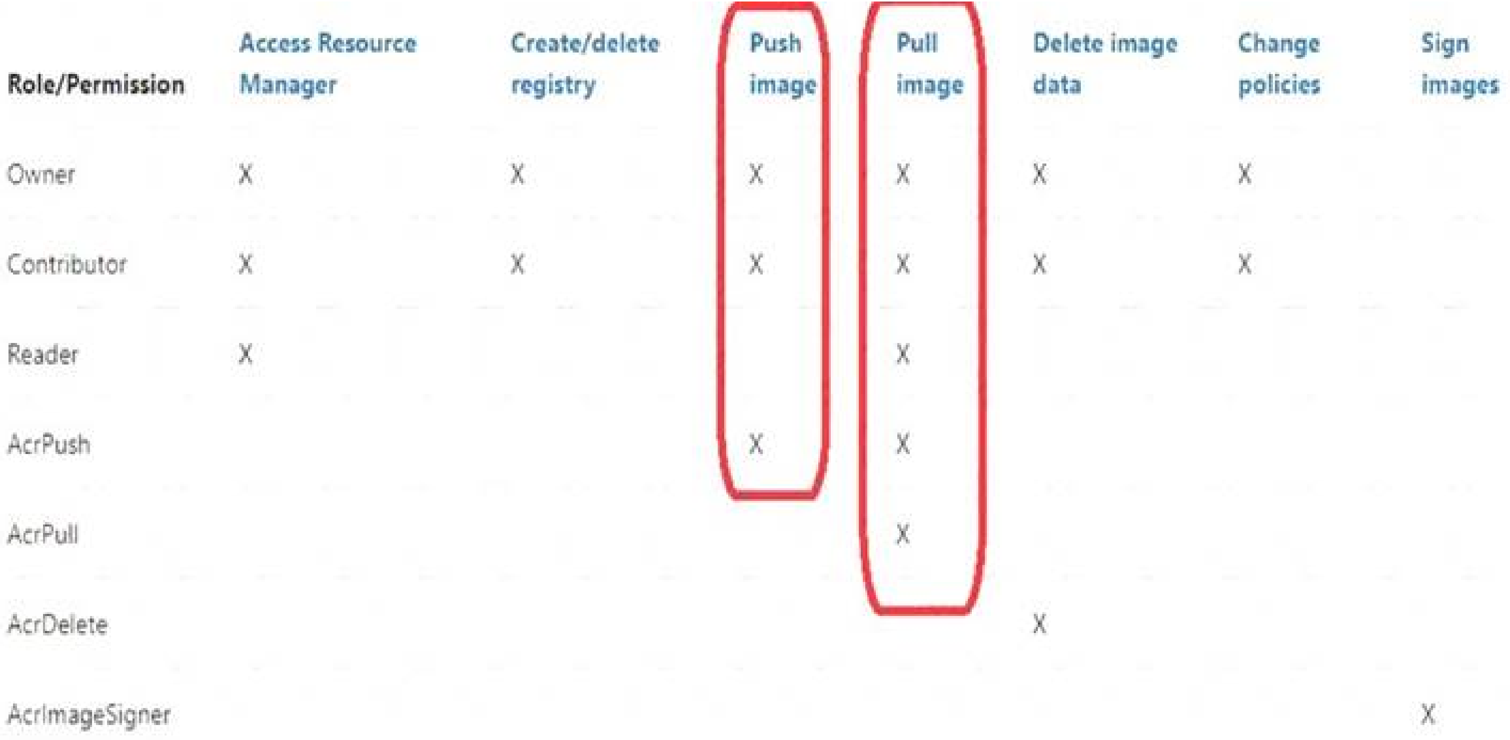
Upload images:
- User1 only
- User1 and User4 only
- User1, User3, and User4
- User1, User2, User3, and User4

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 AcrImagineSigner, 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 8
- (Exam Topic 4)
You have an Azure environment.
You need to identify any Azure configurations and workloads that are non-compliant with ISO 27001 standards. What should you use?

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

Answer: C

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

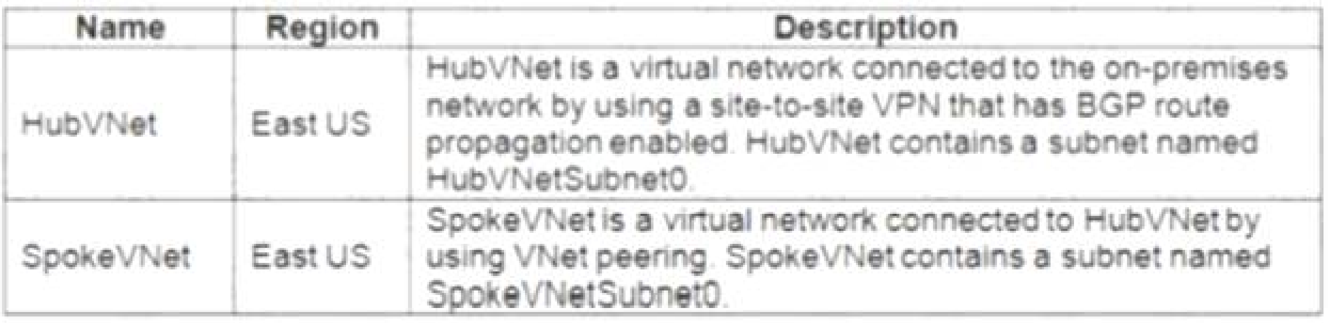
NEW QUESTION 9
- (Exam Topic 4)
You have an Azure Active Din-dory (Azure AD) tenant named contoso.com that contains a user named User1. You plan to publish several apps in the tenant.
You need to ensure that User1 can grant admin consent for the published apps.
Which two possible user roles can you assign to User! to achieve this goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

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

Answer: CE

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

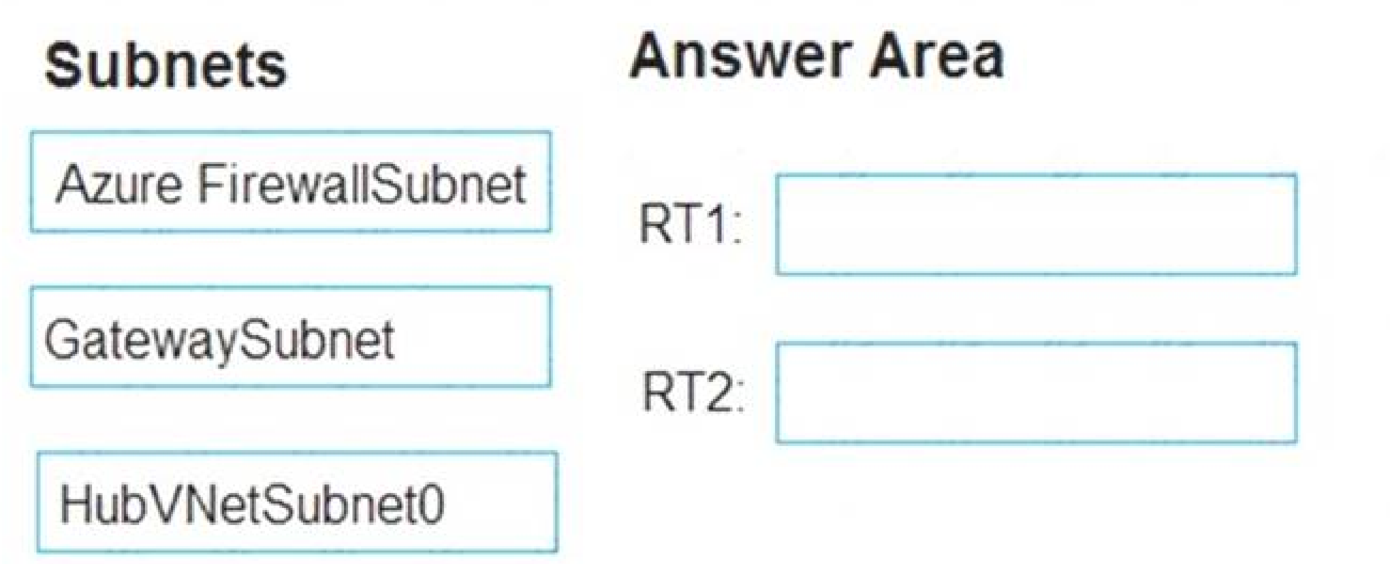
NEW QUESTION 10
- (Exam Topic 4)
You have an Azure subscription that contains the virtual networks shown in the following table.



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

The Azure virtual machines on SpokeVNetSubnet0 can communicate with the computers on the on-premises network.
You plan to deploy an Azure firewall to HubVNet. You create the following two routing tables:
- RT1: Includes a user-defined route that points to the private IP address of the Azure firewall as a next hop address
- RT2: Disables BGP route propagation and defines the private IP address of the Azure firewall as the default gateway

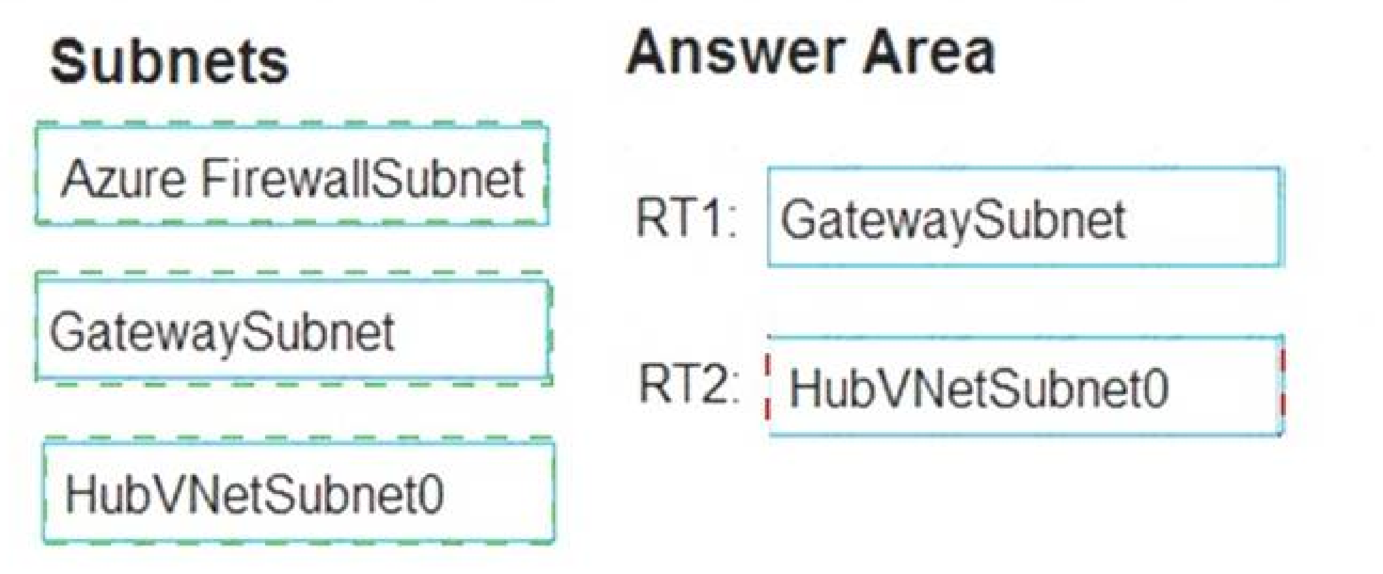
You need to ensure that traffic between SpokeVNetSubnet0 and the on-premises network flows through the Azure firewall.
To which subnet should you associate each route table? To answer, drag the appropriate subnets to the correct route tables. Each subnet may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



Subnets

Azure FirewallSubnet

GatewaySubnet

HubVNetSubnet0

Answer Area

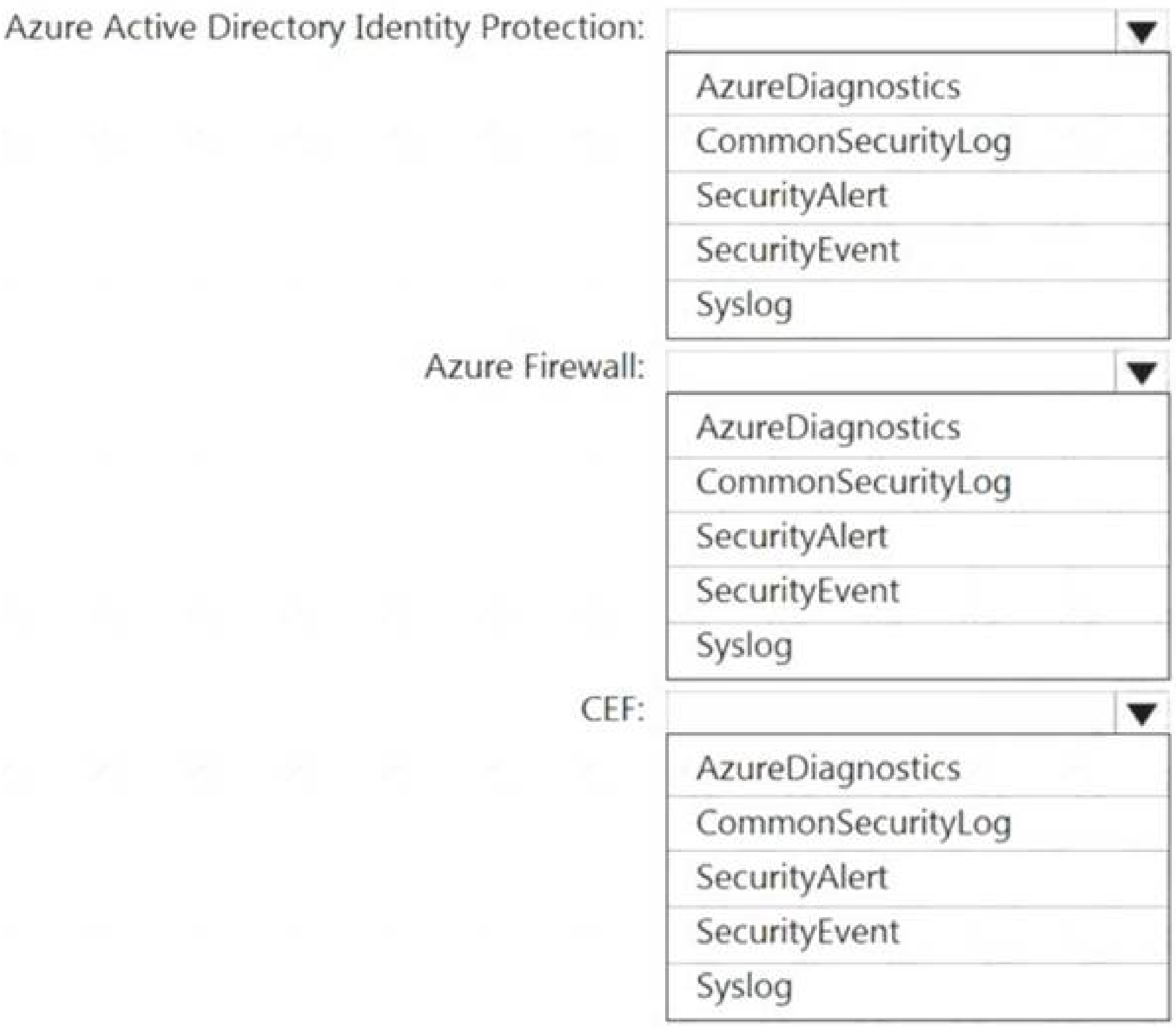
RT1: GatewaySubnet

RT2: HubVNetSubnet0

NEW QUESTION 10
- (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

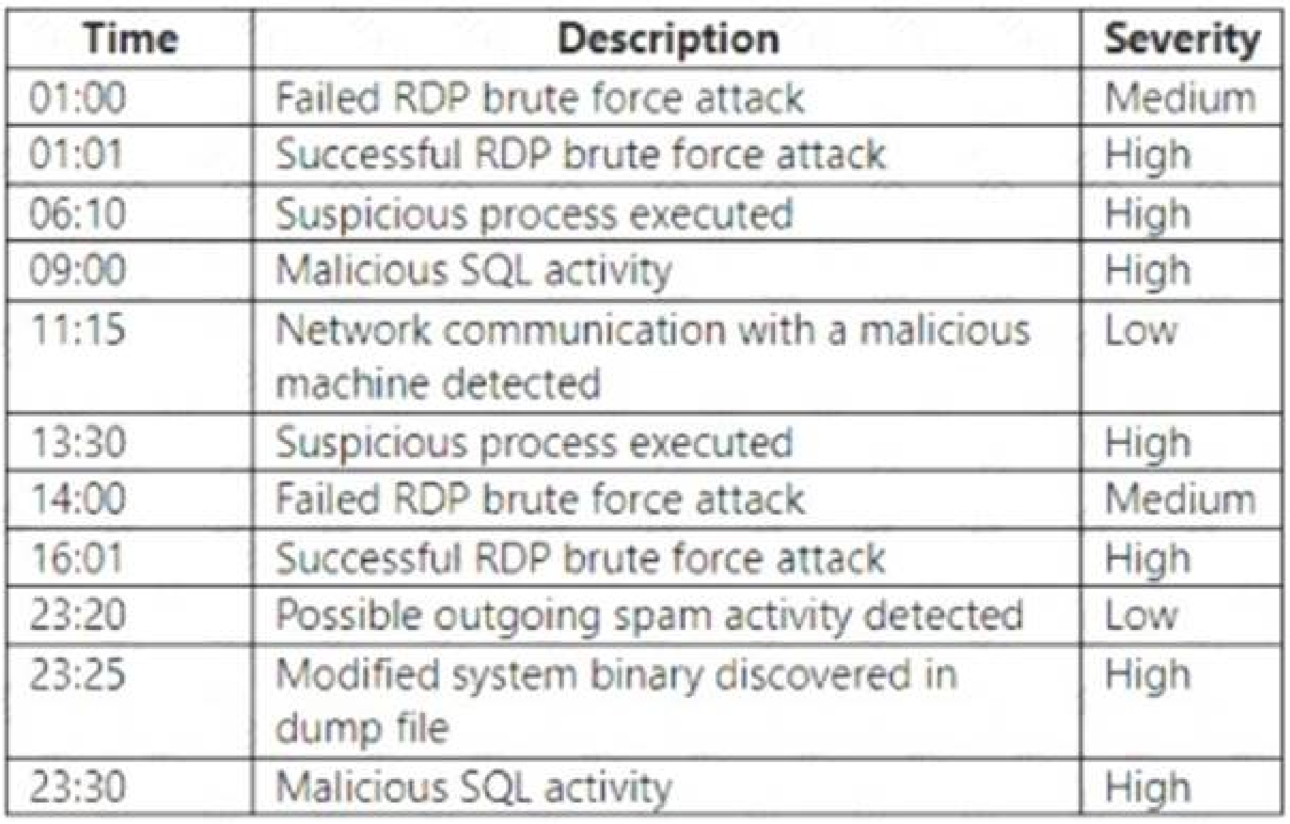
CEF: ▼
AzureDiagnostics
CommonSecurityLog
SecurityAlert
SecurityEvent
Syslog

A. Mastered
B. Not Mastered

Answer: A

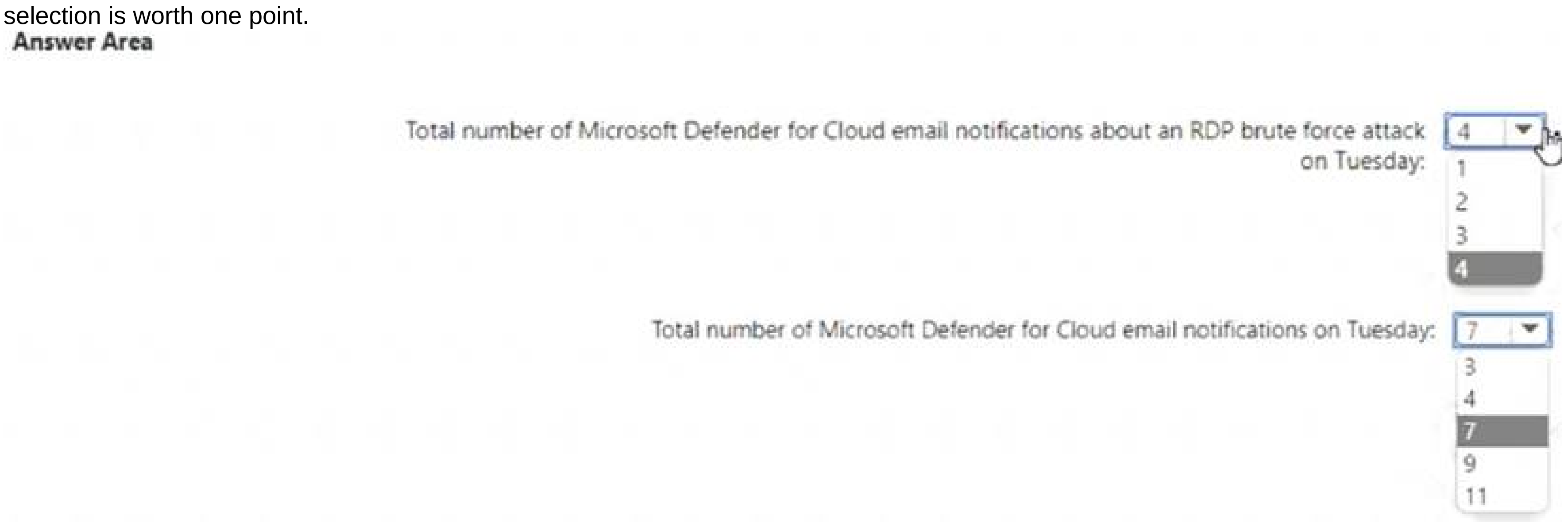
Explanation:
Graphical user interface, application, table Description automatically generated

NEW QUESTION 13
- (Exam Topic 4)
On Monday, you configure an email notification in Microsoft Defender for Cloud to notify user1
@contoso.com about alerts that have a severity level of Low, Medium, or High. On Tuesday, Microsoft Defender for Cloud generates the security alerts shown in the following table.



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

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



Answer Area

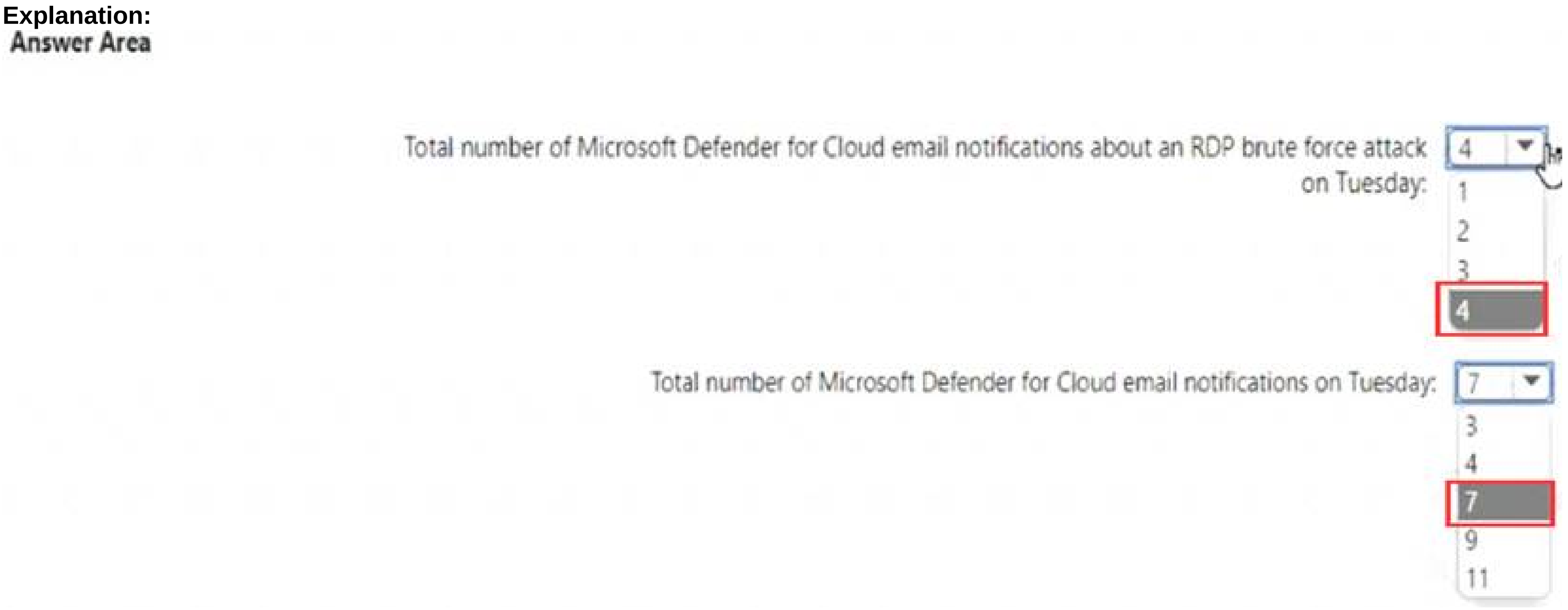
Total number of Microsoft Defender for Cloud email notifications about an RDP brute force attack on Tuesday: 4

Total number of Microsoft Defender for Cloud email notifications on Tuesday: 7

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Total number of Microsoft Defender for Cloud email notifications about an RDP brute force attack on Tuesday: 4

Total number of Microsoft Defender for Cloud email notifications on Tuesday: 7

NEW QUESTION 15
- (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

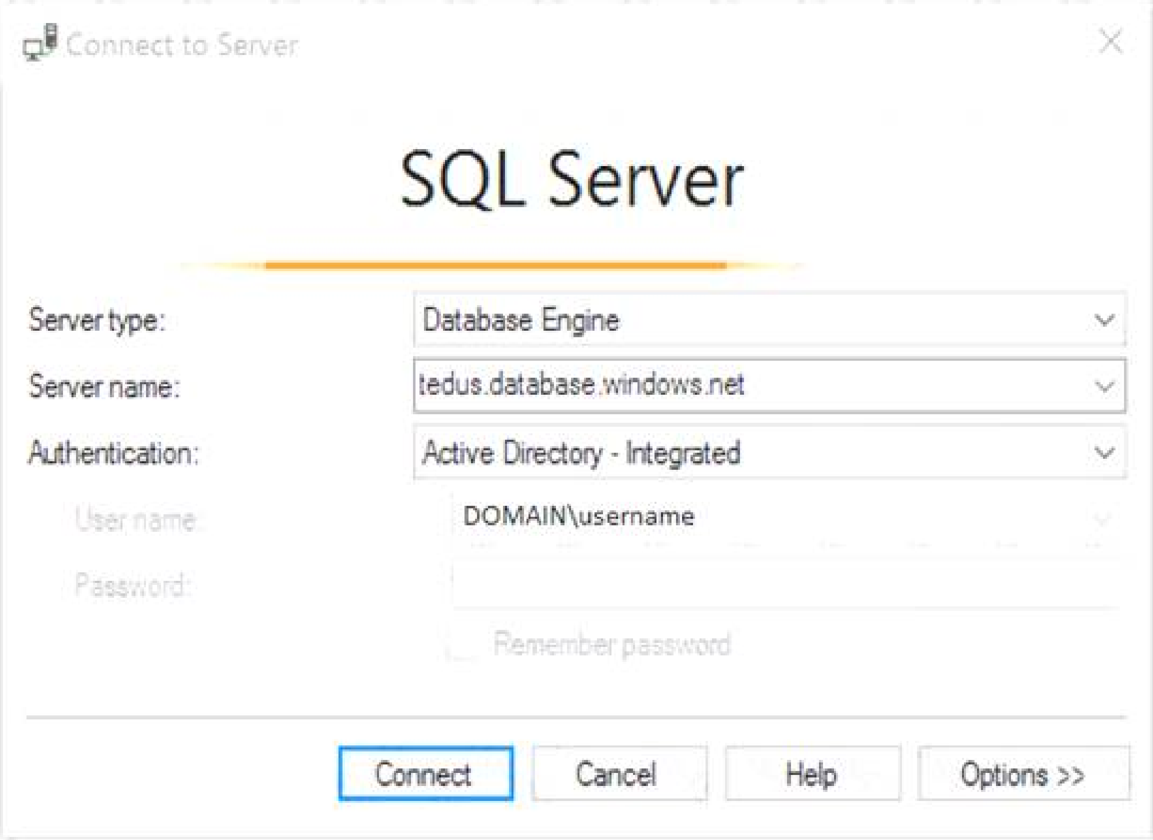
Explanation:
To ‘Read a storage account’, ie. list the blobs in the storage account, you need an ‘Action’ permission. To read the data in a storage account, ie. open a blob, you need a ‘DataAction’ permission.
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-definitions

NEW QUESTION 19
- (Exam Topic 4)
You have a hybrid configuration of Azure Active Directory (Azure AD).
All users have computers that run Windows 10 and are hybrid Azure AD joined.
You have an Azure SQL database that is configured to support Azure AD authentication.
Database developers must connect to the SQL database by using Microsoft SQL Server Management Studio (SSMS) and authenticate by using their on-premises Active Directory account.
You need to tell the developers which authentication method to use to connect to the SQL database from SSMS. The solution must minimize authentication prompts.
Which authentication method should you instruct the developers to use?

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

Answer: C

Explanation:
Azure AD can be the initial Azure AD managed domain. Azure AD can also be an on-premises Active Directory Domain Services that is federated with the Azure AD.
Using an Azure AD identity to connect using SSMS or SSDT
The following procedures show you how to connect to a SQL database with an Azure AD identity using SQL Server Management Studio or SQL Server Database Tools.
Active Directory integrated authentication
Use this method if you are logged in to Windows using your Azure Active Directory credentials from a federated domain.
* 1. Start Management Studio or Data Tools and in the Connect to Server (or Connect to Database Engine) dialog box, in the Authentication box, select Active Directory - Integrated. No password is needed or can be entered because your existing credentials will be presented for the connection.



Server type: Database Engine
Server name: tedus.database.windows.net
Authentication: Active Directory - Integrated
User name: DOMAIN\username
Password:
□ Remember password

* 2. Select the Options button, and on the Connection Properties page, in the Connect to database box, type the name of the user database you want to connect to. (The AD domain name or tenant ID” option is only supported for Universal with MFA connection options, otherwise it is greyed out.)
References:
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/sql-database/sql-database-aad-authentication

NEW QUESTION 20
- (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: Userl -28681041@ExamUsers.com
Azure Password: GpOAe4@lDg
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

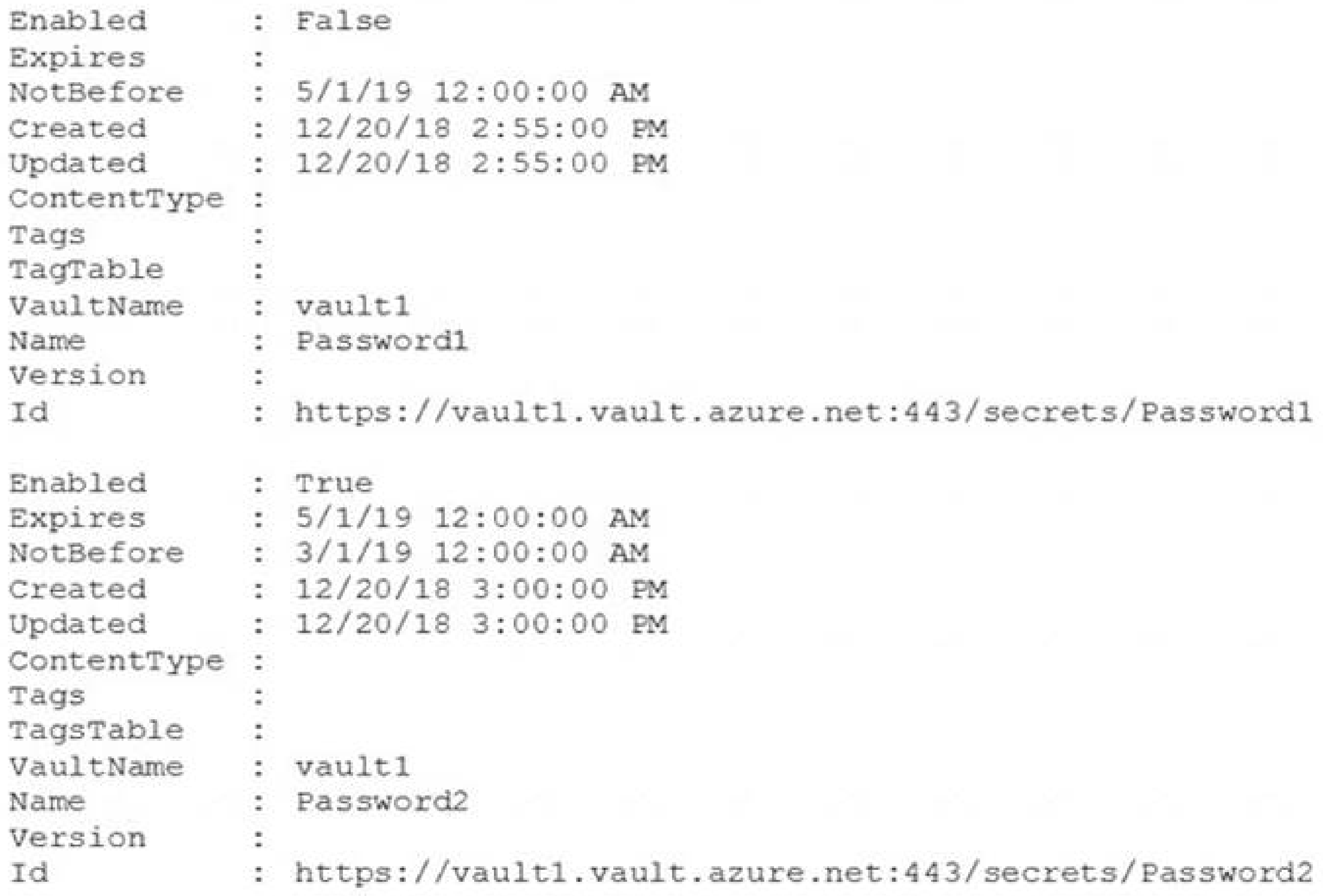
Answer: A

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.

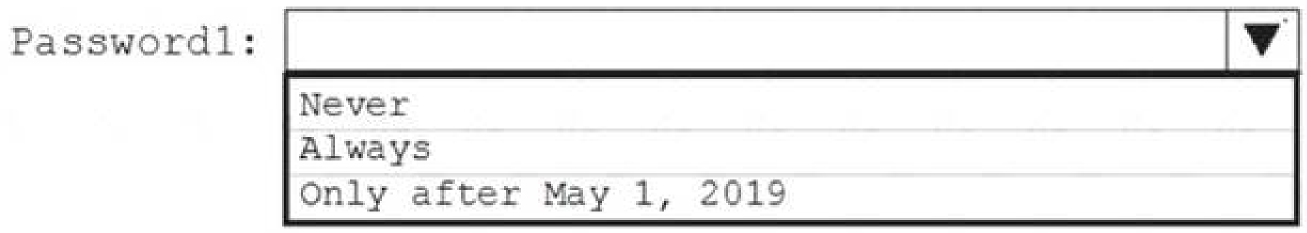
You can find more information on this topic in the following Microsoft documentation: Add a network interface to an application security group using the Azure portal.

NEW QUESTION 24
- (Exam Topic 4)
You have an Azure subscription that contains an Azure key vault named Vault1. On January 1, 2019, Vault1 stores the following secrets.

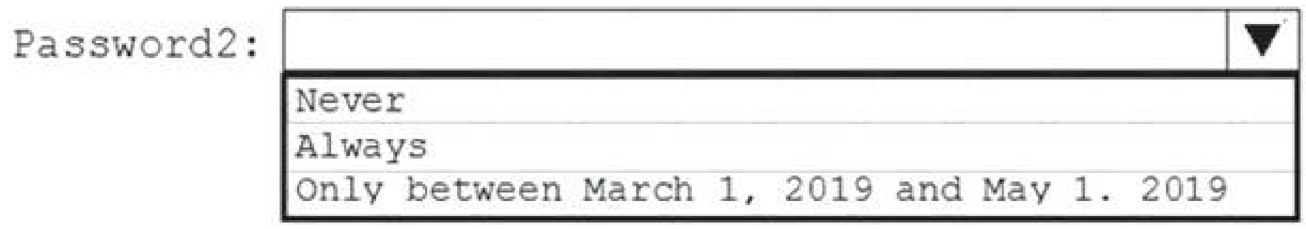


```
Enabled      : False
Expires      :
NotBefore    : 5/1/19 12:00:00 AM
Created      : 12/20/18 2:55:00 PM
Updated      : 12/20/18 2:55:00 PM
ContentType  :
Tags         :
TagTable     :
VaultName    : vault1
Name         : Password1
Version      :
Id           : https://vault1.vault.azure.net:443/secrets/Password1

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

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



Password1: ▼
Never
Always
Only after May 1, 2019

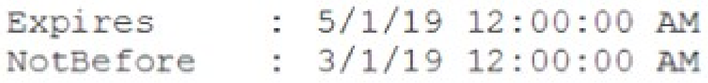


Password2: ▼
Never
Always
Only between March 1, 2019 and May 1. 2019

A. Mastered
B. Not Mastered

Answer: A

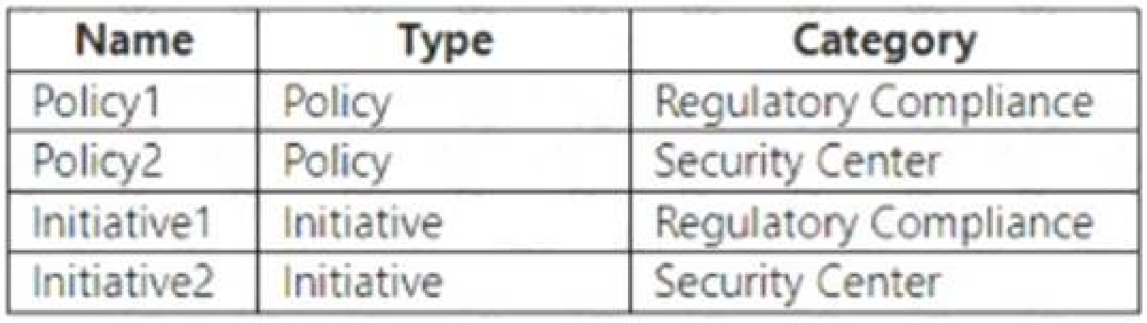
Explanation:
Box 1: Never Password1 is disabled.
Box 2: Only between March 1, 2019 and May 1, Password2:



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

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

NEW QUESTION 25
- (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 30
- (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 RGI.
D. Apply a resource lock to RGI.

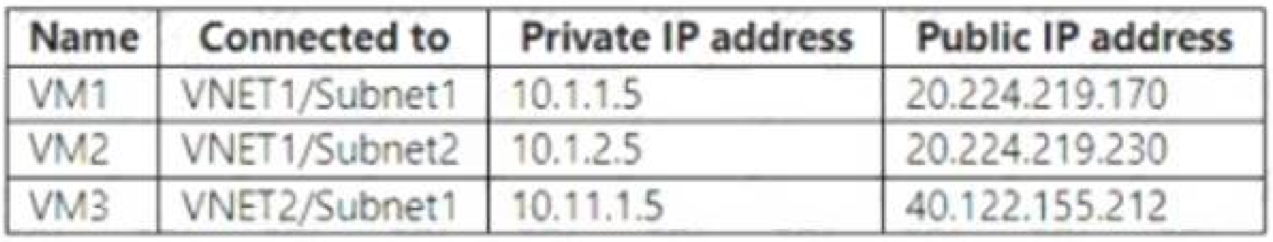
Answer: B

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.

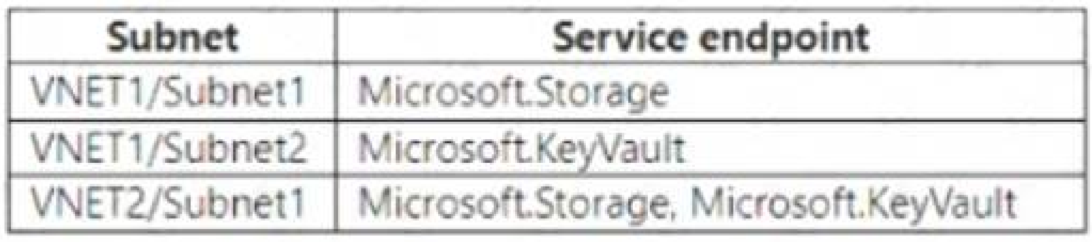
https://learn.microsoft.com/en-us/azure/security/fundamentals/virtual-machines-overview

NEW QUESTION 34
- (Exam Topic 4)
You have an Azure subscription that is linked to an Azure AD tenant and contains the virtual machines shown in the following table.



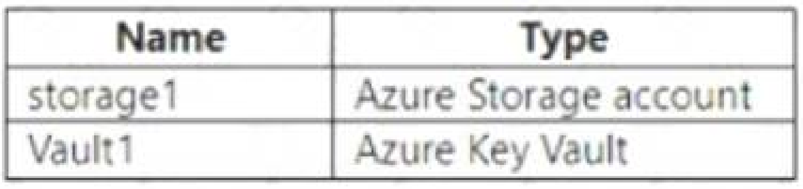
Name	Connected to	Private IP address	Public IP address
VM1	VNET1/Subnet1	10.1.1.5	20.224.219.170
VM2	VNET1/Subnet2	10.1.2.5	20.224.219.230
VM3	VNET2/Subnet1	10.11.1.5	40.122.155.212

The subnets of the virtual networks have the service endpoints shown in the following table.



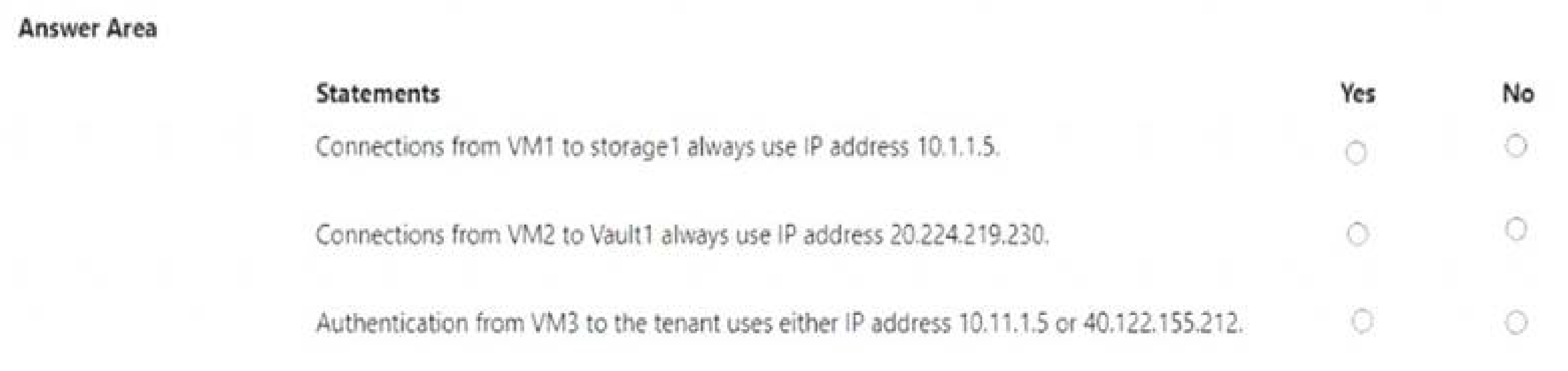
Subnet	Service endpoint
VNET1/Subnet1	Microsoft.Storage
VNET1/Subnet2	Microsoft.KeyVault
VNET2/Subnet1	Microsoft.Storage, Microsoft.KeyVault

You create the resources shown in the following table.



Name	Type
storage1	Azure Storage account
Vault1	Azure Key Vault

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



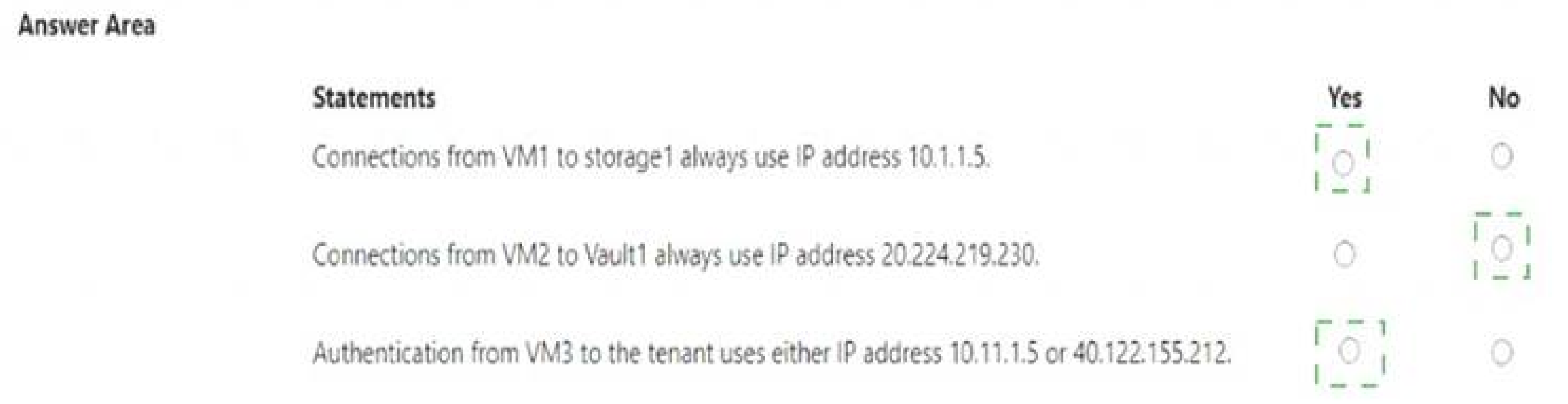
Answer Area

Statements	Yes	No
Connections from VM1 to storage1 always use IP address 10.1.1.5.	○	○
Connections from VM2 to Vault1 always use IP address 20.224.219.230.	○	○
Authentication from VM3 to the tenant uses either IP address 10.11.1.5 or 40.122.155.212.	○	○

A. Mastered
B. Not Mastered

Answer: A

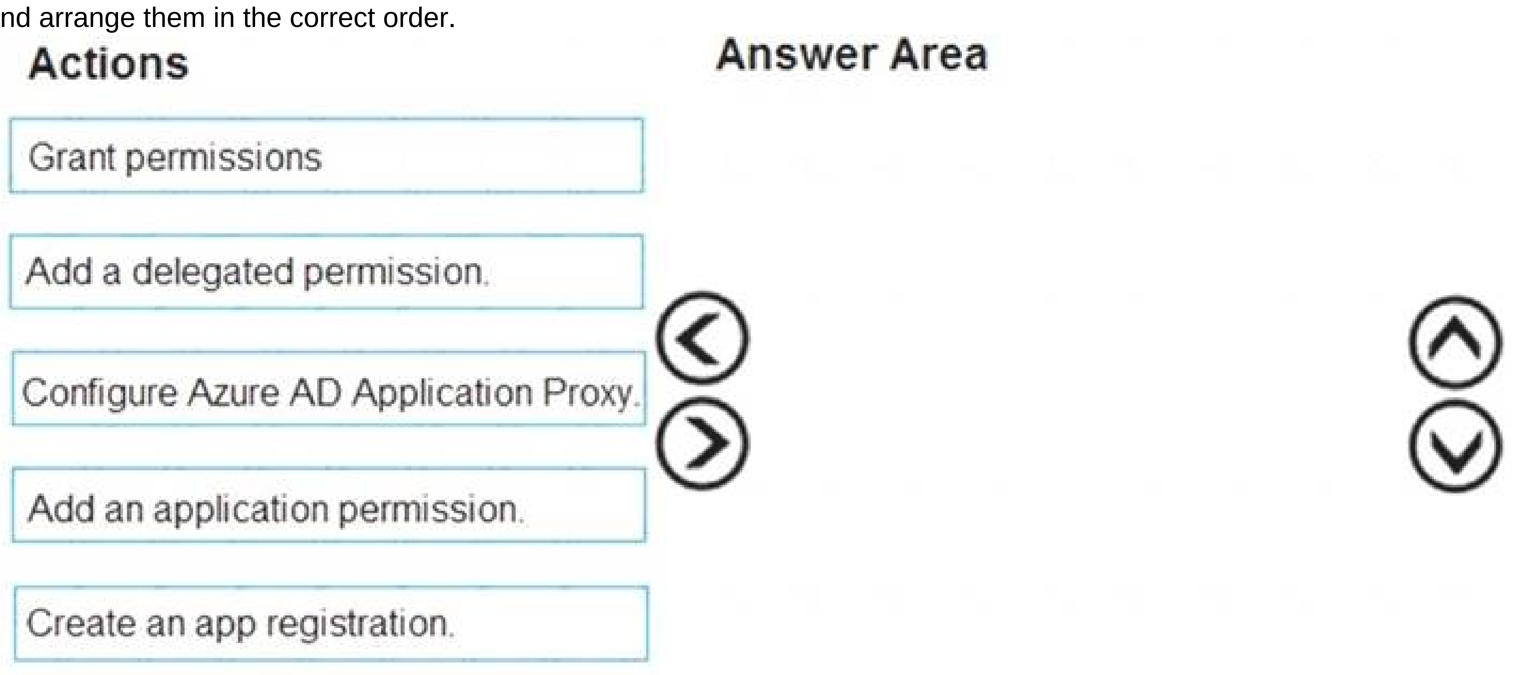
Explanation:



Answer Area

Statements	Yes	No
Connections from VM1 to storage1 always use IP address 10.1.1.5.	[✓ ○]	○
Connections from VM2 to Vault1 always use IP address 20.224.219.230.	○	[✓ ○]
Authentication from VM3 to the tenant uses either IP address 10.11.1.5 or 40.122.155.212.	[✓ ○]	○

NEW QUESTION 38
- (Exam Topic 4)
Your company has an Azure Active Directory (Azure AD) tenant named contoso.com.
The company is developing an application named App1. App1 will run as a service on server that runs Windows Server 2016. App1 will authenticate to contoso.com and access Microsoft Graph to read directory data.
You need to delegate the minimum required permissions to App1.
Which three actions should you perform in sequence from the Azure portal? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Actions

- Grant permissions
- Add a delegated permission.
- Configure Azure AD Application Proxy.
- Add an application permission.
- Create an app registration.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Step 1: Create an app registration
First the application must be created/registered. Step 2: Add an application permission
Application permissions are used by apps that run without a signed-in user present. Step 3: Grant permissions

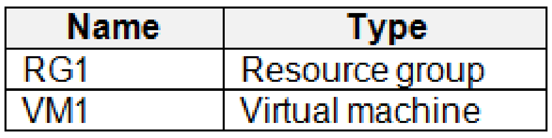
NEW QUESTION 39
- (Exam Topic 4)
You are troubleshooting a security issue for an Azure Storage account.
You enable the diagnostic logs for the storage account. What should you use to retrieve the diagnostics logs?

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

Answer: D

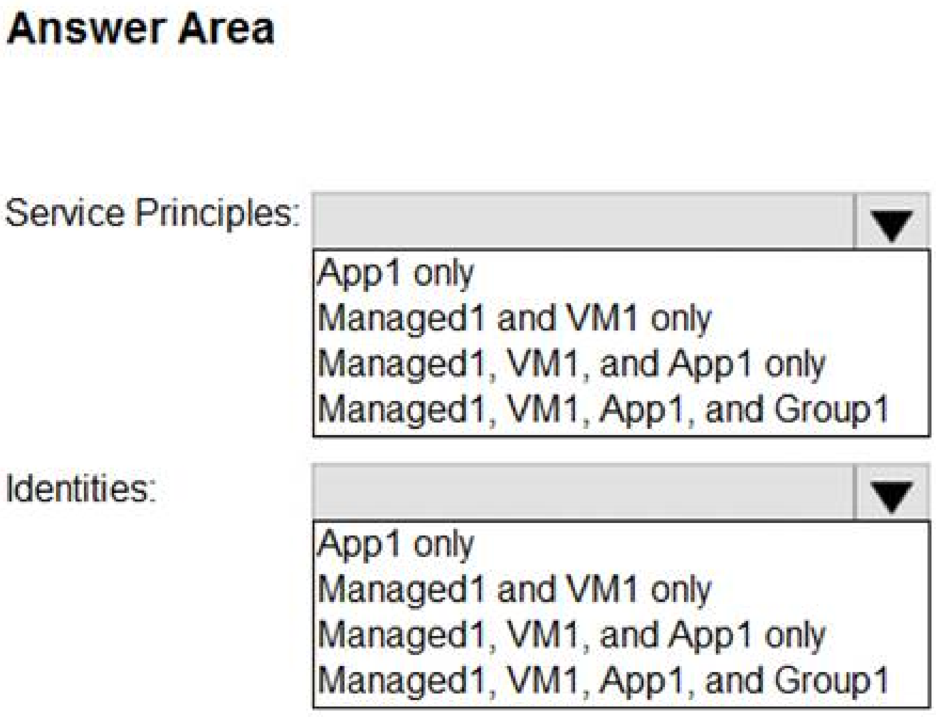
Explanation:
References:
https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-logging?toc=%2fazure%2fstorage%2

NEW QUESTION 44
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.



Name	Type
RG1	Resource group
VM1	Virtual machine

You perform the following tasks:
Create a managed identity named Managed1. Create a Microsoft 365 group named Group1.
You need to identify which service principals were created and which identities can be assigned the Reader role for RG1. What should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

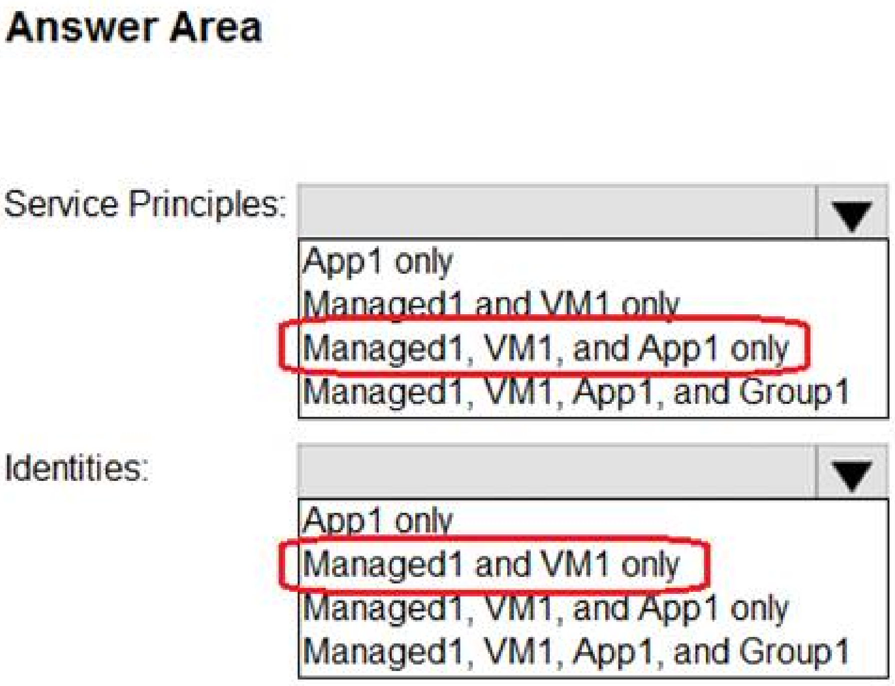
Service Principles:
- App1 only
- Managed1 and VM1 only
- Managed1, VM1, and App1 only
- Managed1, VM1, App1, and Group1

Identities:
- App1 only
- Managed1 and VM1 only
- Managed1, VM1, and App1 only
- Managed1, VM1, App1, and Group1

A. Mastered
B. Not Mastered

Answer: A

Explanation:

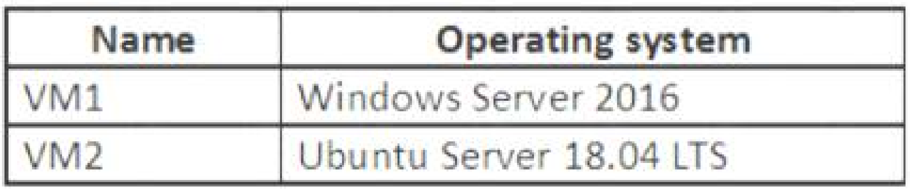


Answer Area

Service Principles:
- App1 only
- Managed1 and VM1 only
- [✓ Managed1, VM1, and App1 only]
- Managed1, VM1, App1, and Group1

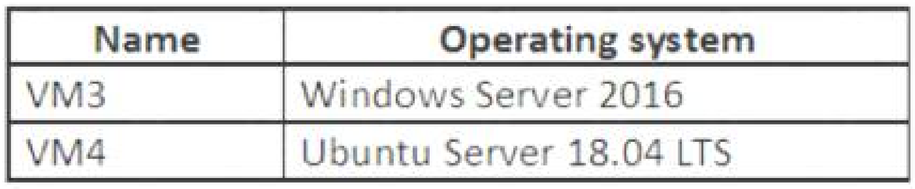
Identities:
- App1 only
- [✓ Managed1 and VM1 only]
- Managed1, VM1, and App1 only
- Managed1, VM1, App1, and Group1

NEW QUESTION 47
- (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

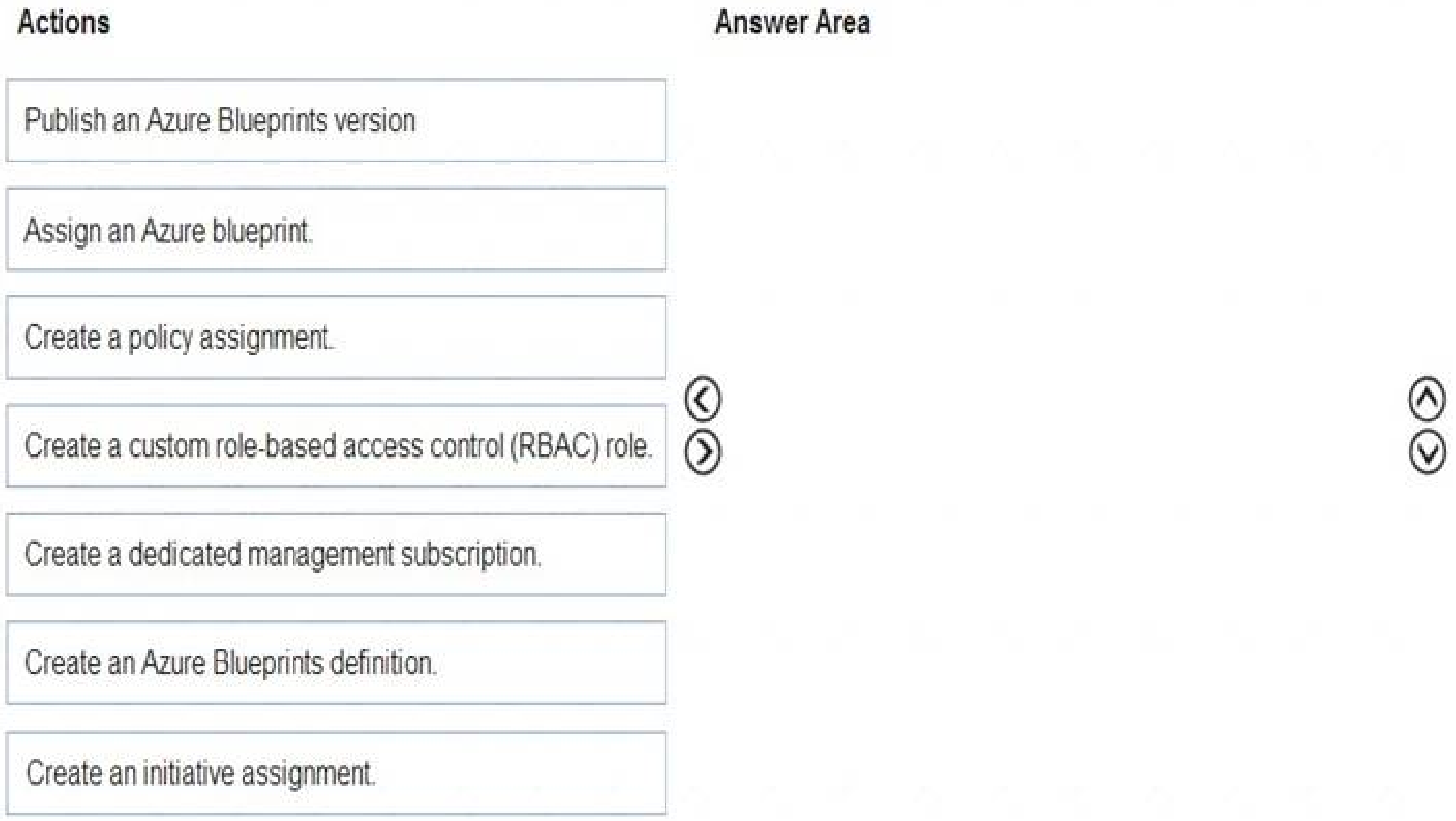
NEW QUESTION 51
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant and a root management group. You create 10 Azure subscriptions and add the subscriptions to the rout management group.
You need to create an Azure Blueprints definition that will be stored in the root management group. What should you do first?

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

Answer: B

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

NEW QUESTION 56
- (Exam Topic 4)
You have five Azure subscriptions linked to a single Azure Active Directory (Azure AD) tenant. You create an Azure Policy initiative named SecurityPolicyInitiative1.
You identify which standard role assignments must be configured on all new resource groups.
You need to enforce SecurityPolicyInitiative1 and the role assignments when a new resource group is created. Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Actions

Publish an Azure Blueprints version

Assign an Azure blueprint.

Create a policy assignment.

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

Create a dedicated management subscription.

Create an Azure Blueprints definition.

Create an initiative assignment.

Answer Area

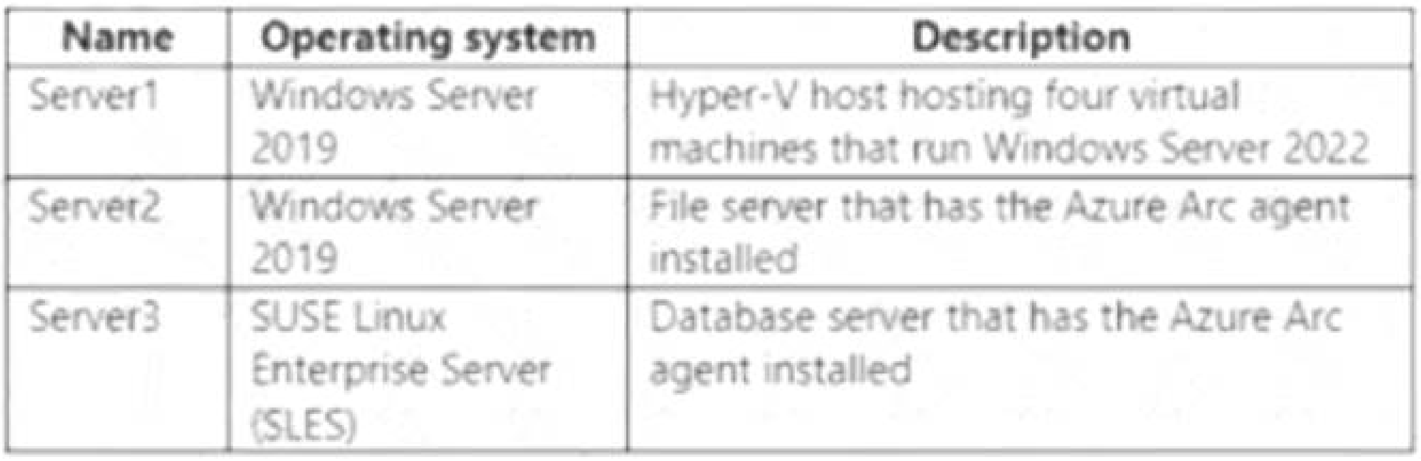
A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:

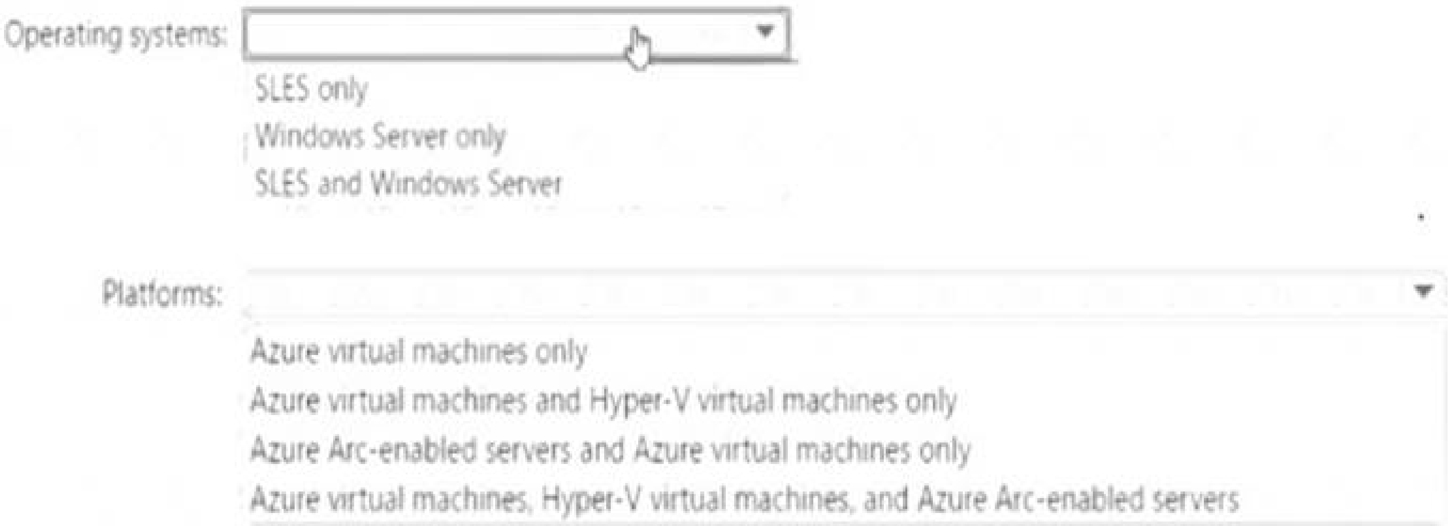
https://docs.microsoft.com/en-us/azure/governance/blueprints/create-blueprint-portal https://docs.microsoft.com/en-us/azure/azure-australia/azure-policy

NEW QUESTION 57
- (Exam Topic 4)
Your on-premises network contains the servers shown in the following table.



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

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



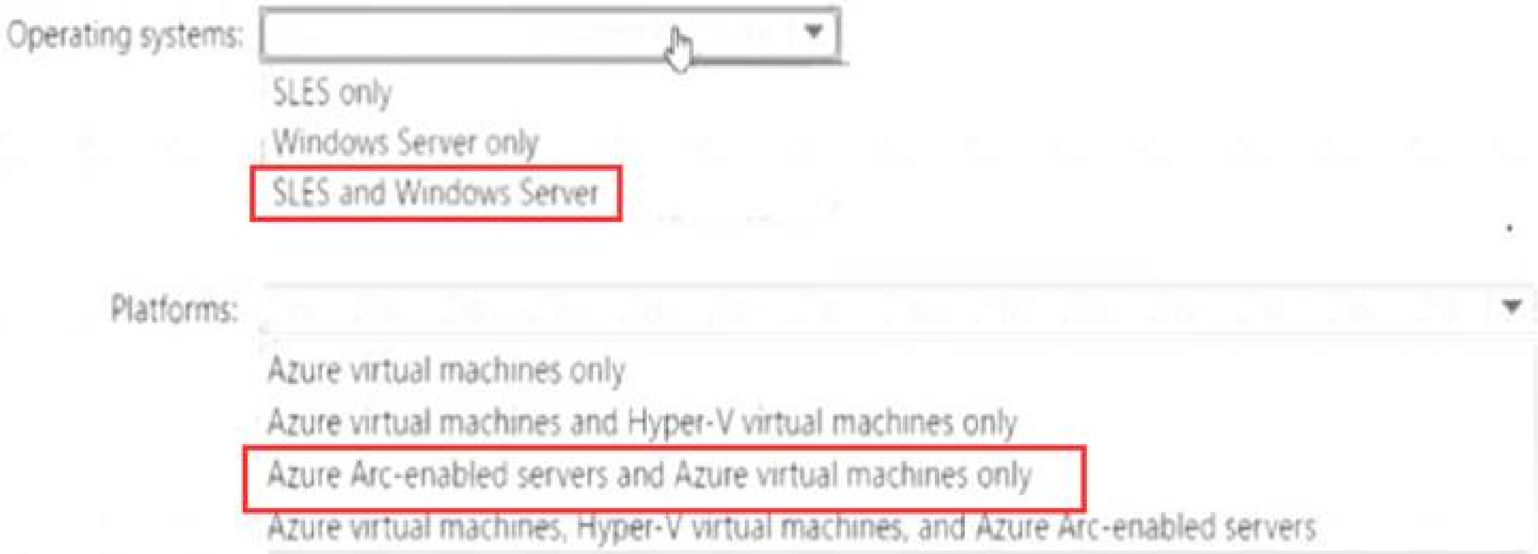
Operating systems:
- SLES only
- Windows Server only
- SLES and Windows Server

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

A. Mastered
B. Not Mastered

Answer: A

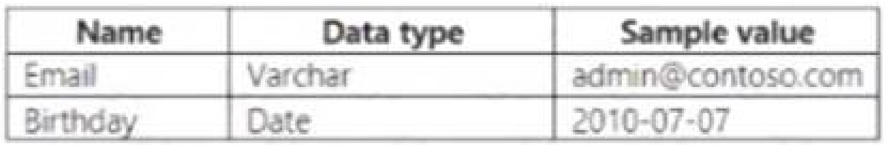
Explanation:



Operating systems:
- SLES only
- Windows Server only
- [✓ SLES and Windows Server]

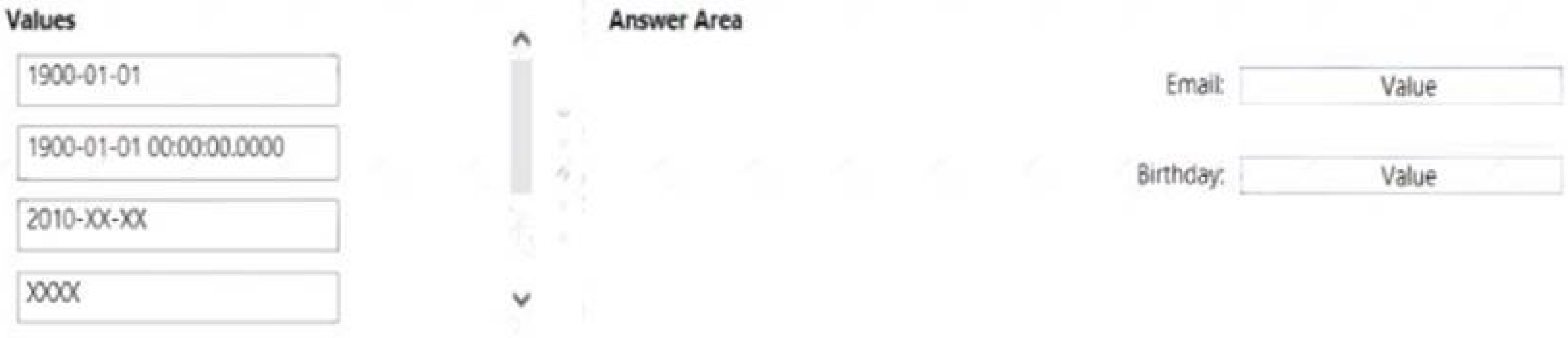
Platforms:
- Azure virtual machines only
- Azure virtual machines and Hyper-V virtual machines only
- [✓ Azure Arc-enabled servers and Azure virtual machines only]
- Azure virtual machines, Hyper-V virtual machines, and Azure Arc-enabled servers

NEW QUESTION 61
- (Exam Topic 4)
You have an Azure subscription that contains an Azure SQL database named SQLDB1. SQLDB1 contains the columns shown in the following table.



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

For the Email and Birthday columns, you implement dynamic data masking by using the default masking function.
Which value will the users see in each column? To answer, drag the appropriate values to the correct columns. Each value may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Values

1900-01-01

1900-01-01 00:00:00.0000

2010-XX-XX

XXXX

Answer Area

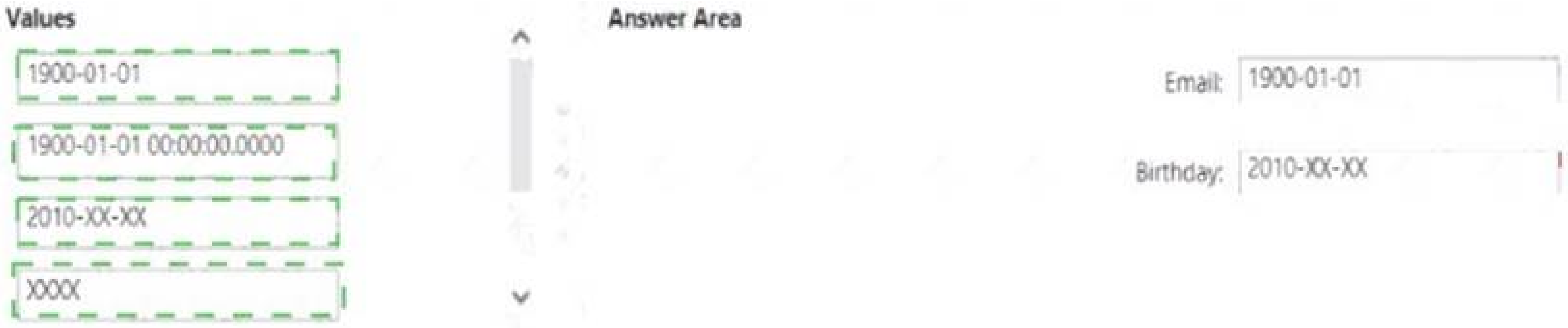
Email: Value

Birthday: Value

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Values

1900-01-01

1900-01-01 00:00:00.0000

2010-XX-XX

XXXX

Answer Area

Email: 1900-01-01

Birthday: 2010-XX-XX

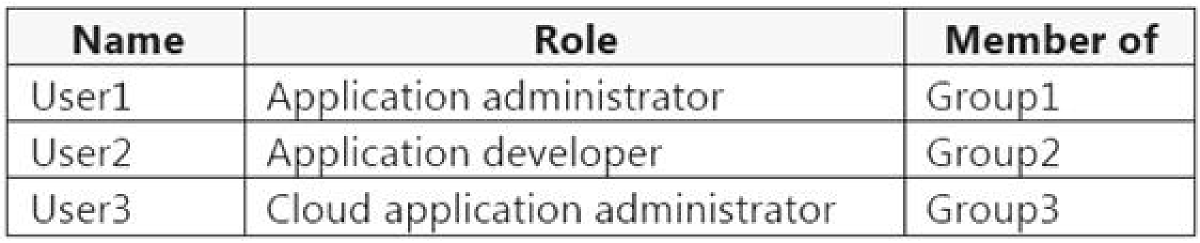
NEW QUESTION 64
- (Exam Topic 4)
You have 15 Azure virtual machines in a resource group named RG1. All virtual machines run identical applications.
You need to prevent unauthorized applications and malware from running on the virtual machines. What should you do?

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

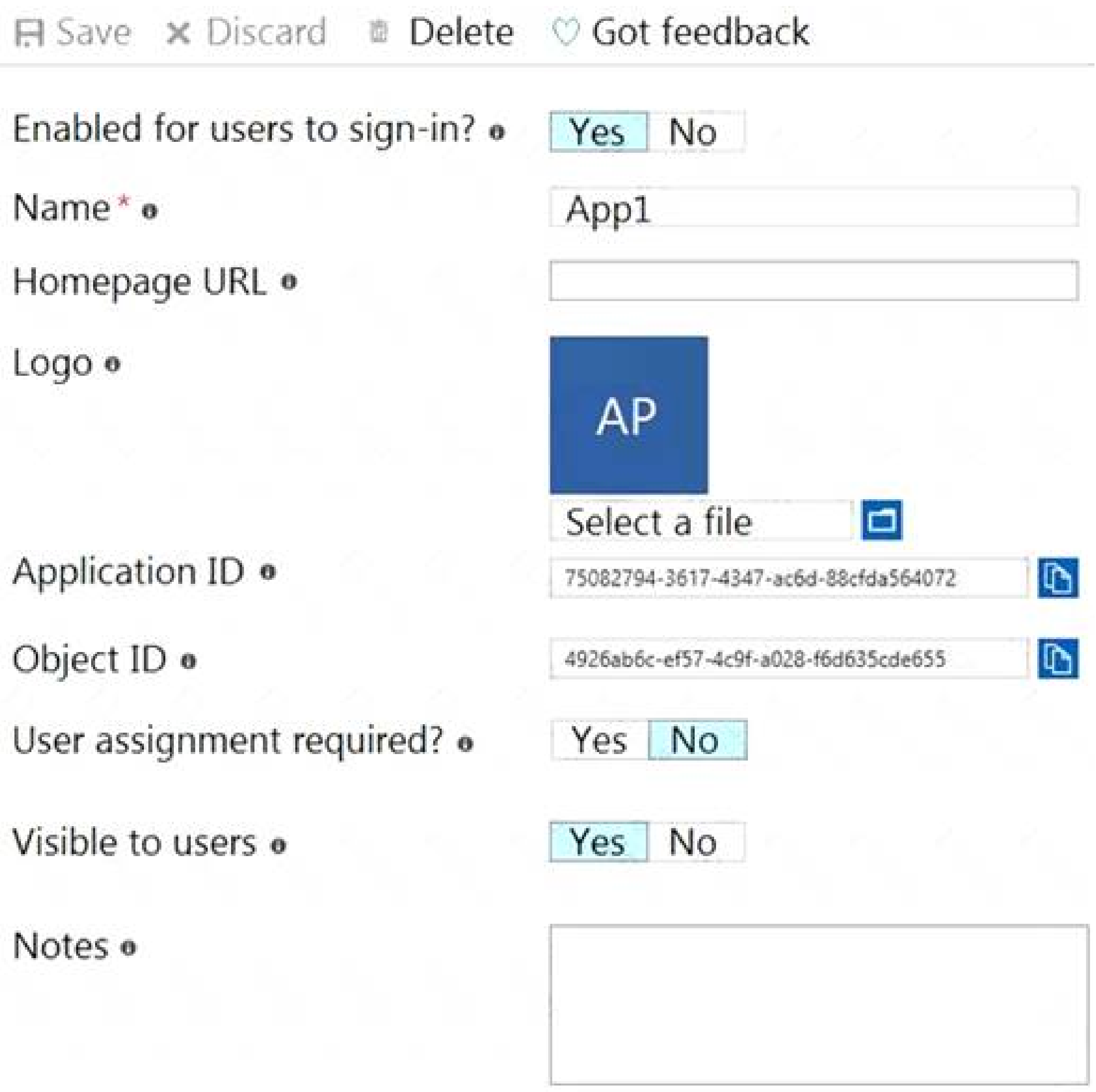
NEW QUESTION 69
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains three security groups named Group1, Group2, and Group3 and the users shown in the following table.



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

Group3 is a member of Group2.
In contoso.com, you register an enterprise application named App1 that has the following settings:
- Owners: User1
- Users and groups: Group2

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



Enabled for users to sign-in? [✓ Yes] No

Name * App1

Homepage URL

Logo AP

Application ID 75082794-3617-4347-ac6d-88cfda564072

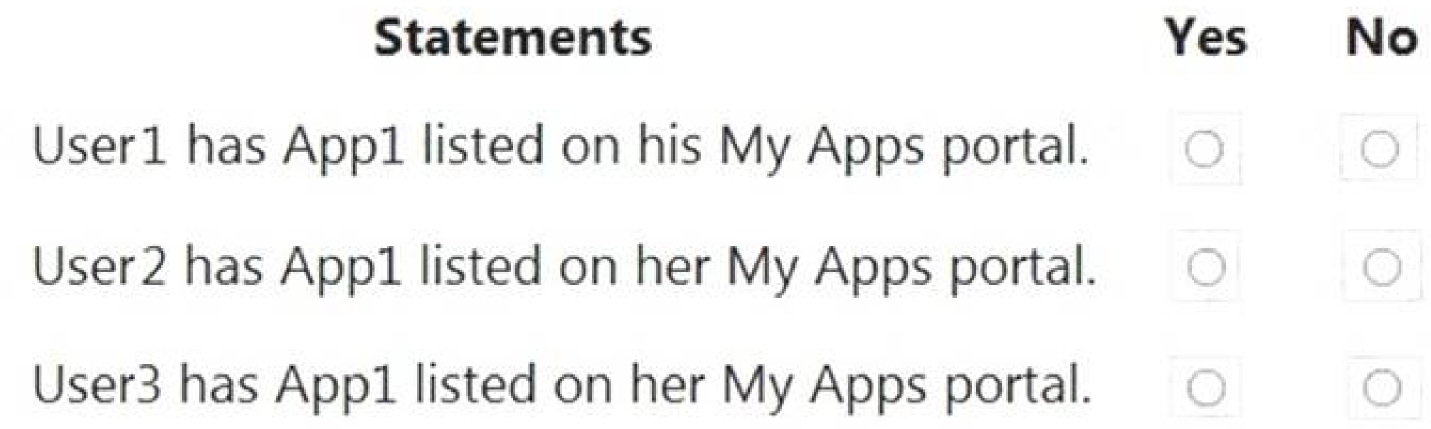
Object ID 4926ab6c-ef57-4c9f-a028-f6d635cde655

User assignment required? Yes [✓ No]

Visible to users [✓ Yes] No

Notes

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



Statements	Yes	No
User1 has App1 listed on his My Apps portal.	○	○
User2 has App1 listed on her My Apps portal.	○	○
User3 has App1 listed on her My Apps portal.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Text Description automatically generated
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal

NEW QUESTION 70
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a hybrid configuration of Azure Active Directory (Azure AD).
You have an Azure HDInsight cluster on a virtual network.
You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials. You need to configure the environment to support the planned authentication.
Solution: You deploy Azure Active Directory Domain Services (Azure AD DS) to the Azure subscription. Does this meet the goal?

A. Yes
B. No

Answer: A

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

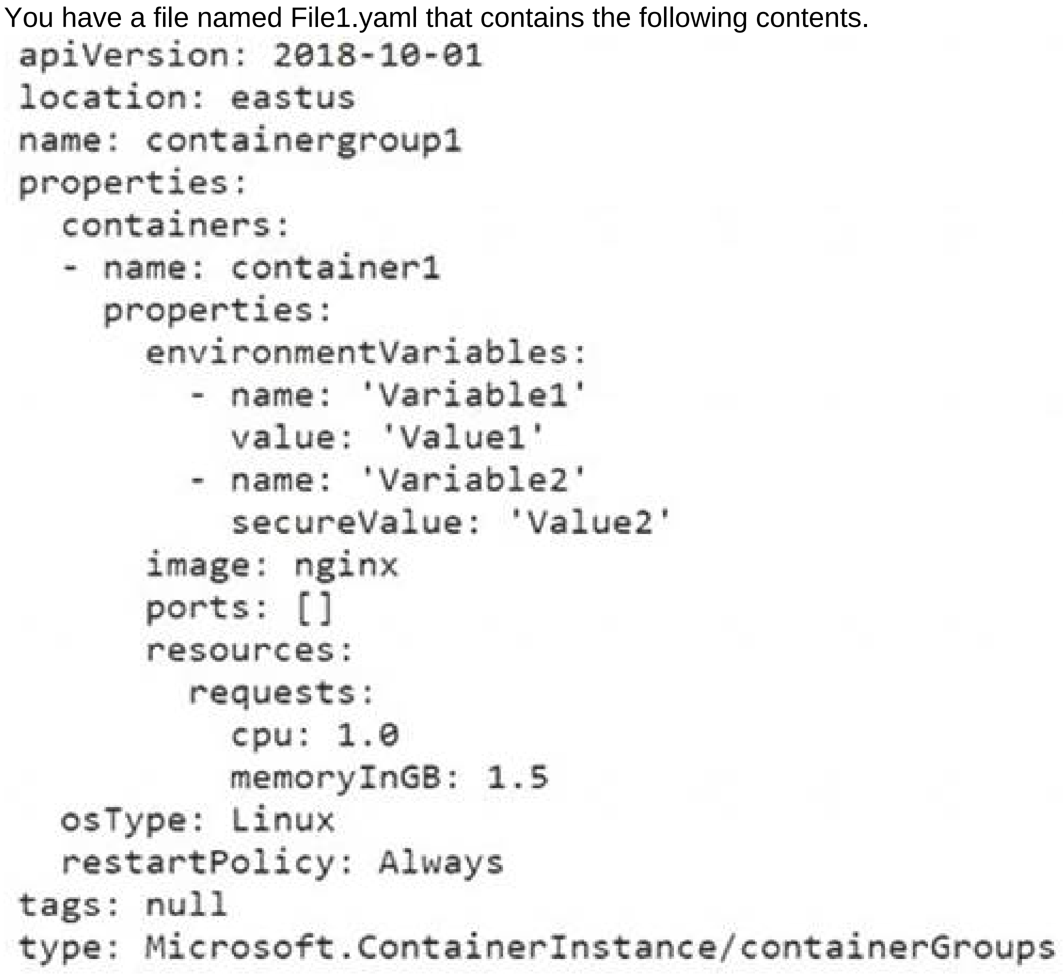
NEW QUESTION 71
- (Exam Topic 4)

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

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

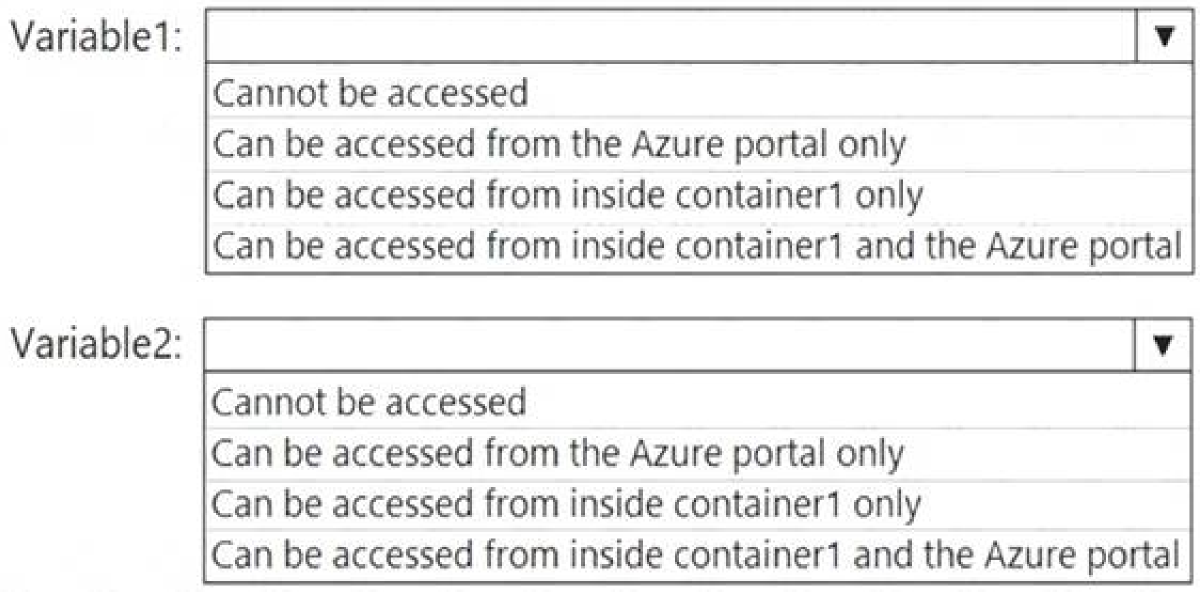
Answer: D

NEW QUESTION 73
- (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

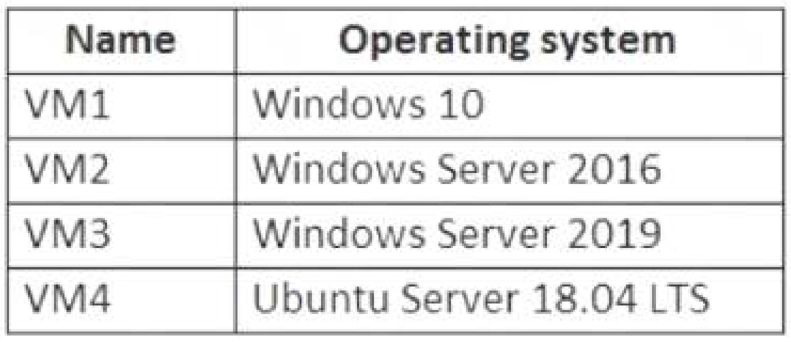
Variable2: ▼
- Cannot be accessed
- Can be accessed from the Azure portal only
- Can be accessed from inside container1 only
- Can be accessed from inside container1 and the Azure portal

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/container-instances/container-instances-environment-variables

NEW QUESTION 75
- (Exam Topic 4)
You have an Azure subscription that contains the Azure virtual machines shown in the following table.



Name	Operating system
VM1	Windows 10
VM2	Windows Server 2016
VM3	Windows Server 2019
VM4	Ubuntu Server 18.04 LTS

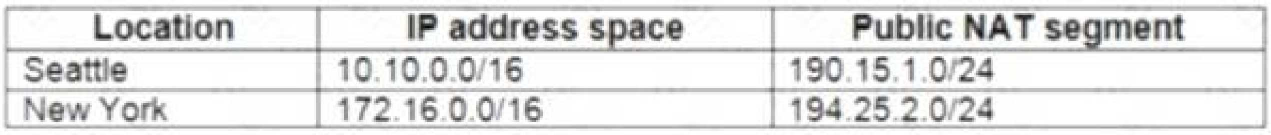
You create an MDM Security Baseline profile named Profile1.
You need to identify to which virtual machines Profile1 can be applied. Which virtual machines should you identify?

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

Answer: A

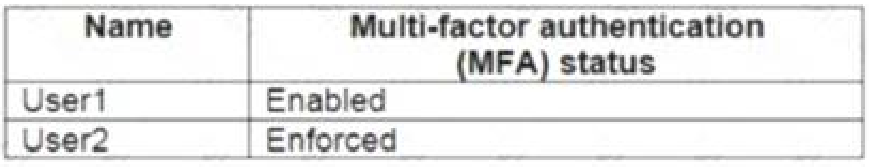
Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines

NEW QUESTION 76
- (Exam Topic 4)
Your company has two offices in Seattle and New York. Each office connects to the Internet by using a NAT device. The offices use the IP addresses shown in the following table.



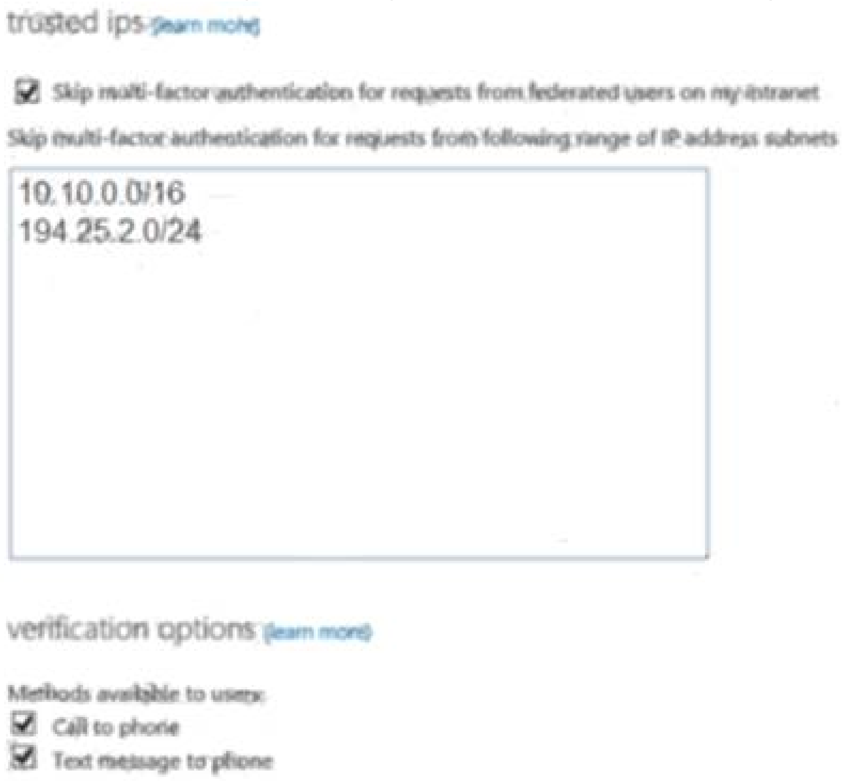
Location	IP address space	Public NAT segment
Seattle	10.10.0.0/16	190.15.1.0/24
New York	172.16.0.0/16	194.25.2.0/24

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



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

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



trusted ips (learn more)

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

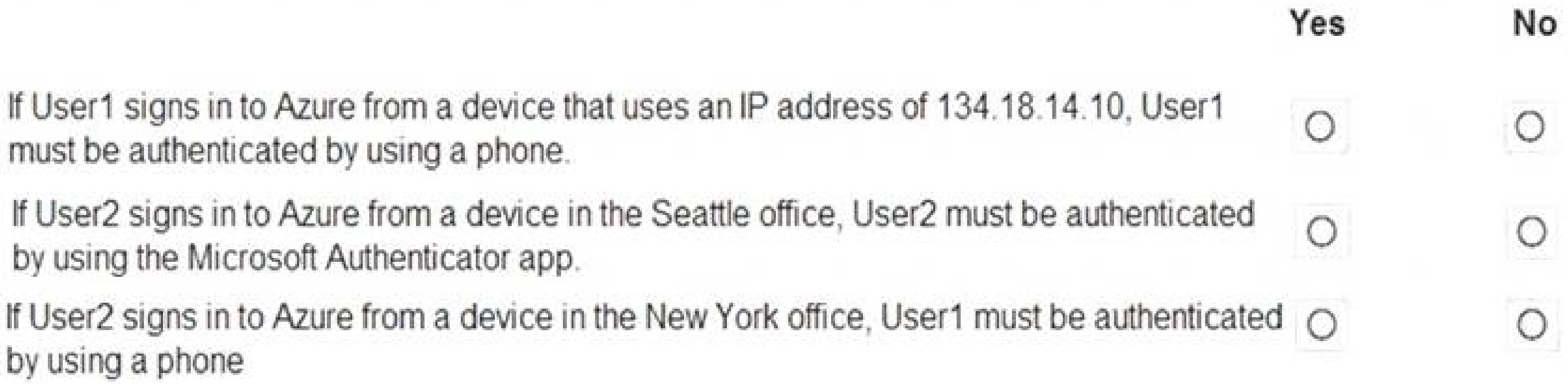
Skip multi-factor authentication for requests from following range of IP address subnets

10.10.0.0/16
194.25.2.0/24

verification options (learn more)

Methods available to users:
☑ Call to phone
☑ Text message to phone

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



	Yes	No
If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.	○	○
If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app.	○	○
If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone	○	○

A. Mastered
B. Not Mastered

Answer: A

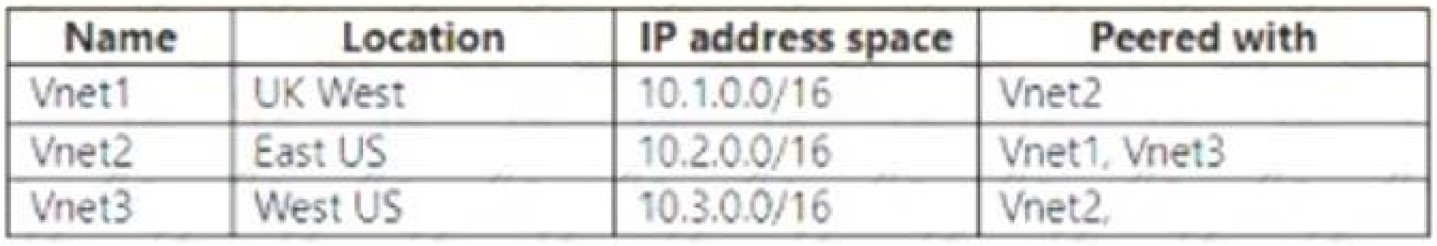
Explanation:
Box 2: No
Use of Microsoft Authenticator is not required.
Note: Microsoft Authenticator is a multifactor app for mobile devices that generates time-based codes used during the Two-Step Verification process.
Box 3: No
The New York IP address subnet is included in the "skip multi-factor authentication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

NEW QUESTION 80
- (Exam Topic 4)
You have an Azure subscription that contains a resource group named RG1 and a security group named ServerAdmins. RG1 contains 10 virtual machines, a virtual network named VNET1, and a network security group JNSG) named NSG1. ServerAdmins can access the virtual machines by using RDP.
You need to ensure that NSG1 only allows RDP connections to the virtual machines for a maximum of 60 minutes when a member of ServerAdmins requests access.
What should you configure?

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

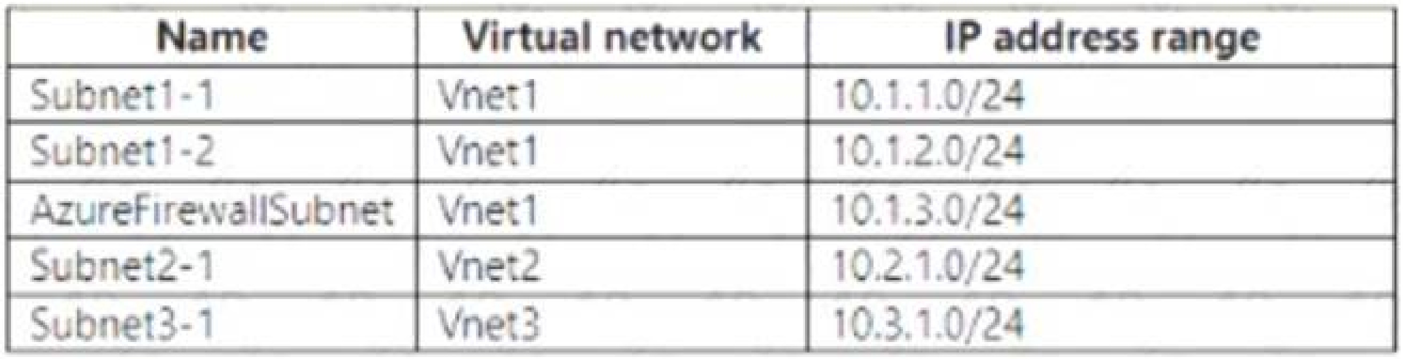
Answer: B

NEW QUESTION 85
- (Exam Topic 4)
You have an Azure subscription that contains the following Azure firewall:
• Name: Fw1
• Azure region: UK West
• Private IP address: 10.1.3.4
• Public IP address: 23.236.62.147
The subscription contains. The virtual networks shown in the following table.



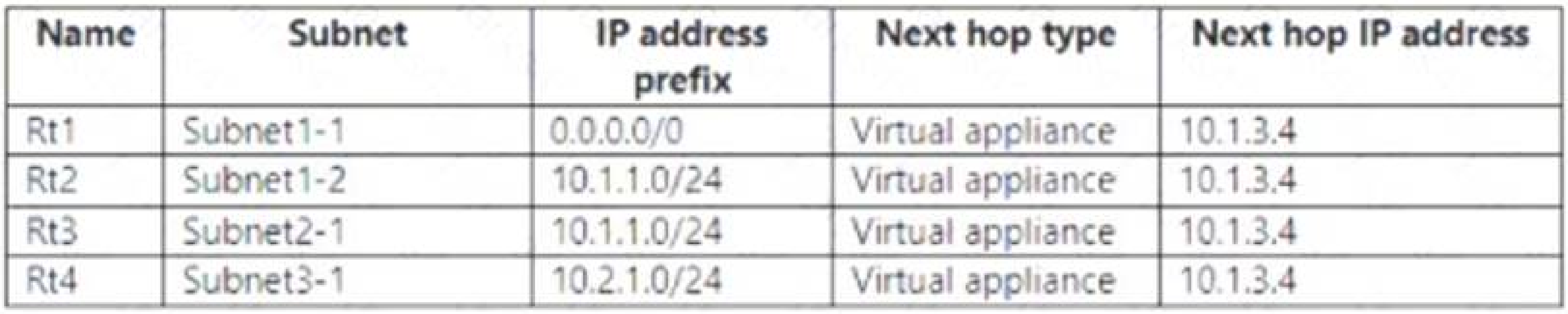
Name	Location	IP address space	Peered with
Vnet1	UK West	10.1.0.0/16	Vnet2
Vnet2	East US	10.2.0.0/16	Vnet1, Vnet3
Vnet3	West US	10.3.0.0/16	Vnet2.

The subscription contains the subnets shown in the following table.



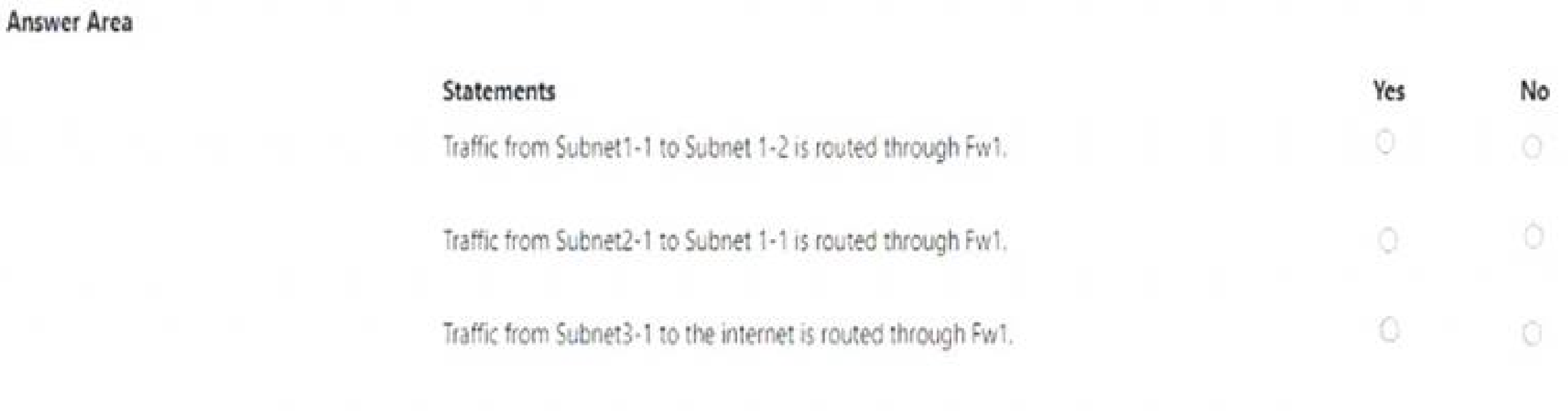
Name	Virtual network	IP address range
Subnet1-1	Vnet1	10.1.1.0/24
Subnet1-2	Vnet1	10.1.2.0/24
AzureFirewallSubnet	Vnet1	10.1.3.0/24
Subnet2-1	Vnet2	10.2.1.0/24
Subnet3-1	Vnet3	10.3.1.0/24

The subscription contains the routes shown in the following table.



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

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



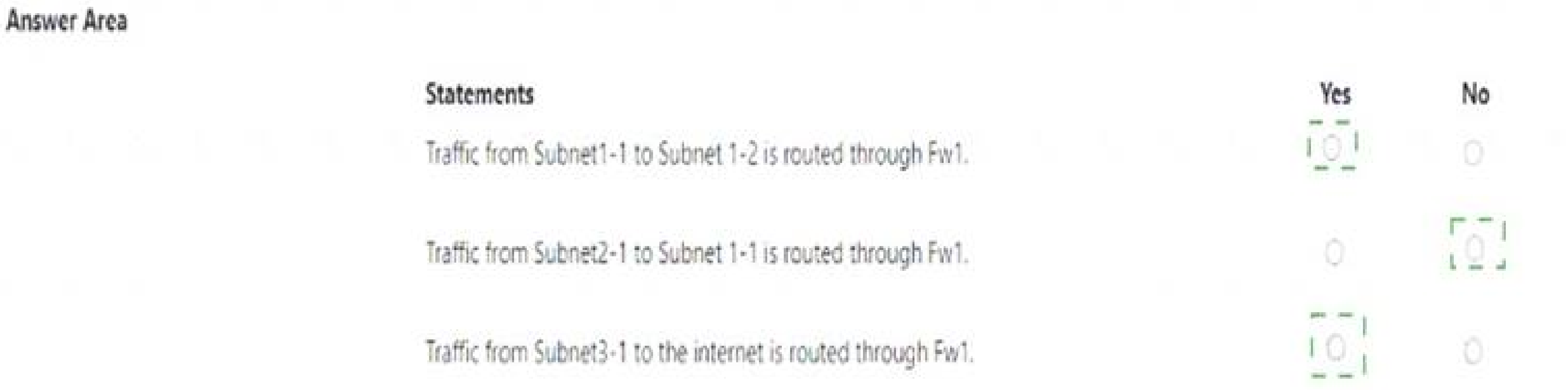
Answer Area

Statements	Yes	No
Traffic from Subnet1-1 to Subnet 1-2 is routed through Fw1.	○	○
Traffic from Subnet2-1 to Subnet 1-1 is routed through Fw1.	○	○
Traffic from Subnet3-1 to the internet is routed through Fw1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

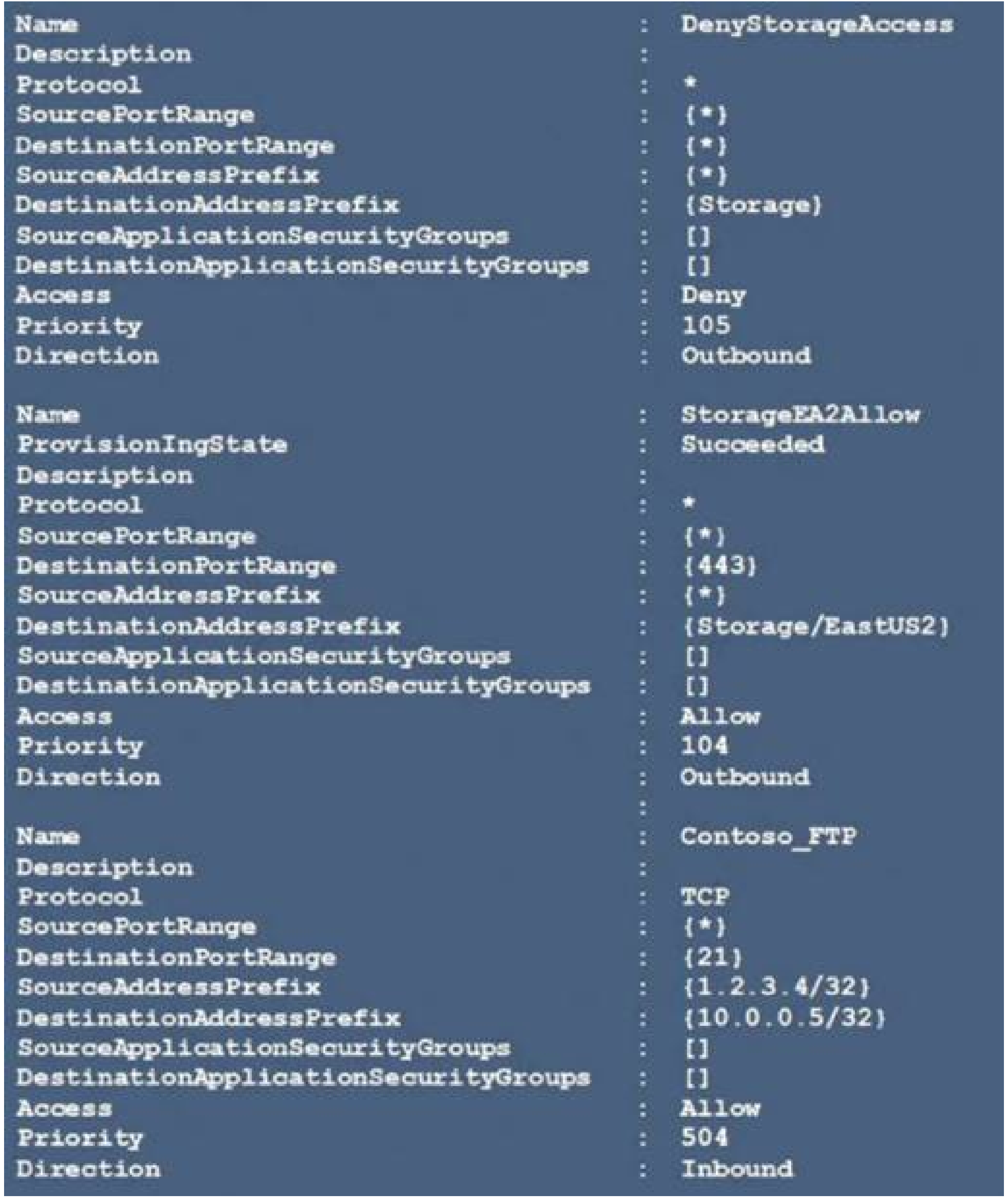
Statements	Yes	No
Traffic from Subnet1-1 to Subnet 1-2 is routed through Fw1.	[✓ ○]	○
Traffic from Subnet2-1 to Subnet 1-1 is routed through Fw1.	○	[✓ ○]
Traffic from Subnet3-1 to the internet is routed through Fw1.	[✓ ○]	○

NEW QUESTION 86

- (Exam Topic 4)

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

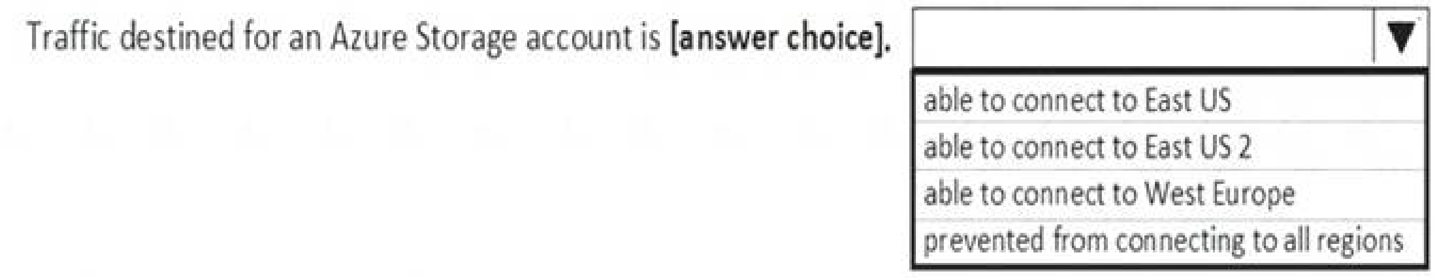
You run Get-AzureRmNetworkSecurityRuleConfig and receive the output shown in the following exhibit.



```
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
```

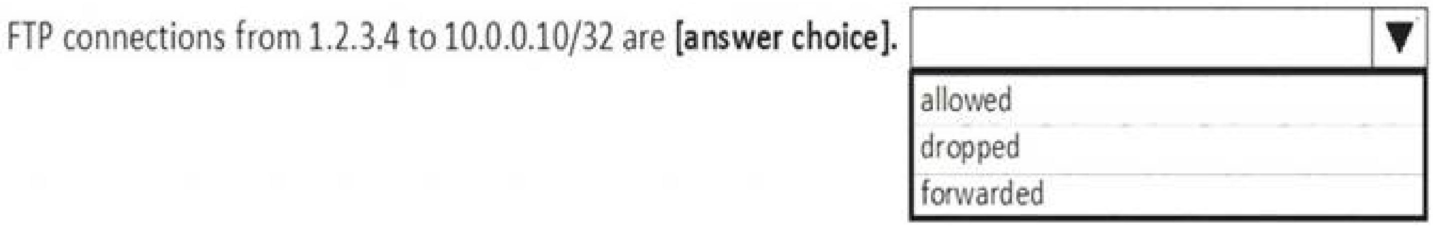
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

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

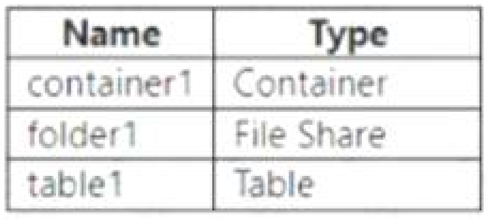
Explanation:
Box 1: able to connect to East US 2
The StorageEA2Allow has DestinationAddressPrefix {Storage/EastUS2} Box 2: dropped
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group

NEW QUESTION 90
- (Exam Topic 4)
You have an Azure subscription that uses Azure AD Privileged Identity Management (PIM). A user named User1 is eligible for the Billing administrator role. You need to ensure that the role can only be used for a maximum of two hours. What should you do?

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

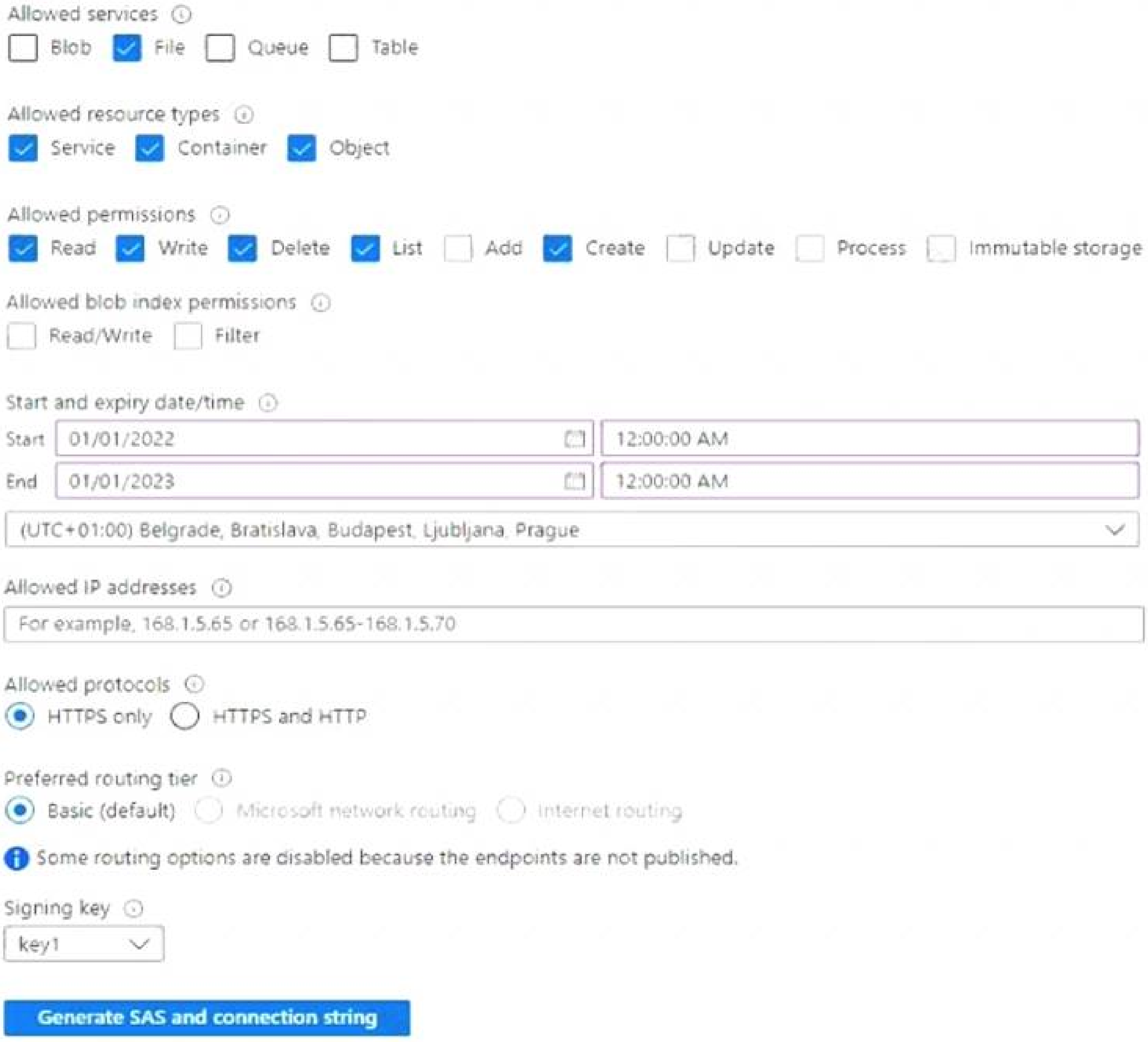
Answer: B

NEW QUESTION 94
- (Exam Topic 4)
You have an Azure subscription that contains a user named User1 and a storage account named storage1. The storage1 account contains the resources shown in the following table.



Name	Type
container1	Container
folder1	File Share
table1	Table

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



Allowed services ⓘ
□ Blob ☑ File □ Queue □ Table

Allowed resource types ⓘ
☑ Service ☑ Container ☑ Object

Allowed permissions ⓘ
☑ Read ☑ Write ☑ Delete ☑ List □ Add ☑ Create □ Update □ Process □ Immutable storage

Allowed blob index permissions ⓘ
□ Read/Write □ Filter

Start and expiry date/time ⓘ
Start 01/01/2022 12:00:00 AM
End 01/01/2023 12:00:00 AM
(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague

Allowed IP addresses ⓘ
For example, 168.1.5.65 or 168.1.5.65-168.1.5.70

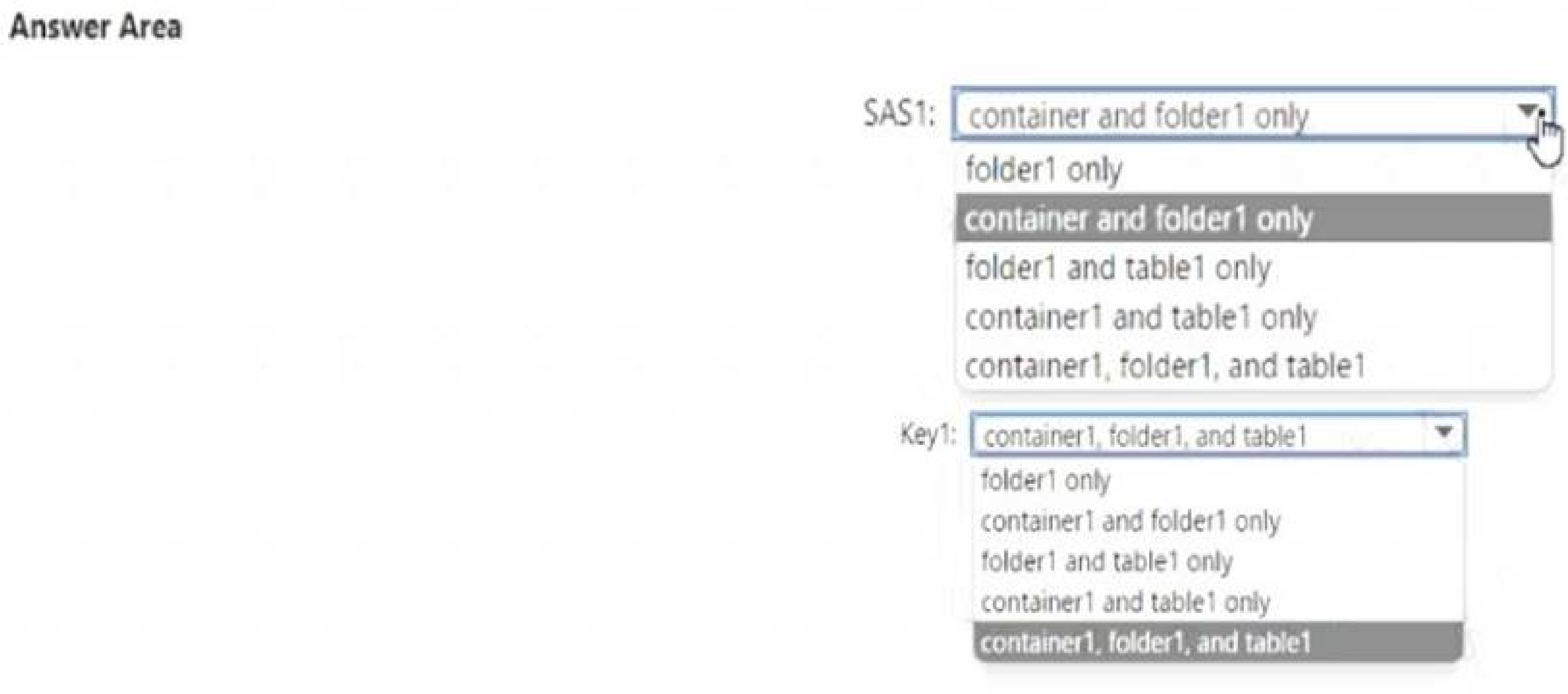
Allowed protocols ⓘ
● HTTPS only ○ HTTPS and HTTP

Preferred routing tier ⓘ
● Basic (default) ○ Microsoft network routing ○ Internet routing

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

Signing key ⓘ
key1

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



Answer Area

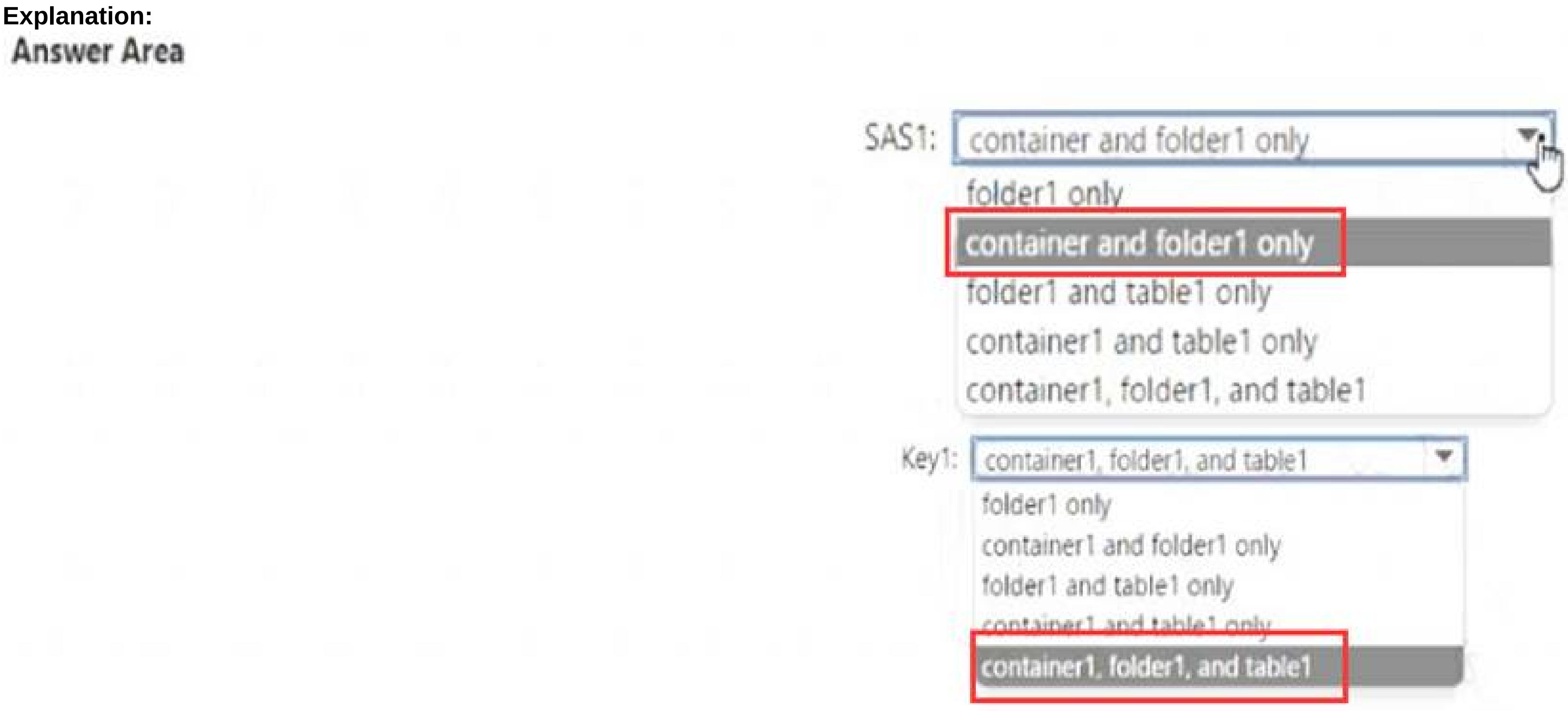
SAS1: container and folder1 only
- folder1 only
- container and folder1 only
- folder1 and table1 only
- container1 and table1 only
- container1, folder1, and table1

Key1: container1, folder1, and table1
- folder1 only
- container1 and folder1 only
- folder1 and table1 only
- container1 and table1 only
- container1, folder1, and table1

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

SAS1: container and folder1 only
- folder1 only
- container and folder1 only
- folder1 and table1 only
- container1 and table1 only
- container1, folder1, and table1

Key1: container1, folder1, and table1
- folder1 only
- container1 and folder1 only
- folder1 and table1 only
- container1 and table1 only
- container1, folder1, and table1

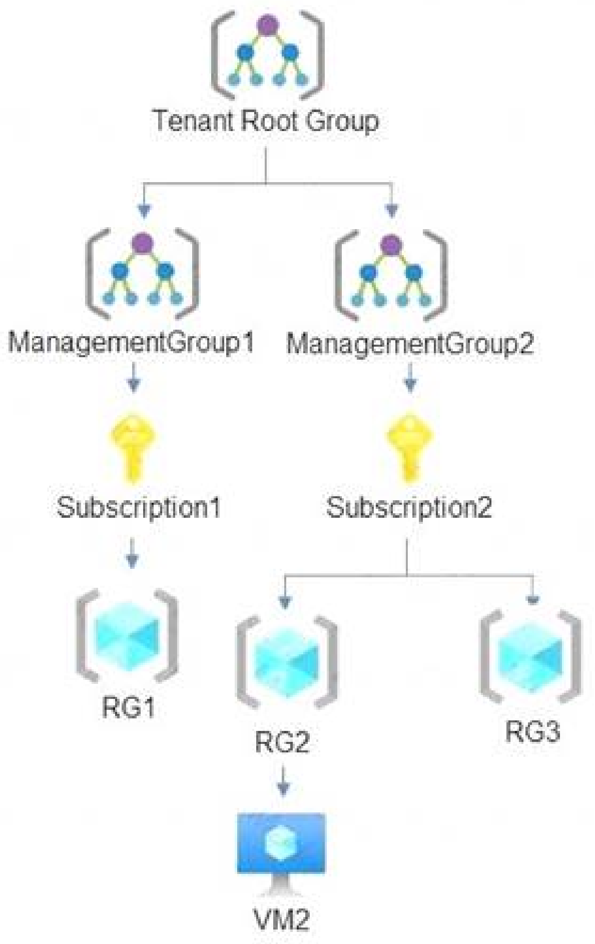
NEW QUESTION 99
- (Exam Topic 4)
You have an Azure subscription that contains a
You need to grant user1 access to blob1. The solution must ensure that the access expires after six days. What should you use?

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

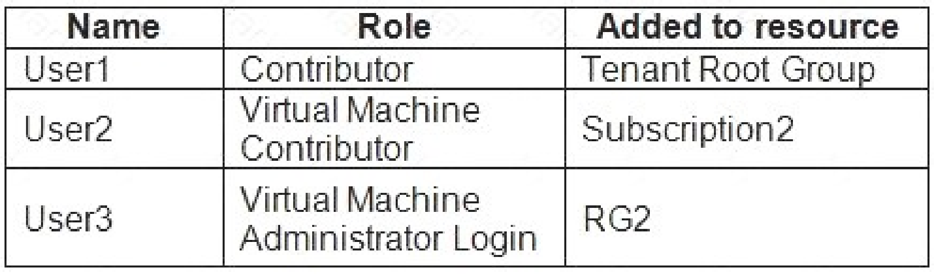
Answer: C

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

NEW QUESTION 103
- (Exam Topic 4)
You have the hierarchy of Azure resources shown in the following exhibit.

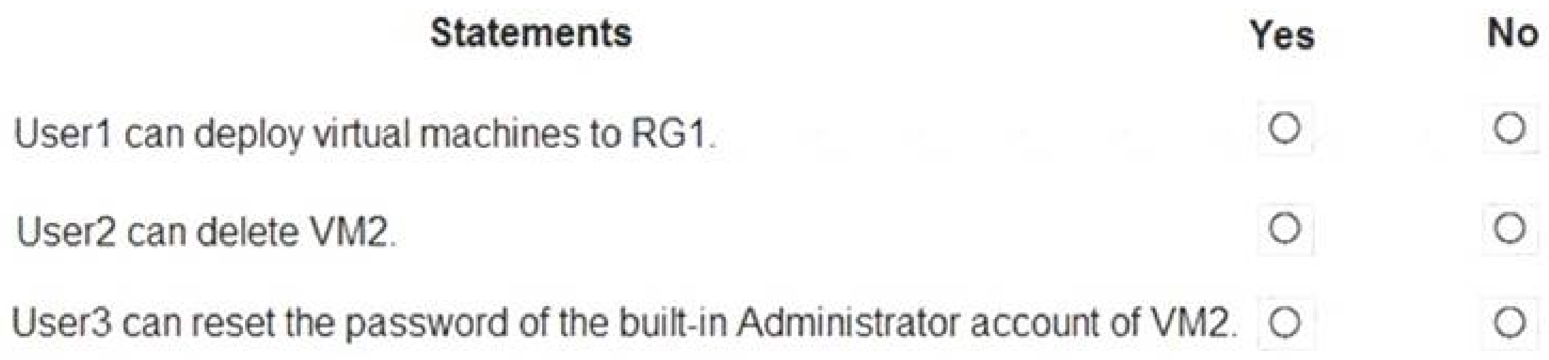


RG1, RG2, and RG3 are resource groups. RG2 contains a virtual machine named VM1.
You assign role-based access control (RBAC) roles to the users shown in the following table.



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.

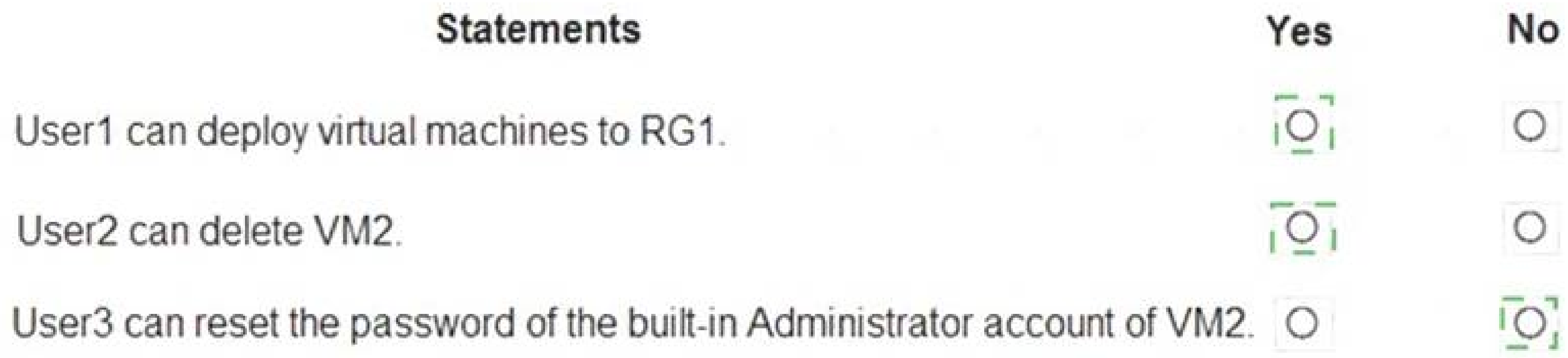


Statements	Yes	No
User1 can deploy virtual machines to RG1.	○	○
User2 can delete VM2.	○	○
User3 can reset the password of the built-in Administrator account of VM2.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:



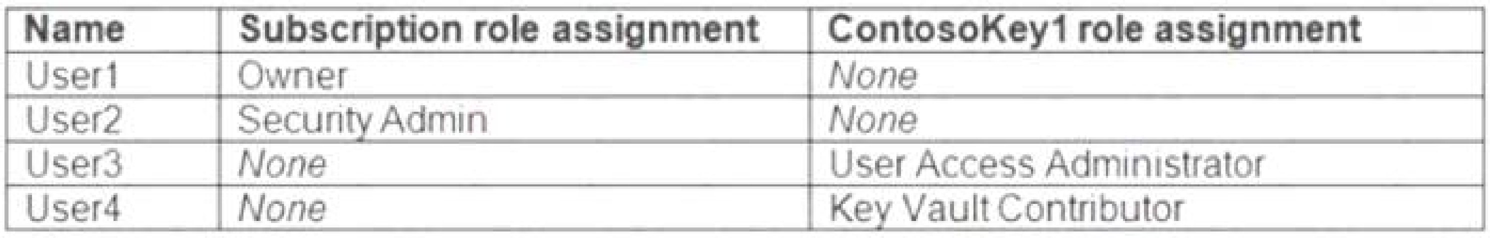
Statements	Yes	No
User1 can deploy virtual machines to RG1.	[✓ ○]	○
User2 can delete VM2.	[✓ ○]	○
User3 can reset the password of the built-in Administrator account of VM2.	○	[✓ ○]

NEW QUESTION 108
- (Exam Topic 4)
You have an Azure AD turned that contains a user named User1. You purchase an App named App1.
User1 needs to publish App1 by using Azure AD Application Proxy. Which role should you assign to User1?

A. Hybrid identity Administrator
B. Cloud App Security Administrator
C. Application Administrator
D. Cloud Application Administrate

Answer: C

NEW QUESTION 109
- (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.

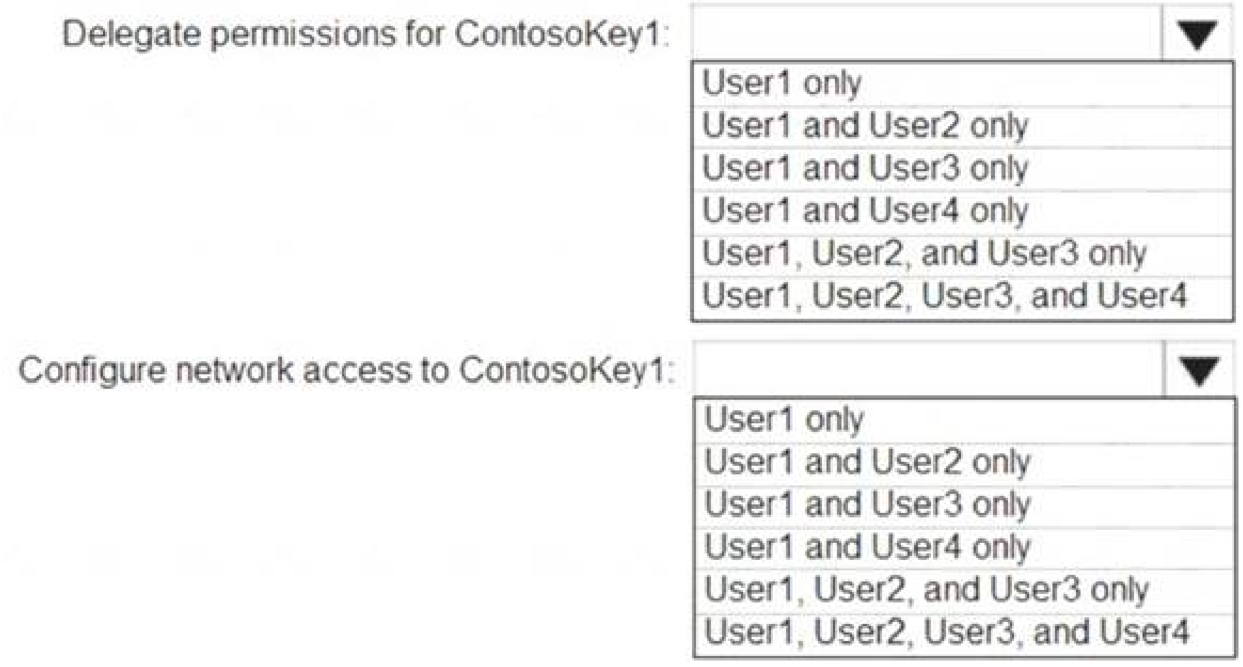


Name	Subscription role assignment	ContosoKey1 role assignment
User1	Owner	*None*
User2	Security Admin	*None*
User3	*None*	User Access Administrator
User4	*None*	Key Vault Contributor

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

- Delegate permissions for ContsosKey1.
- 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 111
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a hybrid configuration of Azure Active Directory (AzureAD). You have an Azure HDInsight cluster on a virtual network.
You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials. You need to configure the environment to support the planned authentication.
Solution: You create a site-to-site VPN between the virtual network and the on-premises network. Does this meet the goal?

A. Yes
B. No

Answer: A

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

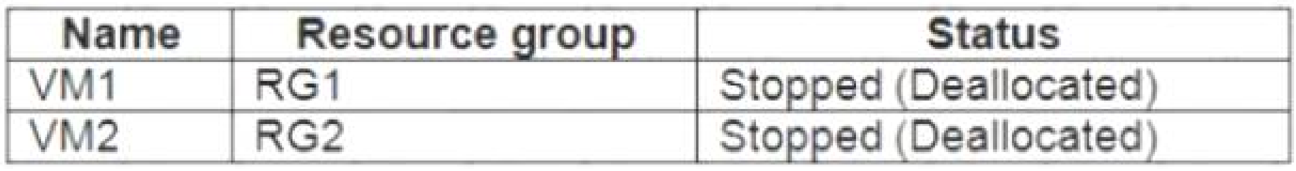
NEW QUESTION 115
- (Exam Topic 4)
You have an Azure subscription that contains a web app named App1.
Users must be able to select between a Google identity or a Microsoft identity when authenticating to App1. You need to add Google as an identity provider in Azure AD.
Which two pieces of information should you configure? Each correct answer presents part of the solution. Each correct selection is worth one point

A. a tenant name
B. a tenant ID
C. the endpoint URL Of an application
D. a client ID
E. a client secret

Answer: DE

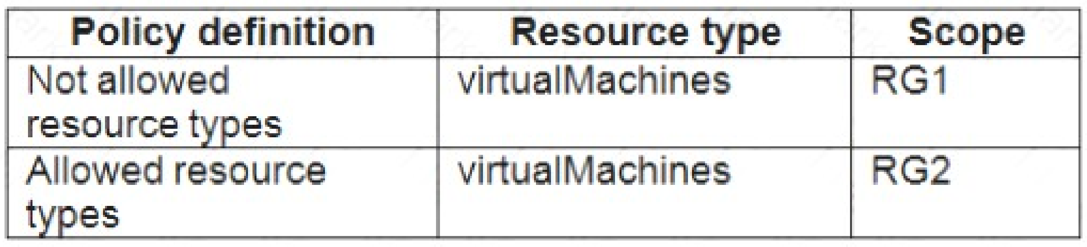
Explanation:
https://learn.microsoft.com/en-us/azure/app-service/configure-authentication-provider-google

NEW QUESTION 118
- (Exam Topic 4)
You have an Azure subscription that contains the virtual machines shown in the following table.



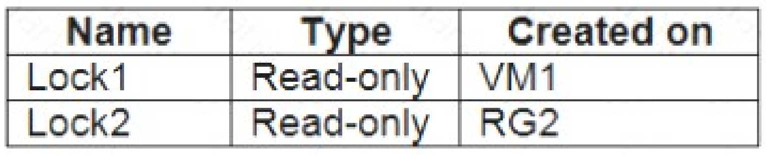
Name	Resource group	Status
VM1	RG1	Stopped (Deallocated)
VM2	RG2	Stopped (Deallocated)

You create the Azure policies shown in the following table.



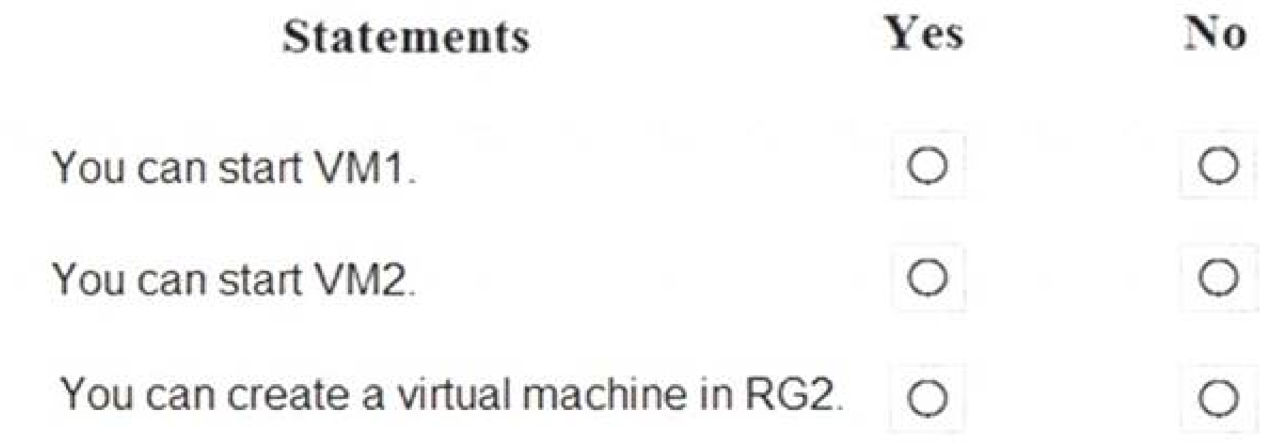
Policy definition	Resource type	Scope
Not allowed resource types	virtualMachines	RG1
Allowed resource types	virtualMachines	RG2

You create the resource locks shown in the following table.



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

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



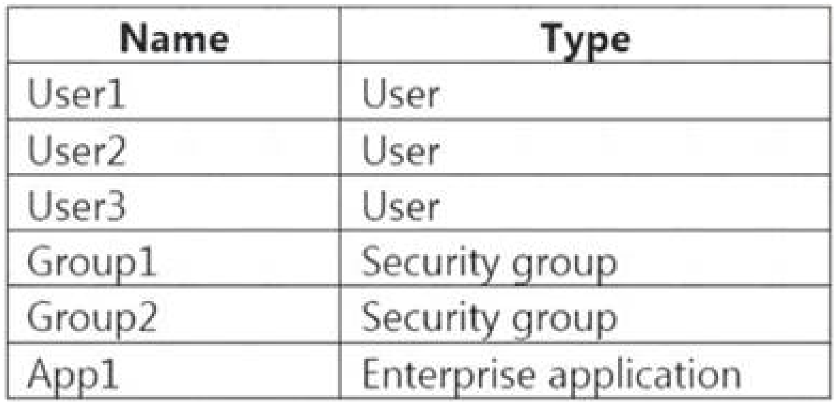
Statements	Yes	No
You can start VM1.	○	○
You can start VM2.	○	○
You can create a virtual machine in RG2.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
NO NO NO
1) cannot perform write operation because following scope(s) are locked: 'subscriptions/xxxx/resourceGroups/xxx' Please remove the lock and try again.
2) When creating a VM in a resource group with a Read Only lock an error is shown: "The selected resource group is read only"
3) Because of the read only lock virtual machines cannot be started nor stopped when the lock is added after the machine started. (not part of this use case, but still good to know.
The article referenced in the answer states different because that is scoped to blueprints.
In the Lock Resources pages is states the following regarding starting VMs:
"A ReadOnly lock on a resource group that contains a virtual machine prevents all users from starting or restarting the virtual machine. These operations require a POST request."
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

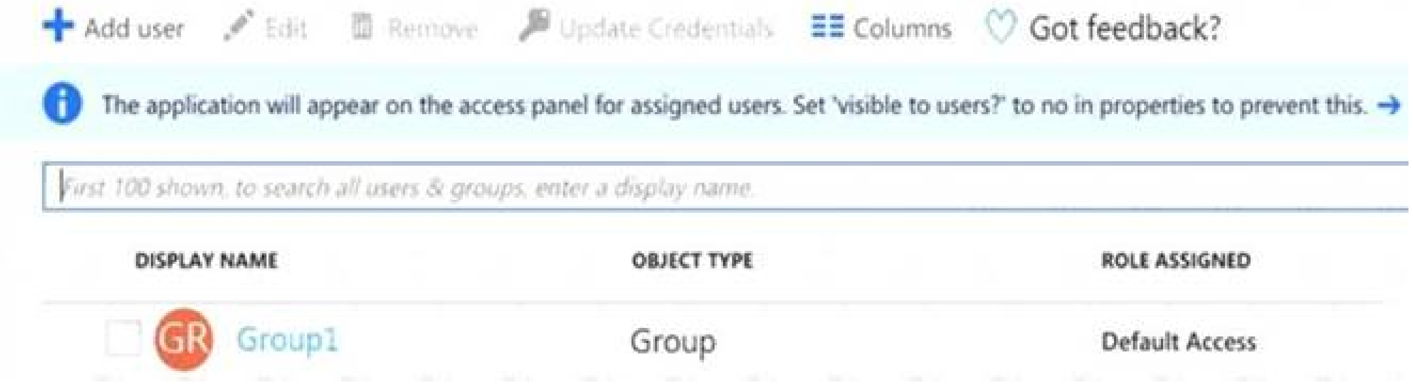
NEW QUESTION 123
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains the resources shown in the following table.



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.

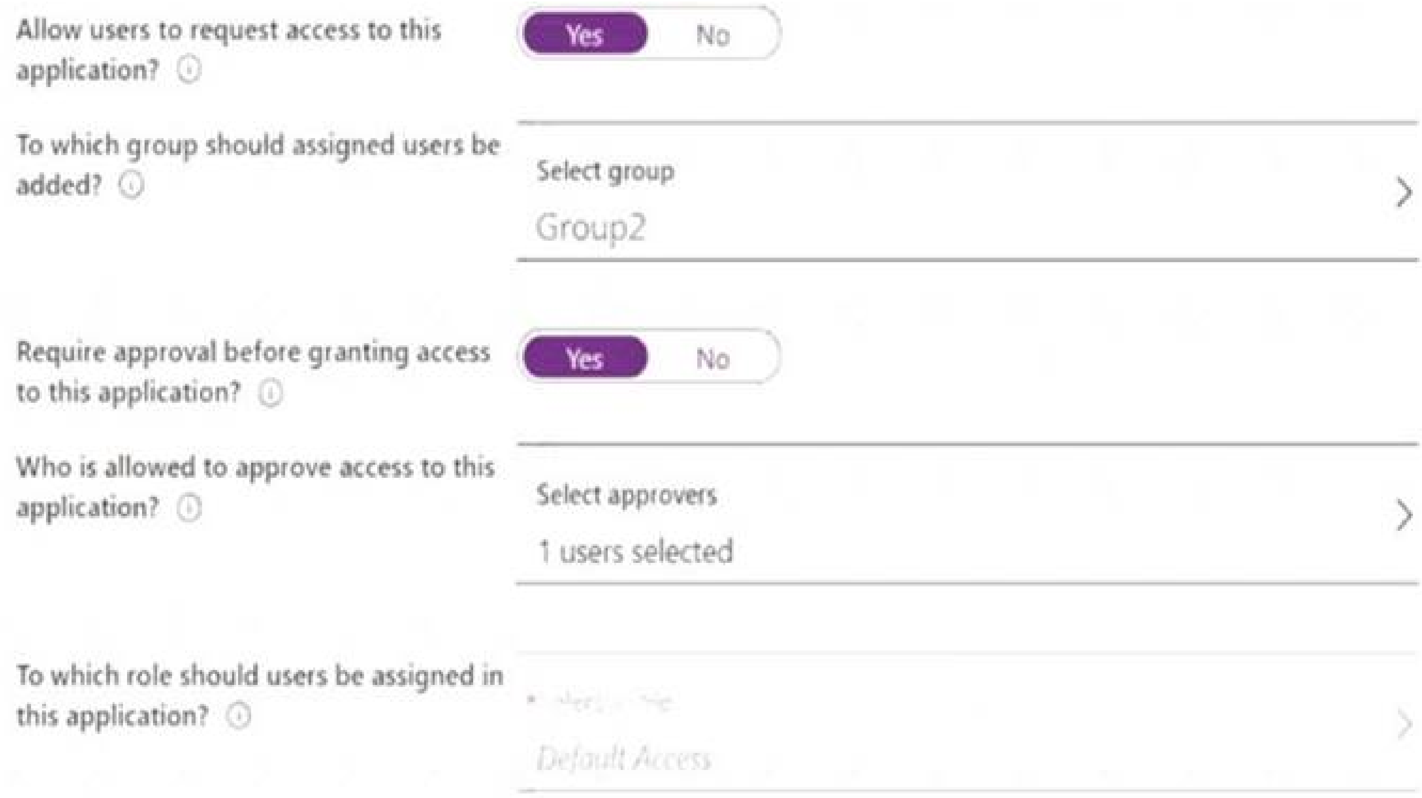


The application will appear on the access panel for assigned users. Set 'visible to users?' to no in properties to prevent this.

First 100 shown, to search all users & groups, enter a display name.

DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
GR Group1	Group	Default Access

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



Allow users to request access to this application? Yes [✓ 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

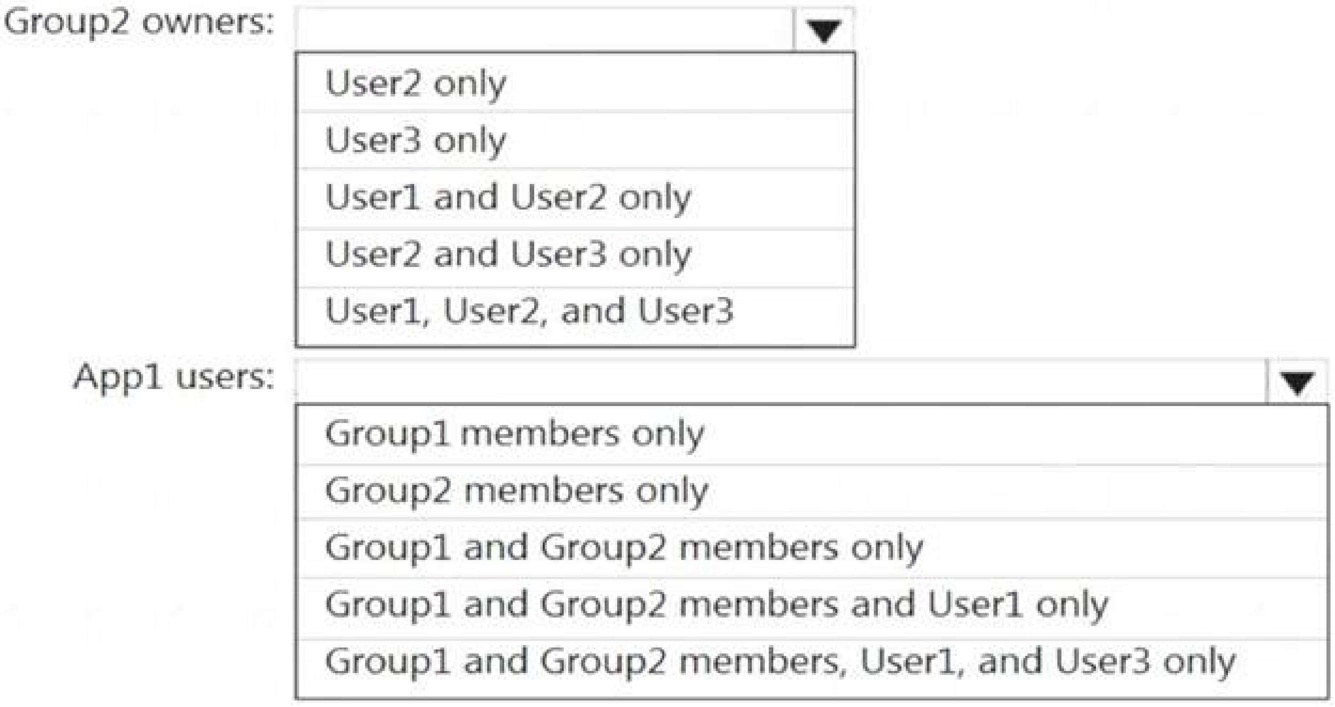
To which role should users be assigned in this application? [illegible] Default Access

User3 is configured to approve access to Appl.

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

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

NOTE: Each correct selection is worth one point.



Group2 owners:
- User2 only
- User3 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

App1 users:
- Group1 members only
- Group2 members only
- Group1 and Group2 members only
- Group1 and Group2 members and User1 only
- Group1 and Group2 members, User1, and User3 only

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 124
- (Exam Topic 4)
You are troubleshooting a security issue for an Azure Storage account You enable Azure Storage Analytics logs and archive It to a storage account. What should you use to retrieve the diagnostics logs?

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

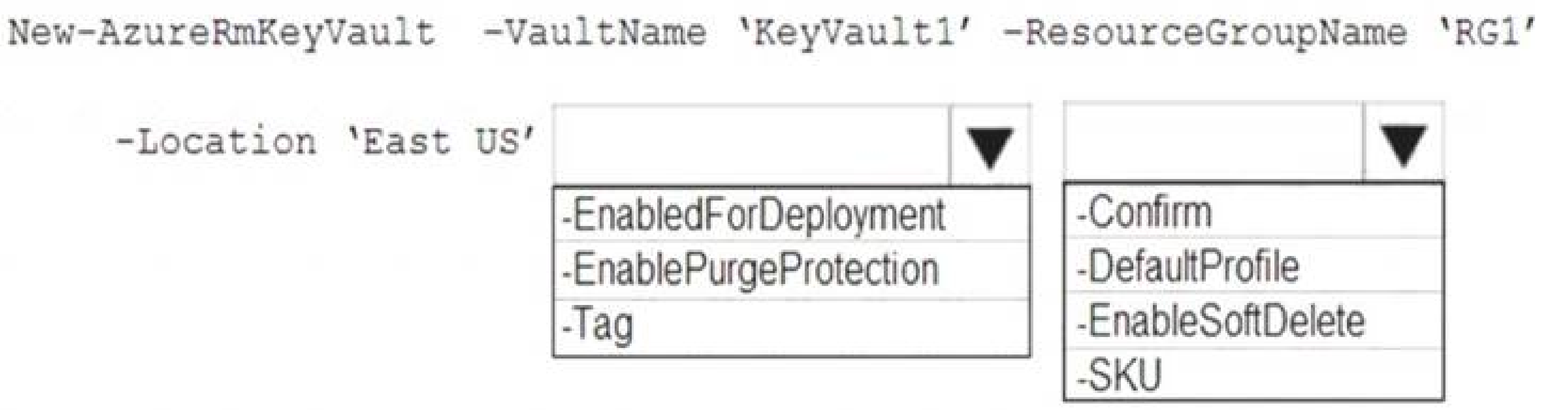
Answer: A

NEW QUESTION 128
- (Exam Topic 4)
You have an Azure subscription that contains an Azure Data Lake Storage Gen2 account named storage1. You deploy an Azure Synapse Analytics workspace named synapsews1 to a managed virtual network. You need to enable access from synapsews1 to storage1. What should you configure?

A. a virtual network gateway
B. a network security group (NSG)
C. a private endpoint
D. peering

Answer: C

NEW QUESTION 130
- (Exam Topic 4)
You need to create an Azure key vault. The solution must ensure that any object deleted from the key vault be retained for 90 days.
How should you complete the command? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



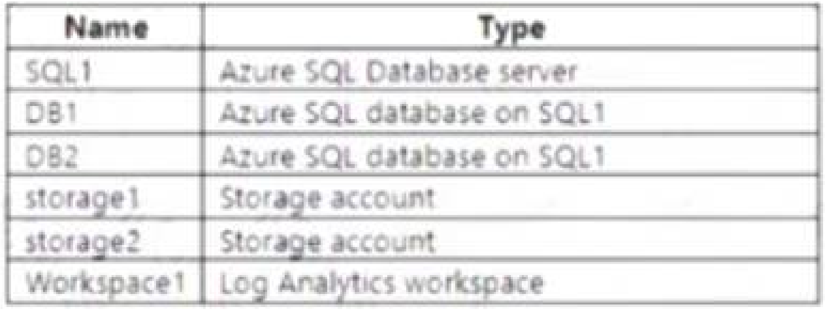
```
New-AzureRmKeyVault  -VaultName 'KeyVault1' -ResourceGroupName 'RG1'

    -Location 'East US'
```

A. Mastered
B. Not Mastered

Answer: A

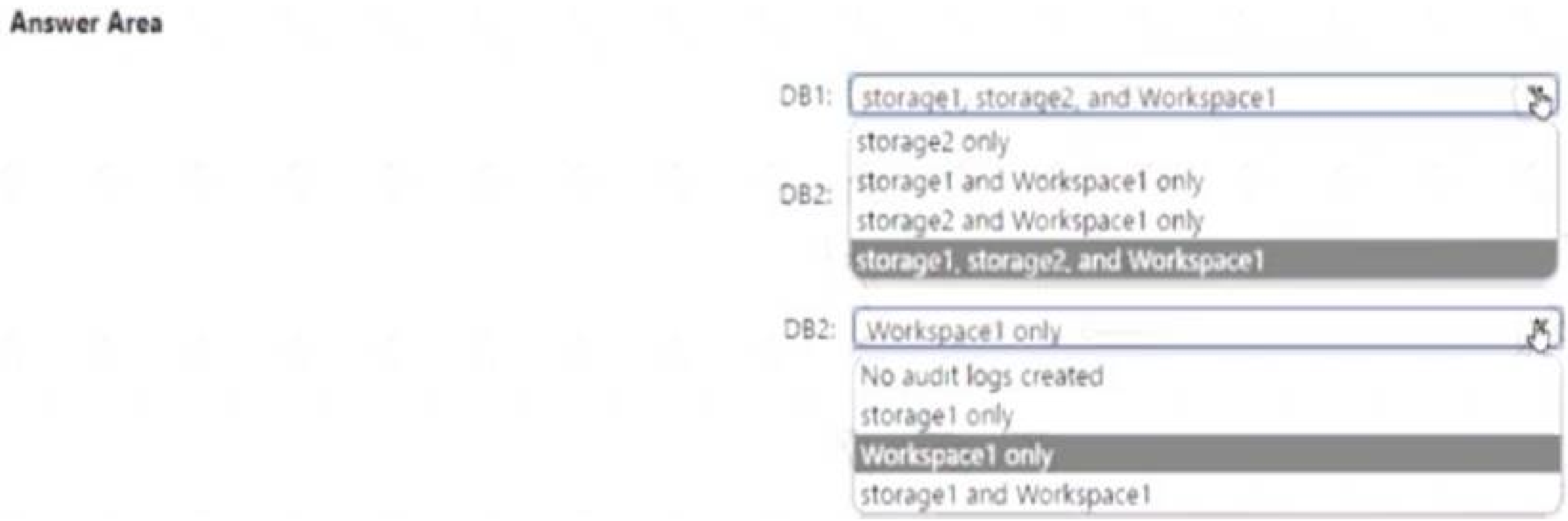
Explanation:
Box 1: -EnablePurgeProtection
If specified, protection against immediate deletion is enabled for this vault; requires soft delete to be enabled as well.
Box 2: -EnableSoftDelete
Specifies that the soft-delete functionality is enabled for this key vault. When soft-delete is enabled, for a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

NEW QUESTION 134
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.



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

SQL1 has the following configurations:
• Auditing: Enabled
• Audit log destination: storage1, Workspace1 DB1 has the following configurations:
• Auditing: Enabled
• Audit log destination: storage2 DB2 has auditing disabled.
Where are the audit logs for DB1 and DB2 stored? To answer, select the appropriate options in the answer area
NOTE: Each correct selection is worth one point.



Answer Area

DB1: storage1, storage2, and Workspace1
- storage2 only
- storage1 and Workspace1 only
- storage2 and Workspace1 only
- storage1, storage2, and Workspace1

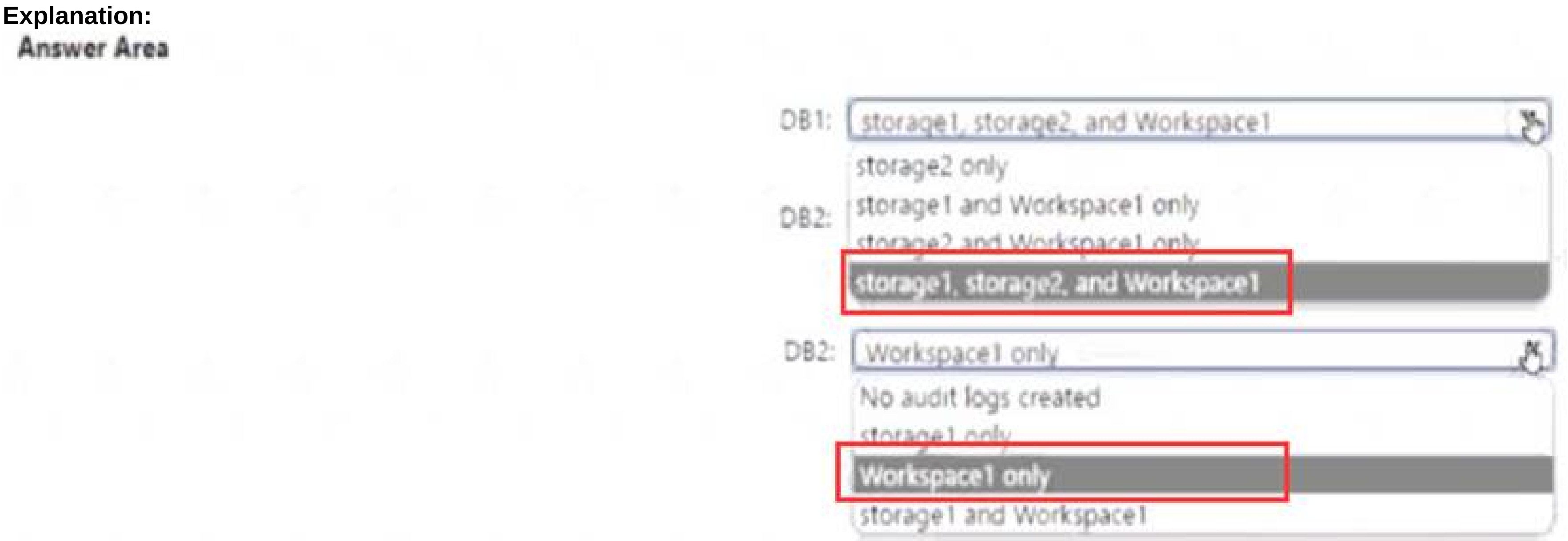
DB2:

DB2: Workspace1 only
- No audit logs created
- storage1 only
- Workspace1 only
- storage1 and Workspace1

A. Mastered
B. Not Mastered

Answer: A

Explanation:



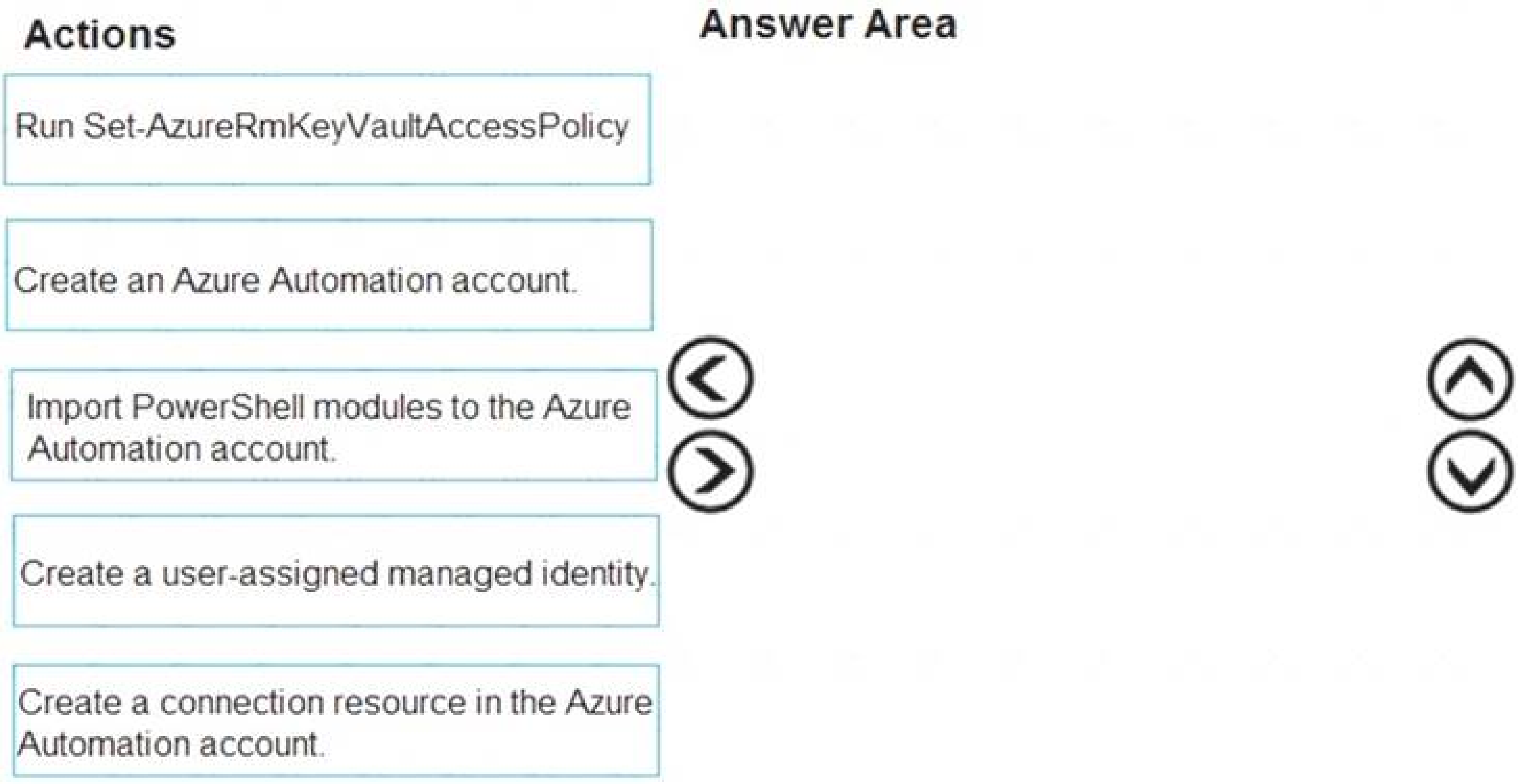
Answer Area

DB1: storage1, storage2, and Workspace1
- storage2 only
- storage1 and Workspace1 only
- storage2 and Workspace1 only
- storage1, storage2, and Workspace1

DB2:

DB2: Workspace1 only
- No audit logs created
- storage1 only
- Workspace1 only
- storage1 and Workspace1

NEW QUESTION 135
- (Exam Topic 4)
You have an Azure subscription named Sub1 that contains an Azure Storage account named Contosostorage1 and an Azure key vault named Contosokeyvault1.
You plan to create an Azure Automation runbook that will rotate the keys of Contosostorage1 and store them in Contosokeyvault1.
You need to implement prerequisites to ensure that you can implement the runbook.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Actions

- Run Set-AzureRmKeyVaultAccessPolicy
- Create an Azure Automation account.
- Import PowerShell modules to the Azure Automation account.
- Create a user-assigned managed identity.
- Create a connection resource in the Azure Automation account.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Step 1: Create an Azure Automation account

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

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

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

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

References:

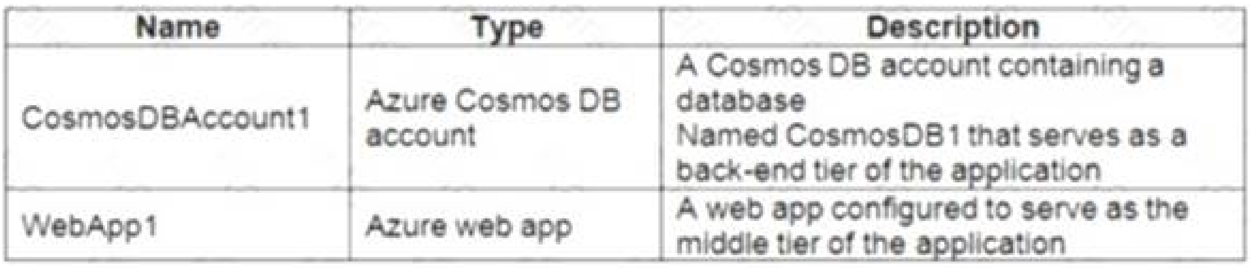
https://www.rahulpnath.com/blog/accessing-azure-key-vault-from-azure-runbook/

NEW QUESTION 137

- (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.



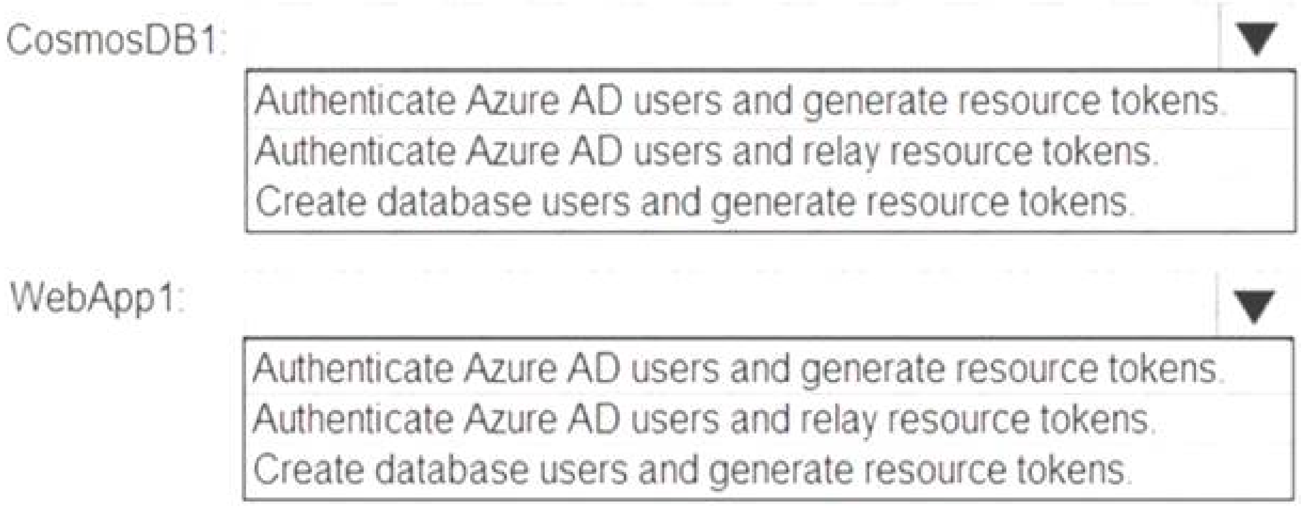
Name	Type	Description
CosmosDBAccount1	Azure Cosmos DB account	A Cosmos DB account containing a database Named CosmosDB1 that serves as a back-end tier of the application
WebApp1	Azure web app	A web app configured to serve as the middle tier of the application

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

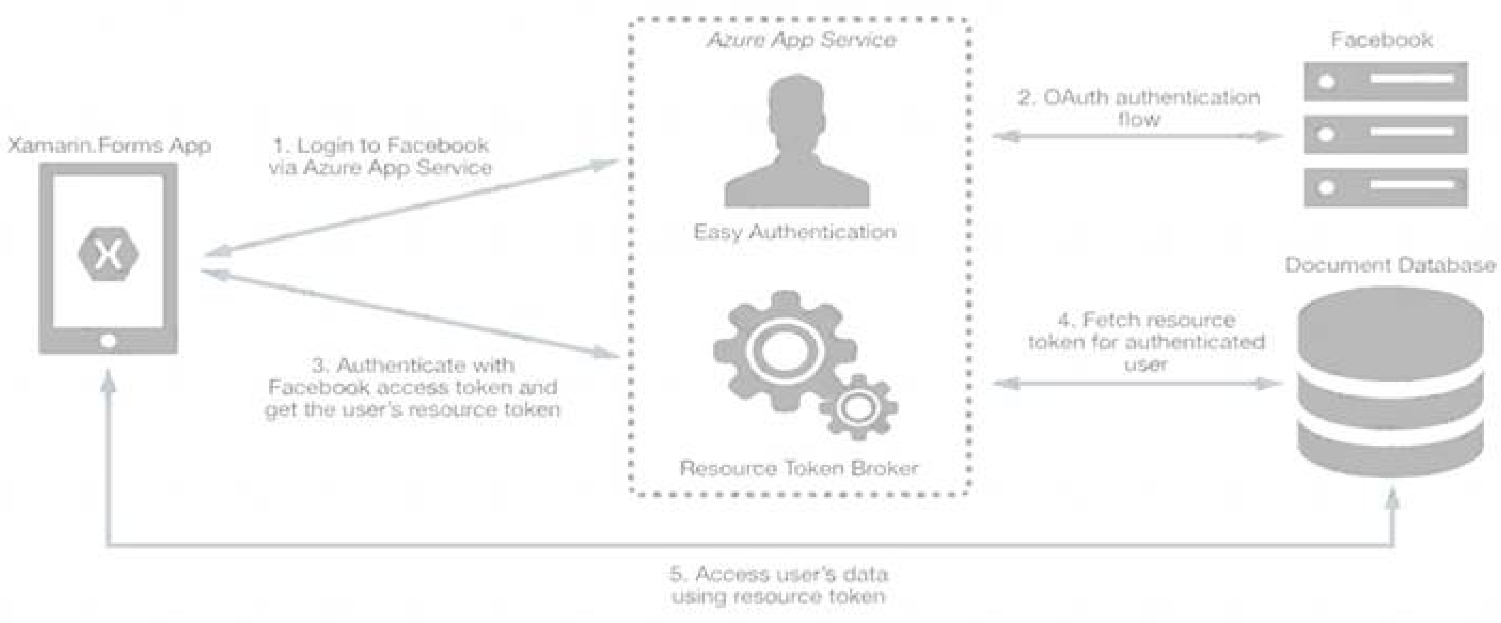
Explanation:

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.

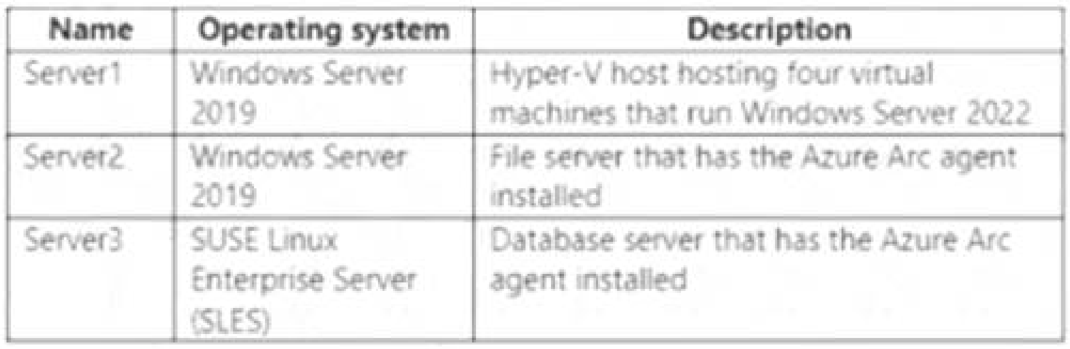
WebApp1: Authenticate Azure AD users and relay resource tokens

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:


Azure App Service
Facebook
2. OAuth authentication flow
Xamarin.Forms App
1. Login to Facebook via Azure App Service
Easy Authentication
Document Database
4. Fetch resource token for authenticated user
3. Authenticate with Facebook access token and get the user's resource token
Resource Token Broker
5. Access user's data using resource token

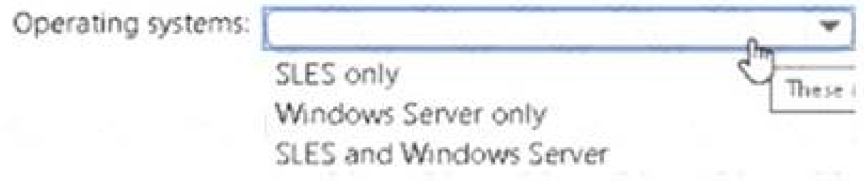
References:
https://docs.microsoft.com/en-us/xamarin/xamarin-forms/data-cloud/cosmosdb/authentication

NEW QUESTION 142
- (Exam Topic 4)
Your on-premises network contains the servers shown in the following table.

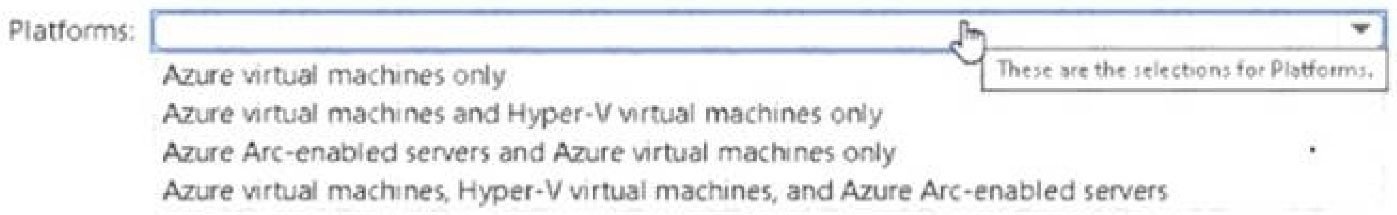


Name	Operating system	Description
Server1	Windows Server 2019	Hyper-V host hosting four virtual machines that run Windows Server 2022
Server2	Windows Server 2019	File server that has the Azure Arc agent installed
Server3	SUSE Linux Enterprise Server (SLES)	Database server that has the Azure Arc agent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

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



Operating systems:
SLES only
Windows Server only
SLES and Windows Server

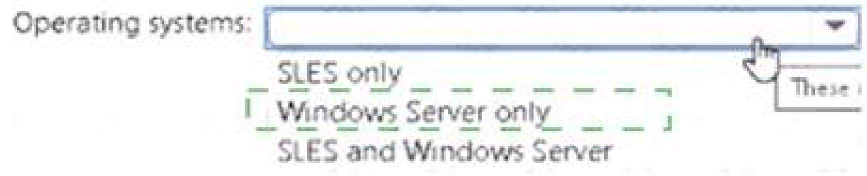


Platforms:
Azure virtual machines only
Azure virtual machines and Hyper-V virtual machines only
Azure Arc-enabled servers and Azure virtual machines only
Azure virtual machines, Hyper-V virtual machines, and Azure Arc-enabled servers

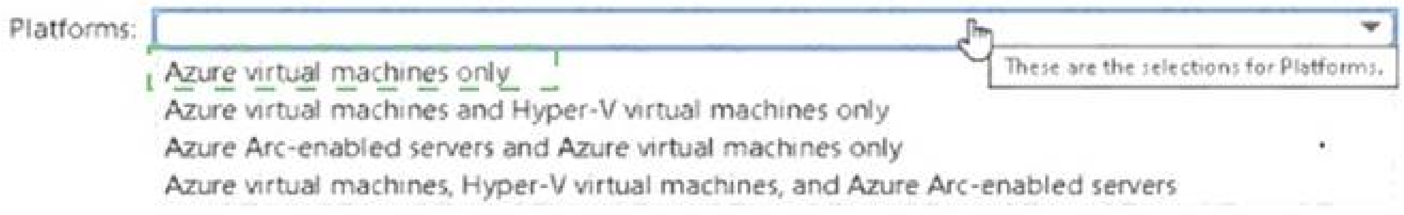
A. Mastered
B. Not Mastered

Answer: A

Explanation:



Operating systems:
SLES only
[✓ Windows Server only]
SLES and Windows Server



Platforms:
[✓ Azure virtual machines only]
Azure virtual machines and Hyper-V virtual machines only
Azure Arc-enabled servers and Azure virtual machines only
Azure virtual machines, Hyper-V virtual machines, and Azure Arc-enabled servers

NEW QUESTION 143
- (Exam Topic 4)
Your network contains an on-premises Active Directory domain named corp.contoso.com.
You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
You sync all on-premises identities to Azure AD.
You need to prevent users who have a givenName attribute that starts with TEST from being synced to Azure AD. The solution must minimize administrative effort.
What should you use?

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

Answer: A

Explanation:
Use the Synchronization Rules Editor and write attribute-based filtering rule. References:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration

NEW QUESTION 146
- (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: Userl -28681041@ExamUsers.com
Azure Password: GpOAe4@lDg
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 adminl@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 adminl@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 147
- (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 152
- (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

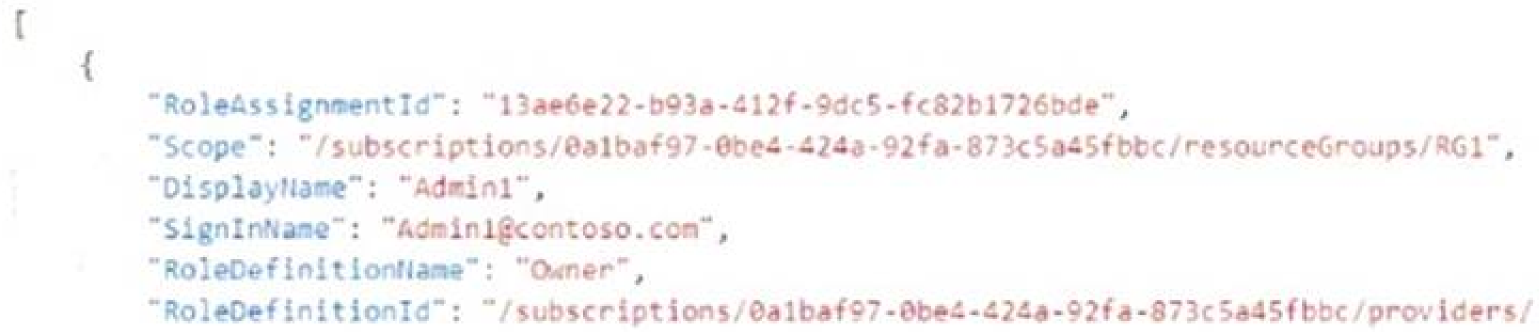
NEW QUESTION 157
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com. The User administrator role is assigned to a user named Admin1.
An external partner has a Microsoft account that uses the user1@outlook.com sign in.
Admin1 attempts to invite the external 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

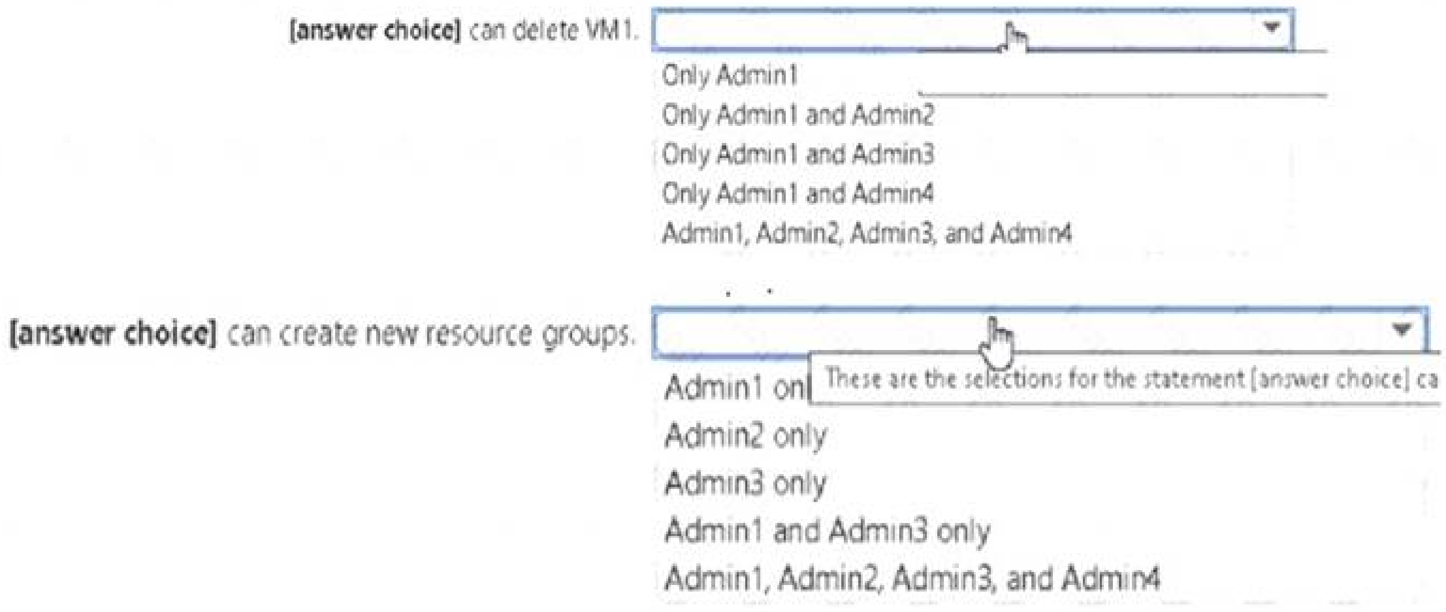
Explanation:
You need to allow guest invitations in the External collaboration settings.

NEW QUESTION 158
- (Exam Topic 4)
You have the role assignments shown in the following exhibit.



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

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



[answer choice] can delete VM1.
- Only Admin1
- Only Admin1 and Admin2
- Only Admin1 and Admin3
- Only Admin1 and Admin4
- Admin1, Admin2, Admin3, and Admin4

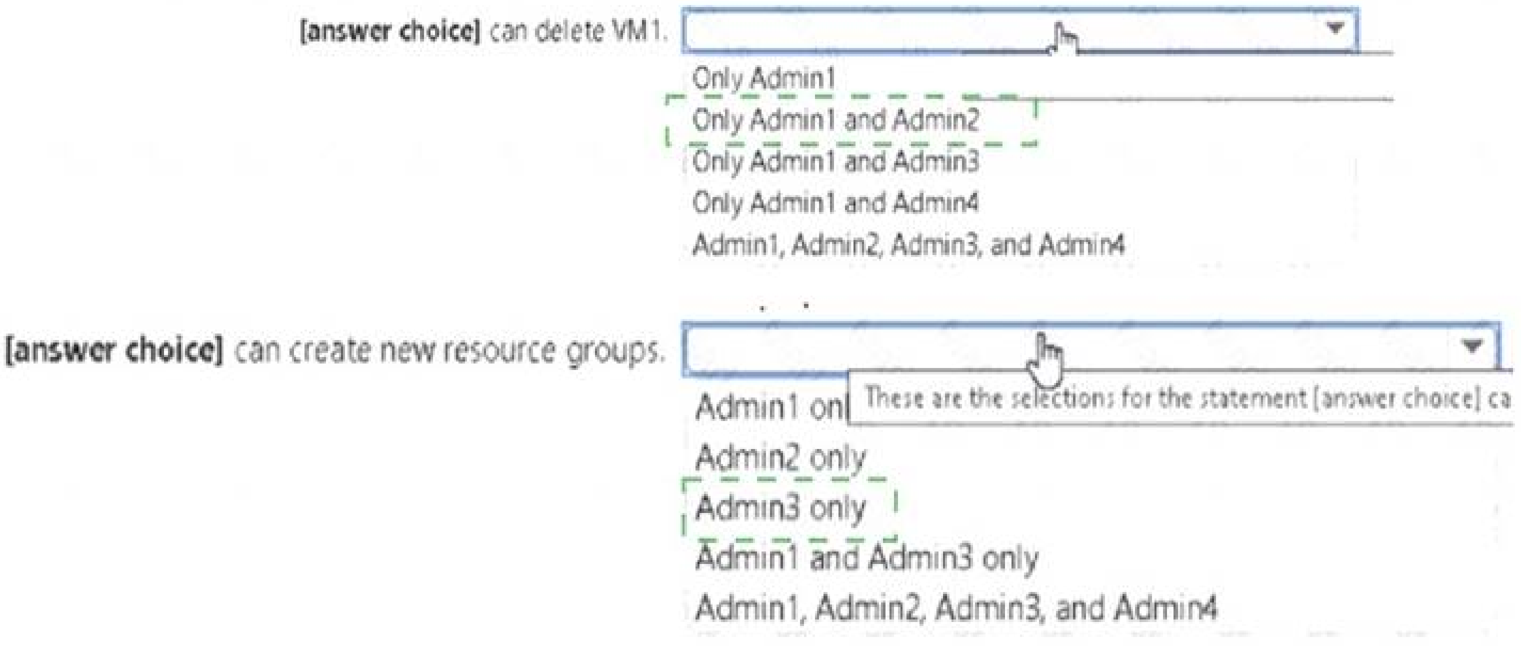
[answer choice] can create new resource groups.
- Admin1 onl
- Admin2 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, Admin3, and Admin4

These are the selections for the statement [answer choice] ca

A. Mastered
B. Not Mastered

Answer: A

Explanation:



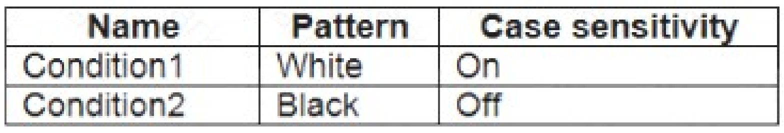
[answer choice] can delete VM1.

- Only Admin1
- Only Admin1 and Admin2
- Only Admin1 and Admin3
- Only Admin1 and Admin4
- Admin1, Admin2, Admin3, and Admin4

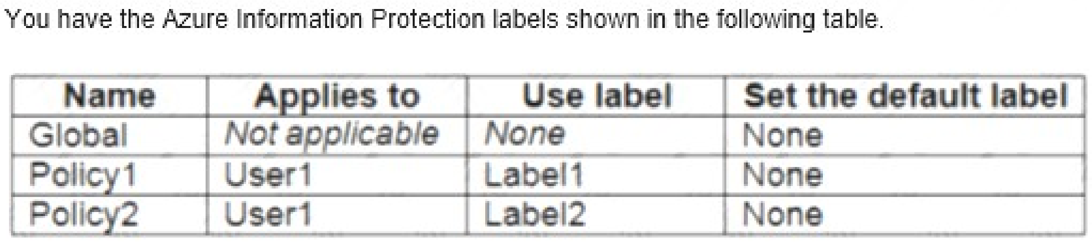
[answer choice] can create new resource groups.

- Admin1 onl These are the selections for the statement [answer choice] ca
- Admin2 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, Admin3, and Admin4

NEW QUESTION 162
- (Exam Topic 4)
You have the Azure Information Protection conditions shown in the following table.



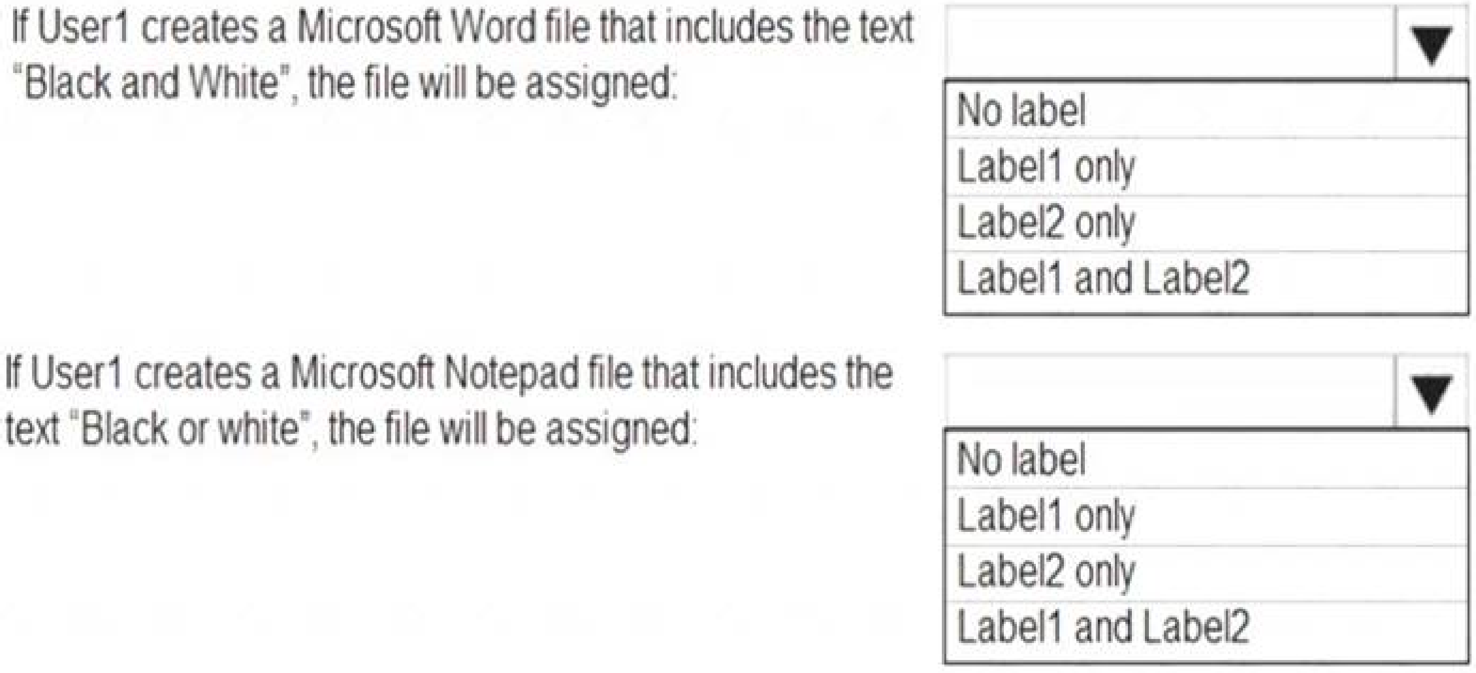
Name	Pattern	Case sensitivity
Condition1	White	On
Condition2	Black	Off



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

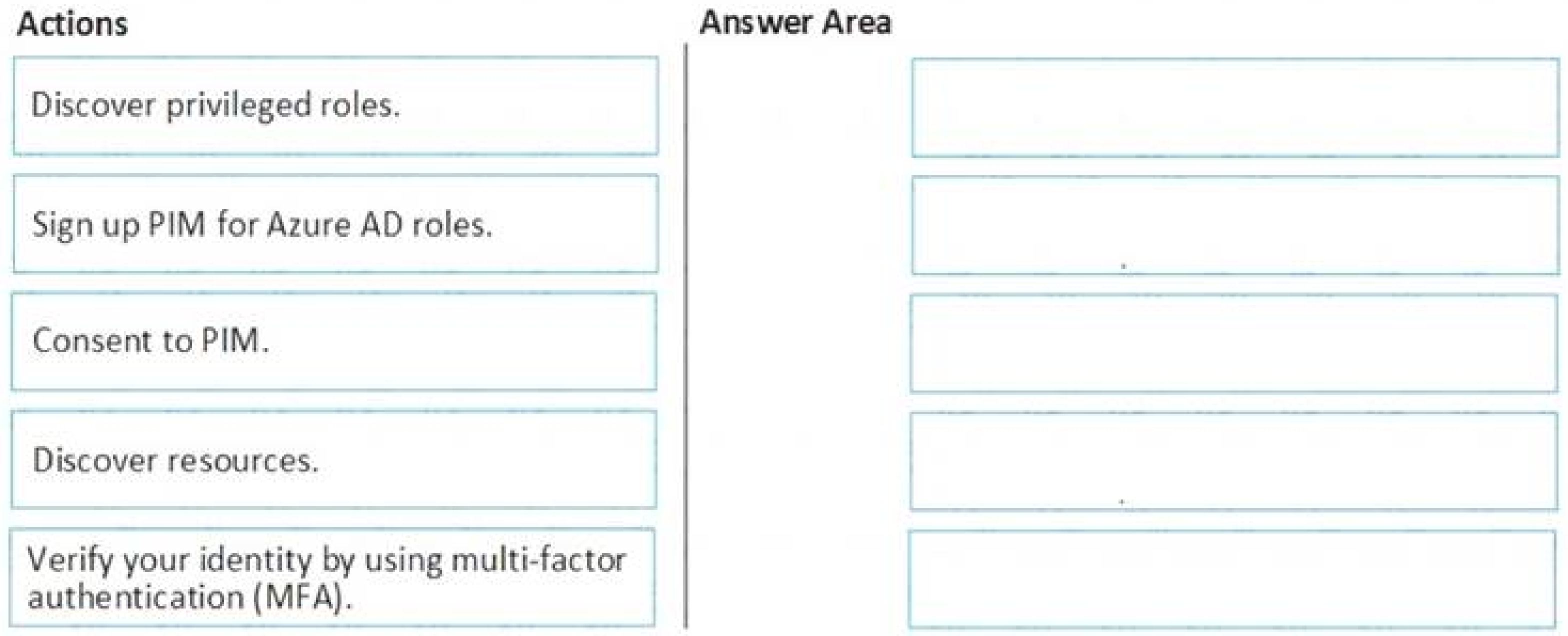
Explanation:
Box 1: Label 2 only
How multiple conditions are evaluated when they apply to more than one label

- 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 163

- (Exam Topic 4)
You create an Azure subscription with Azure AD Premium P2.
You need to ensure that you can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to secure Azure roles.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Actions

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

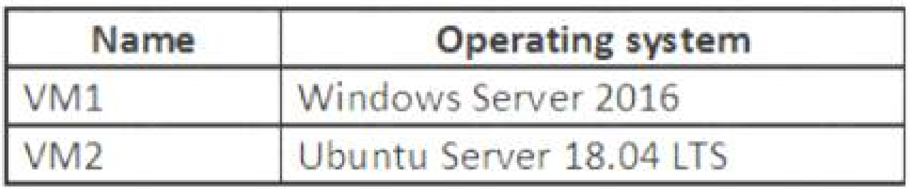
Answer Area

A. Mastered
B. Not Mastered

Answer: A

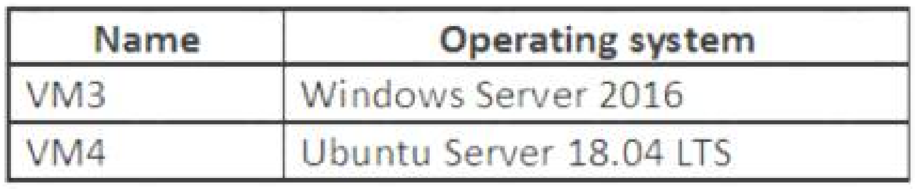
Explanation:
* 1. Verify your identity with MFA
* 2. Consent to PIM
* 3. Sign up PIM for AAD Roles

NEW QUESTION 168
- (Exam Topic 4)
You have an Azure subscription that contains the virtual machines shown in the following table.



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

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



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

On which virtual machines is the Microsoft Monitoring agent installed?

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

Answer: D

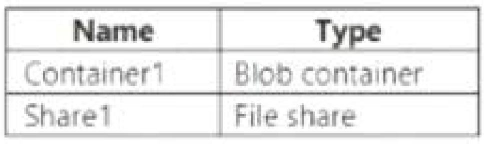
Explanation:
When automatic provisioning is enabled, Security Center provisions the Microsoft Monitoring Agent on all supported Azure VMs and any new ones that are created.
Supported Operating systems include: Ubuntu 14.04 LTS (x86/x64), 16.04 LTS (x86/x64), and 18.04 LTS (x64) and Windows Server 2008 R2, 2012, 2012 R2, 2016, version 1709 and 1803.
References:
https://docs.microsoft.com/en-us/azure/security-center/security-center-faq

NEW QUESTION 172
- (Exam Topic 4)
You have an Azure subscription that contains a user named UseR1. You need to ensure that UseR1 can perform the following tasks:
• Create groups.
• Create access reviews for role-assignable groups.
• Assign Azure AD roles to groups.
The solution must use the principle of least privilege. Which role should you assign to User1?

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

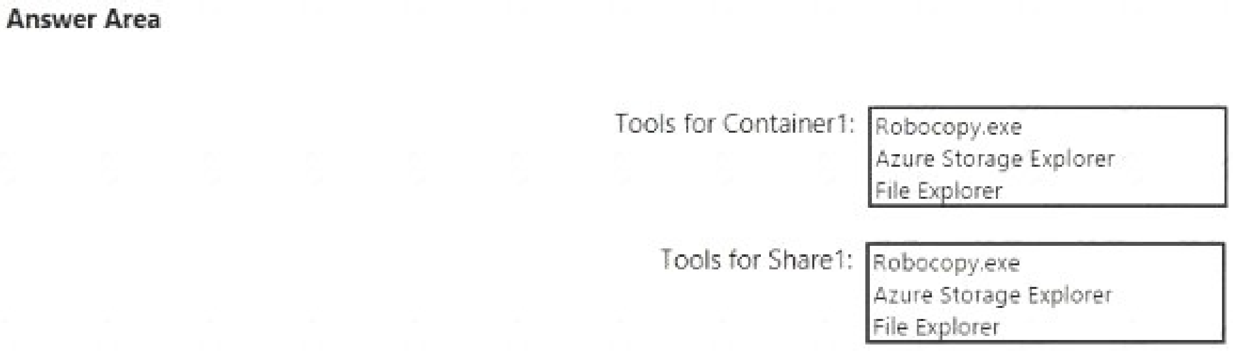
Answer: C

NEW QUESTION 174
- (Exam Topic 4)
You have an Azure subscription named Sub1. Sub1 has an Azure Storage account named Storage1 that contains the resources shown in the following table.



Name	Type
Container1	Blob container
Share1	File share

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



Answer Area

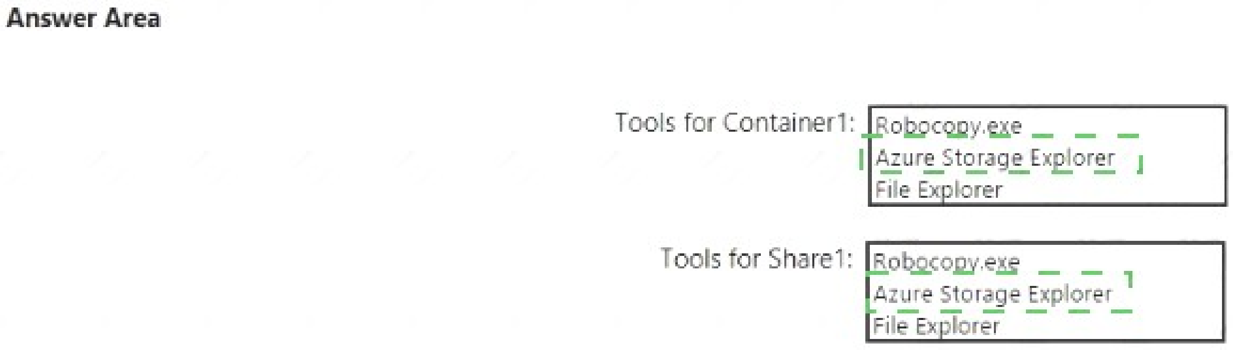
Tools for Container1:
Robocopy.exe
Azure Storage Explorer
File Explorer

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Tools for Container1:
Robocopy.exe
[✓ Azure Storage Explorer]
File Explorer

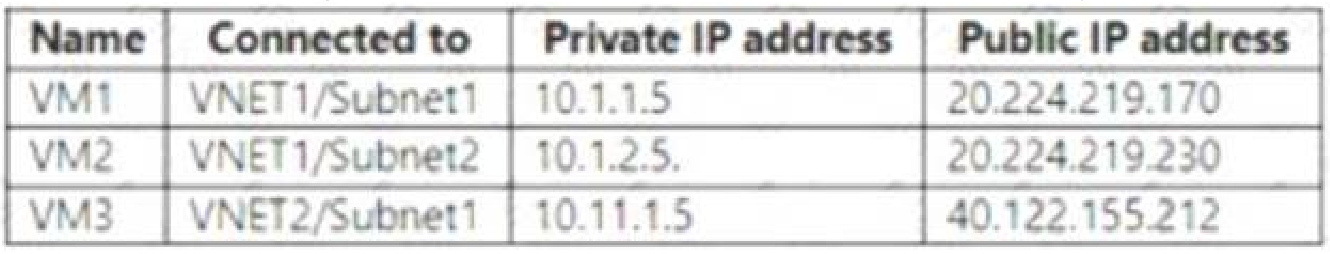
Tools for Share1:
Robocopy.exe
[✓ Azure Storage Explorer]
File Explorer

NEW QUESTION 176
- (Exam Topic 4)
You have an Azure subscription.
You need to deploy an Azure virtual WAN to meet the following requirements:
• Create three secured virtual hubs located in the East US, West US, and North Europe Azure regions.
• Ensure that security rules sync between the regions. What should you use?

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

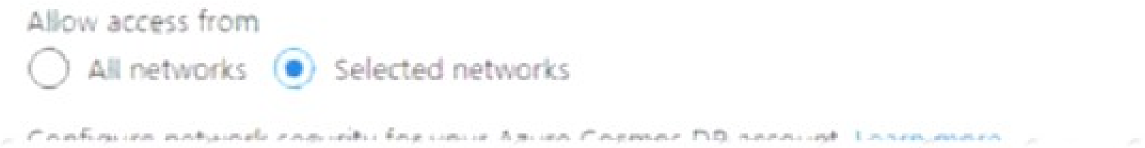
Answer: A

NEW QUESTION 180
- (Exam Topic 4)
You have an Azure subscription that contains the virtual machines shown in the following table.



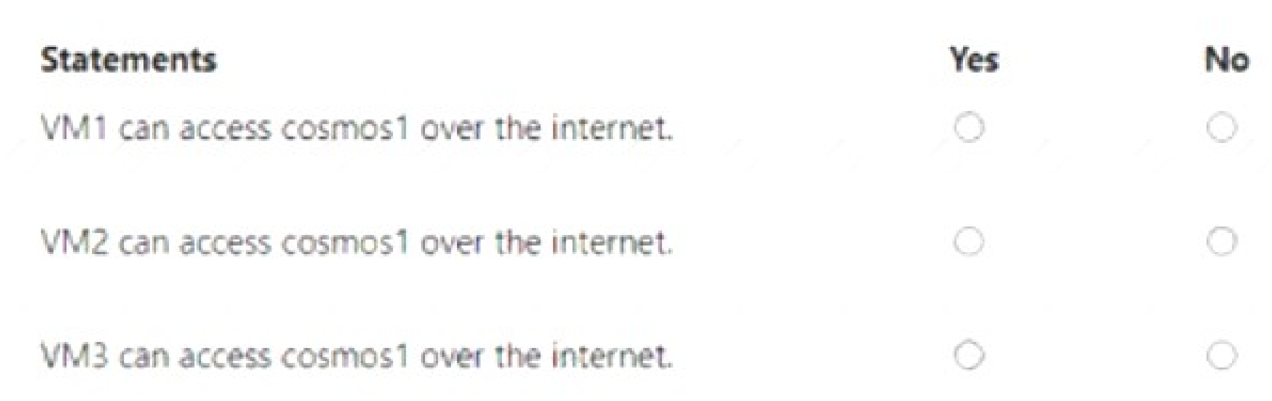
Name	Connected to	Private IP address	Public IP address
VM1	VNET1/Subnet1	10.1.1.5	20.224.219.170
VM2	VNET1/Subnet2	10.1.2.5.	20.224.219.230
VM3	VNET2/Subnet1	10.11.1.5	40.122.155.212

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.	○	○
VM2 can access cosmos1 over the internet.	○	○
VM3 can access cosmos1 over the internet.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Yes, Yes, No

NEW QUESTION 181
- (Exam Topic 4)
Lab Task
Task 7
You need to ensure that connections through an Azure Application Gateway named Homepage-AGW are inspected for malicious requests.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Enable Web Application Firewall (WAF) for the application gateway. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to select a WAF policy and a WAF mode for the application gateway. You can choose a predefined policy or create a custom policy with your own rules and exclusions.
Configure WAF policy settings. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to select the managed rulesets and rule groups that you want to enable or disable for the WAF policy. You can also configure custom rules to match specific patterns or conditions and take actions such as blocking or logging requests.
Monitor WAF logs. You can use different types of logs in Azure to manage and troubleshoot the application gateway and the WAF policy. You can access some of these logs through the portal, such as metrics and health probes. You can also export the logs to Azure Storage, Event Hubs, or Log Analytics and view them in different tools, such as Azure Monitor, Excel, or Power BI.

NEW QUESTION 183
- (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 187
- (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 189

- (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 create a new stored access policy. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Shared access signatures provides access to a particular resource such as blog. Stored access policies are a group of Shared Access Signatures (SAS). In order to revoke access to a SAS you can either:
* 1. Rotate the Key1 or Key 2, that is the access keys used to sign the SAS. Rotating the access keys used to sign the SAS, invalidates any previously signed SAS hence revoking the SAS issused before
* 2. Remove the stored access policy which an SAS is linked to. If a Stored Access Policy is removed, it also invalidates the SASs liked to the Stored Access Policy.

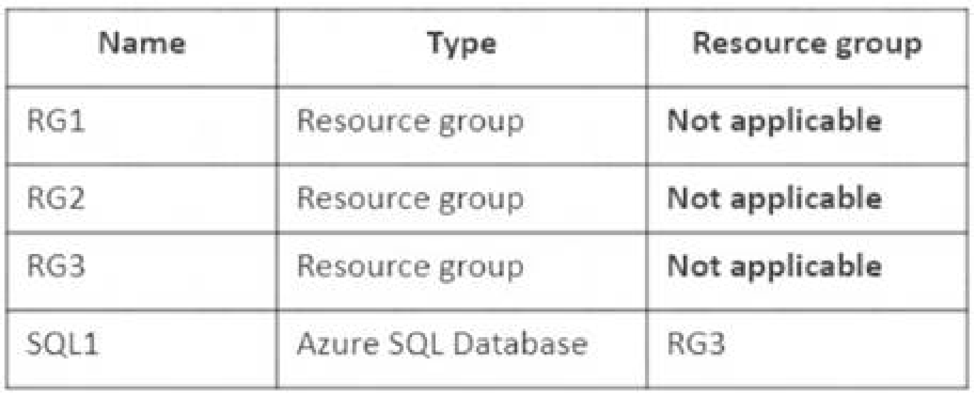
NEW QUESTION 191
- (Exam Topic 4)
You have an Azure subscription that contains a user named Adminl1 and a virtual machine named VM1. VM1 runs Windows Server 2019 and was deployed by using an Azure Resource Manager template. VM1 is the member of a backend pool of a public Azure Basic Load Balancer.
Admin1 reports that VM1 is listed as Unsupported on the Just in time VM access blade of Azure Security Center.
You need to ensure that Admin1 can enable just in time (JIT) VM access for VM1. What should you do?

A. Create and configure an additional public IP address for VM 1.
B. Replace the Basic Load Balancer with an Azure Standard Load Balancer.
C. Assign an Azure Active Directory Premium Plan 1 license to Admin1.
D. Create and configure a network security group (NSG).

Answer: D

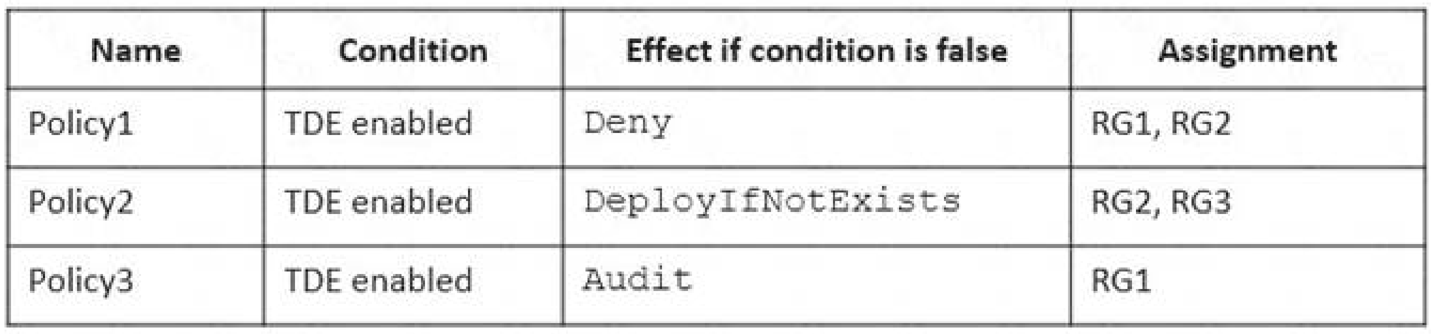
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time?tabs=jit-config-asc%2Cjit-re

NEW QUESTION 196
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.



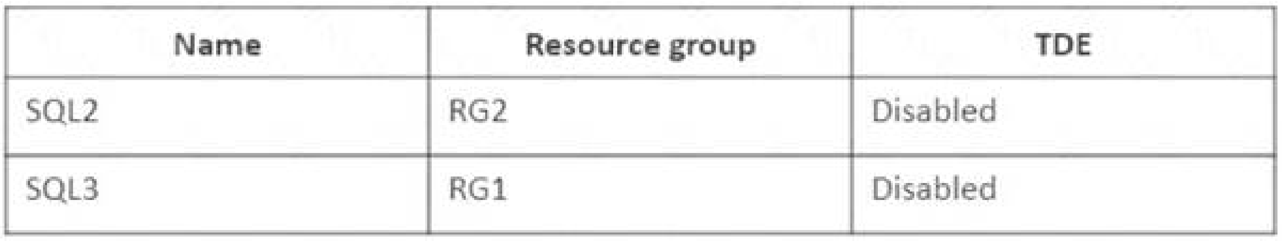
Name	Type	Resource group
RG1	Resource group	Not applicable
RG2	Resource group	Not applicable
RG3	Resource group	Not applicable
SQL1	Azure SQL Database	RG3

Transparent Data Encryption (TDE) is disabled on SQL1.
You assign policies to the resource groups as shown in the following table.



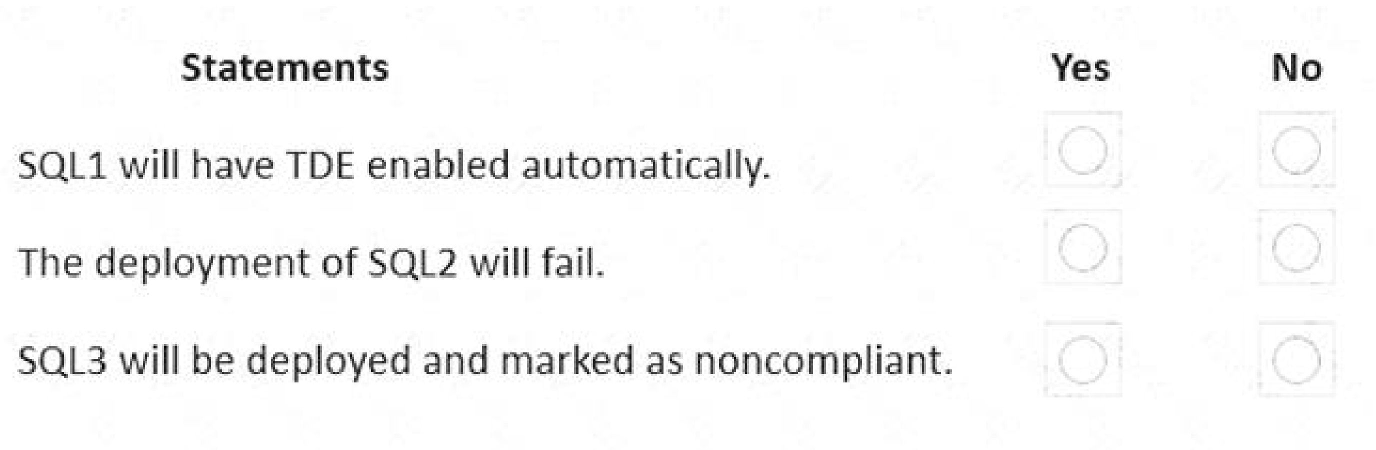
Name	Condition	Effect if condition is false	Assignment
Policy1	TDE enabled	Deny	RG1, RG2
Policy2	TDE enabled	DeployIfNotExists	RG2, RG3
Policy3	TDE enabled	Audit	RG1

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



Name	Resource group	TDE
SQL2	RG2	Disabled
SQL3	RG1	Disabled

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



Statements	Yes	No
SQL1 will have TDE enabled automatically.	○	○
The deployment of SQL2 will fail.	○	○
SQL3 will be deployed and marked as noncompliant.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

NEW QUESTION 201
- (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 203
- (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

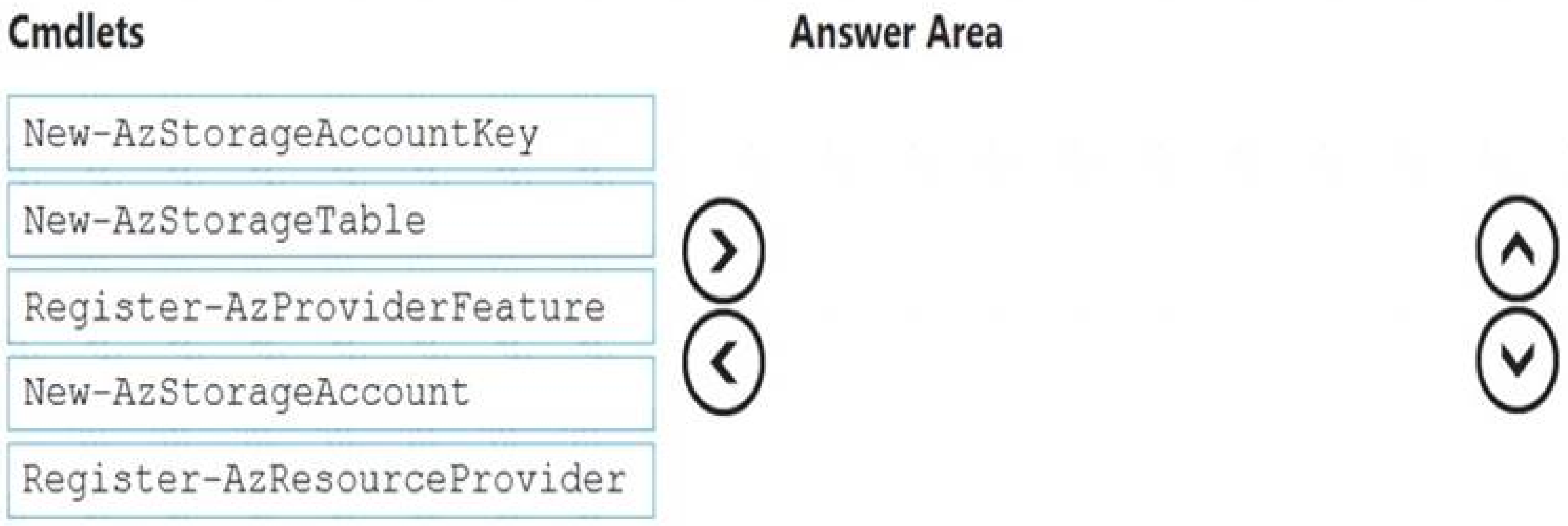
NEW QUESTION 205
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.
You need to ensure that User1 can create and manage administrative units. The solution must use the principle of least privilege.
Which role should you assign to User1?

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

Answer: A

NEW QUESTION 210
- (Exam Topic 4) You have an Azure subscription. You plan to create a storage account.
You need to use customer-managed keys to encrypt the tables in the storage account.
From Azure Cloud Shell, which three cmdlets should you run in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area

and arrange them in the correct order.



Cmdlets

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

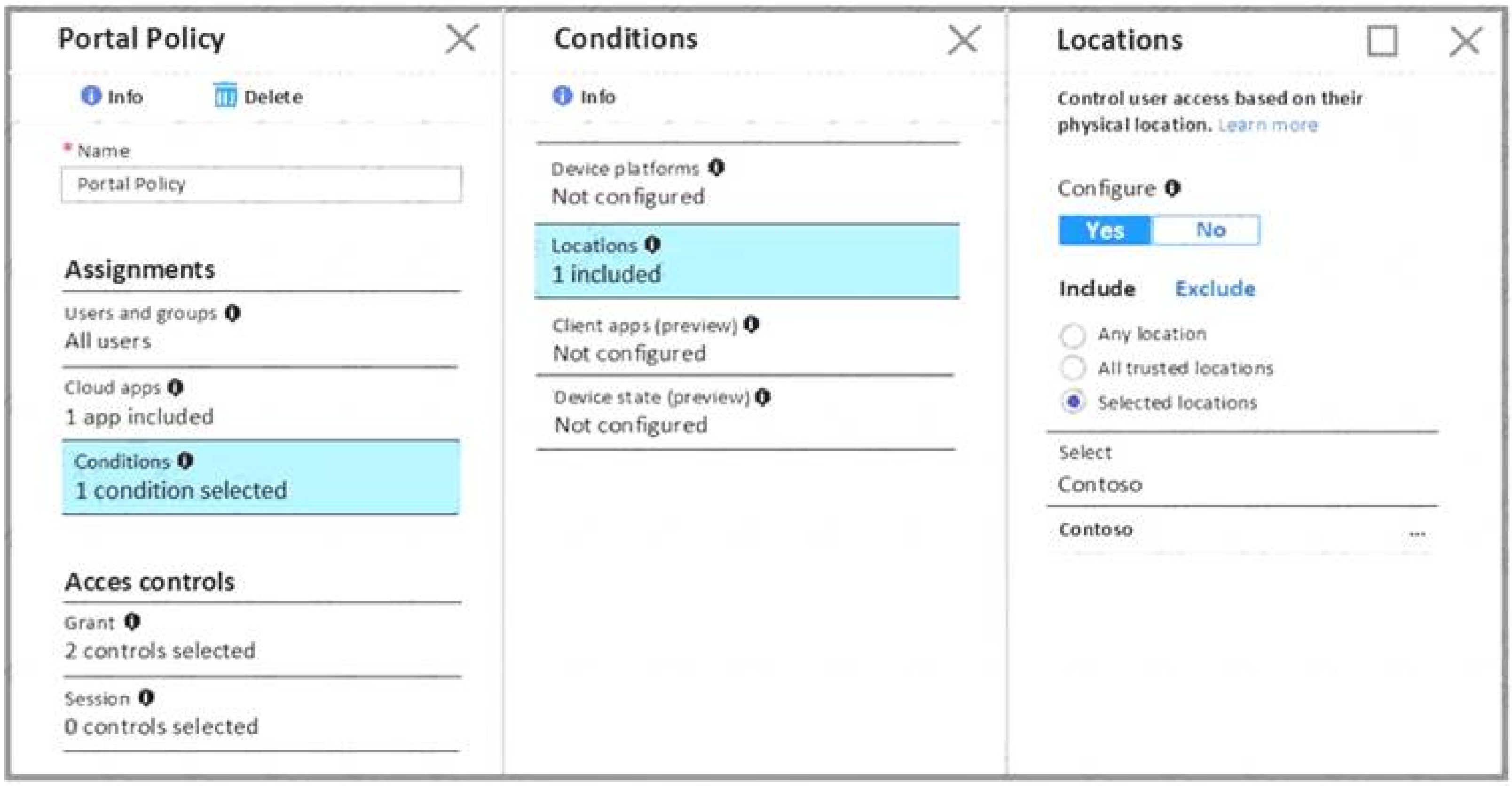
Answer Area

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 215
- (Exam Topic 4)
You create a new Azure subscription that is associated to a new Azure Active Directory (Azure AD) tenant. You create one active conditional access policy named Portal Policy. Portal Policy is used to provide access to the Microsoft Azure Management cloud app.
The Conditions settings for Portal Policy are configured as shown in the Conditions exhibit. (Click the Conditions tab.)



Portal Policy

* Name
Portal Policy

Assignments

Users and groups
All users

Cloud apps
1 app included

Conditions
1 condition selected

Acces controls

Grant
2 controls selected

Session
0 controls selected

Conditions

Device platforms
Not configured

Locations
1 included

Client apps (preview)
Not configured

Device state (preview)
Not configured

Locations

Control user access based on their physical location. Learn more

Configure
[✓ Yes] No

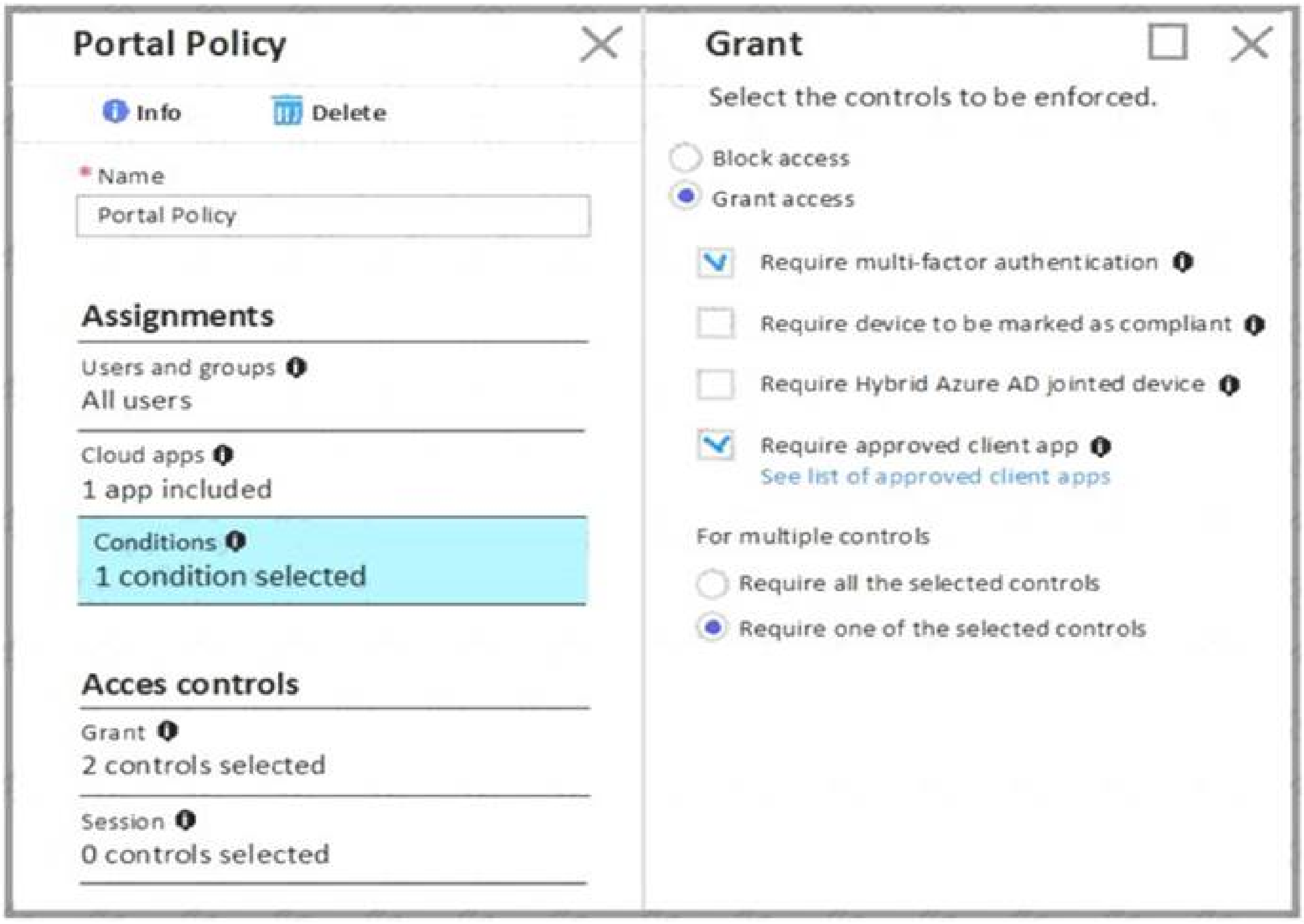
Include Exclude

○ Any location
○ All trusted locations
● Selected locations

Select
Contoso

Contoso ...

The Grant settings for Portal Policy are configured as shown in the Grant exhibit. (Click the Grant tab.)



Portal Policy

* Name: Portal Policy

Assignments

Users and groups: All users

Cloud apps: 1 app included

Conditions: 1 condition selected

Acces controls

Grant: 2 controls selected

Session: 0 controls selected

Grant

Select the controls to be enforced.

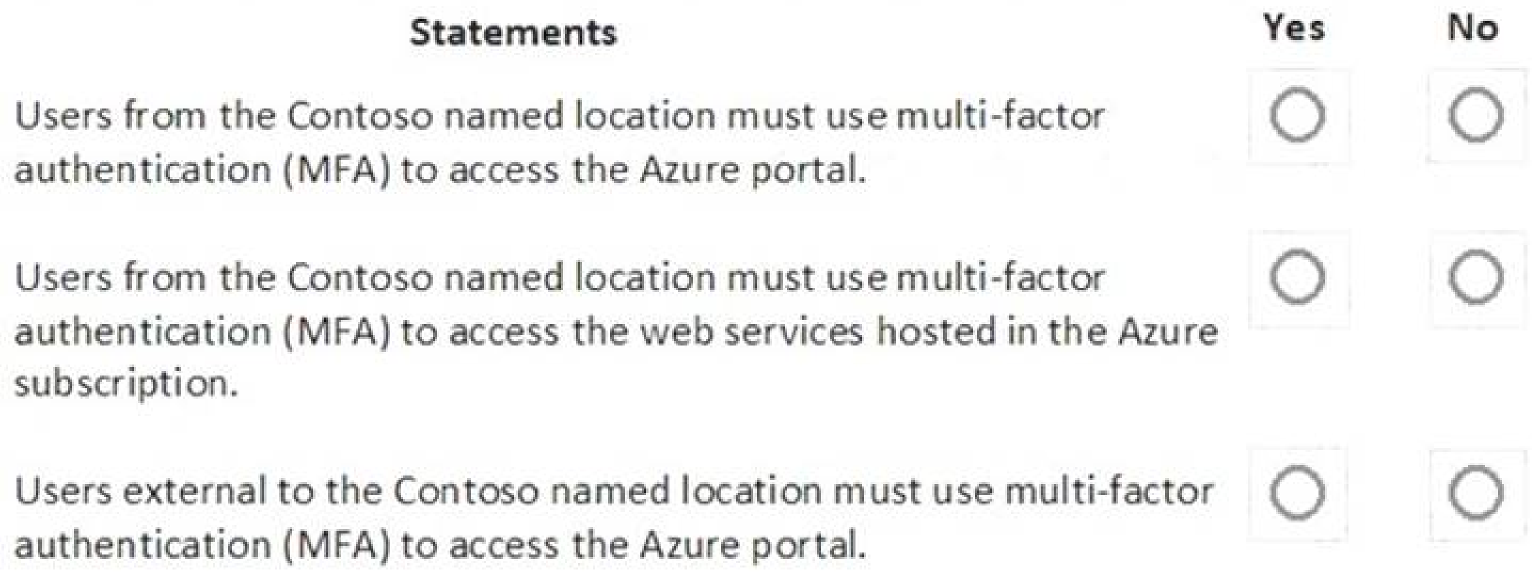
○ Block access
● Grant access

☑ Require multi-factor authentication
□ Require device to be marked as compliant
□ Require Hybrid Azure AD jointed device
☑ Require approved client app
See list of approved client apps

For multiple controls

○ Require all the selected controls
● Require one of the selected controls

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
Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	○	○
Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription.	○	○
Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: No
The Contoso location is excluded Box 2: NO
Box 3: NO
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

NEW QUESTION 217
- (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: Userl -28681041@ExamUsers.com
Azure Password: GpOAe4@lDg
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

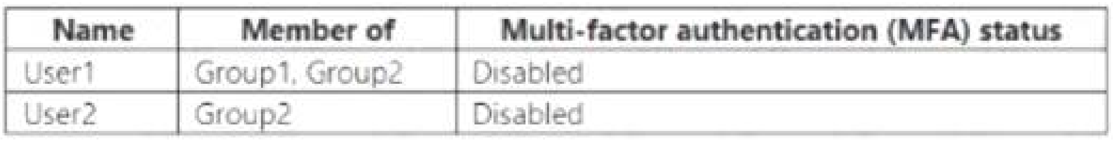
Answer: A

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.

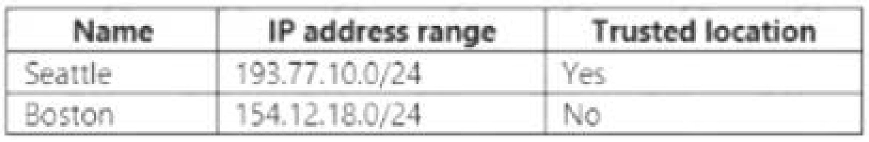
https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security

NEW QUESTION 219
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.



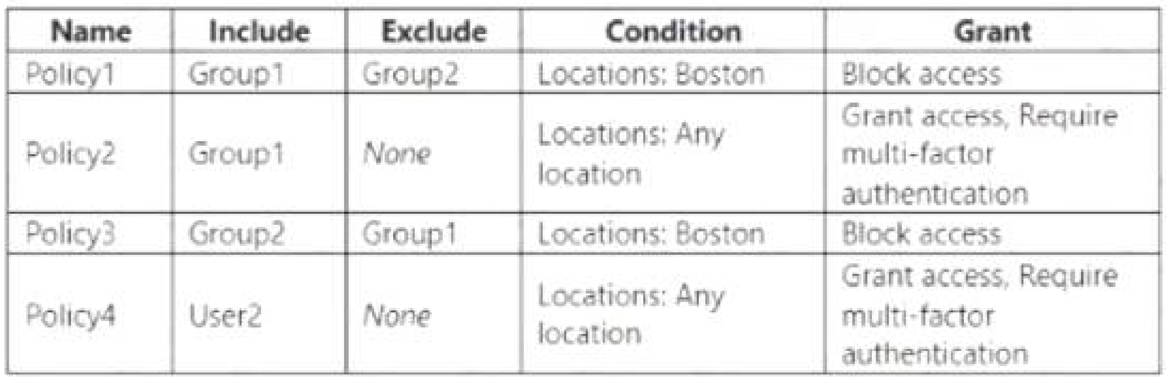
Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Disabled
User2	Group2	Disabled

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



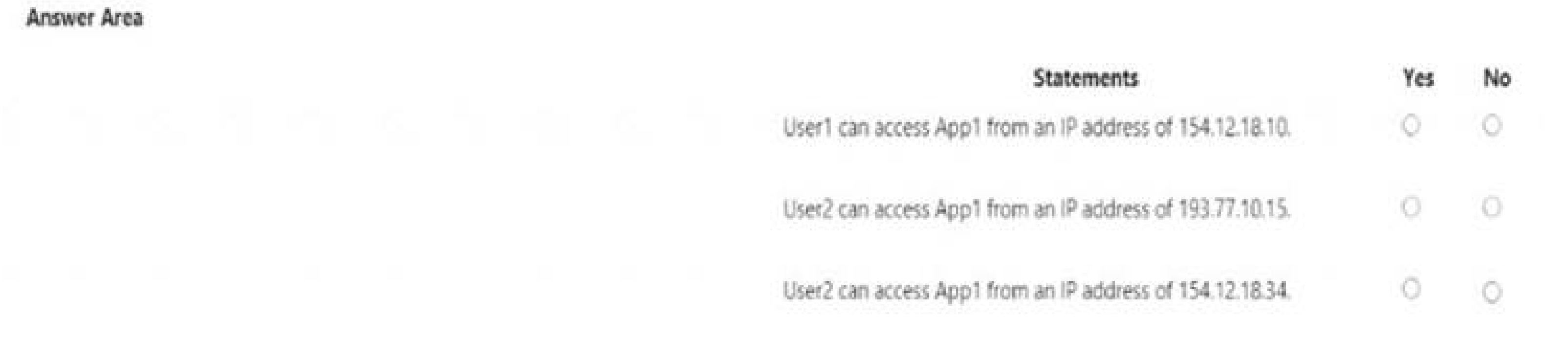
Name	IP address range	Trusted location
Seattle	193.77.10.0/24	Yes
Boston	154.12.18.0/24	No

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.



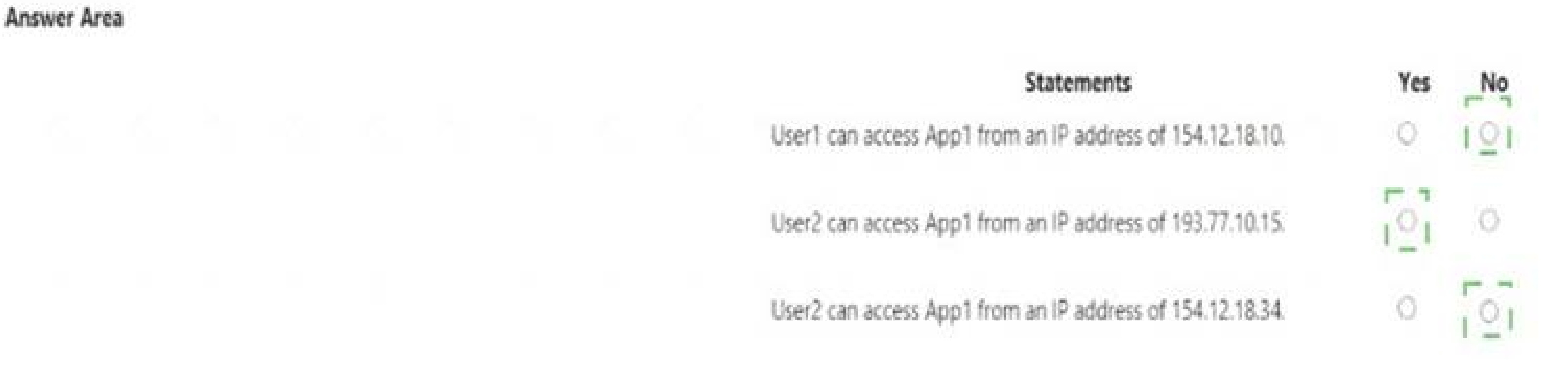
Answer Area

Statements	Yes	No
User1 can access App1 from an IP address of 154.12.18.10.	○	○
User2 can access App1 from an IP address of 193.77.10.15.	○	○
User2 can access App1 from an IP address of 154.12.18.34.	○	○

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.	○	[✓ ○]
User2 can access App1 from an IP address of 193.77.10.15.	[✓ ○]	○
User2 can access App1 from an IP address of 154.12.18.34.	○	[✓ ○]

NEW QUESTION 223
- (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?

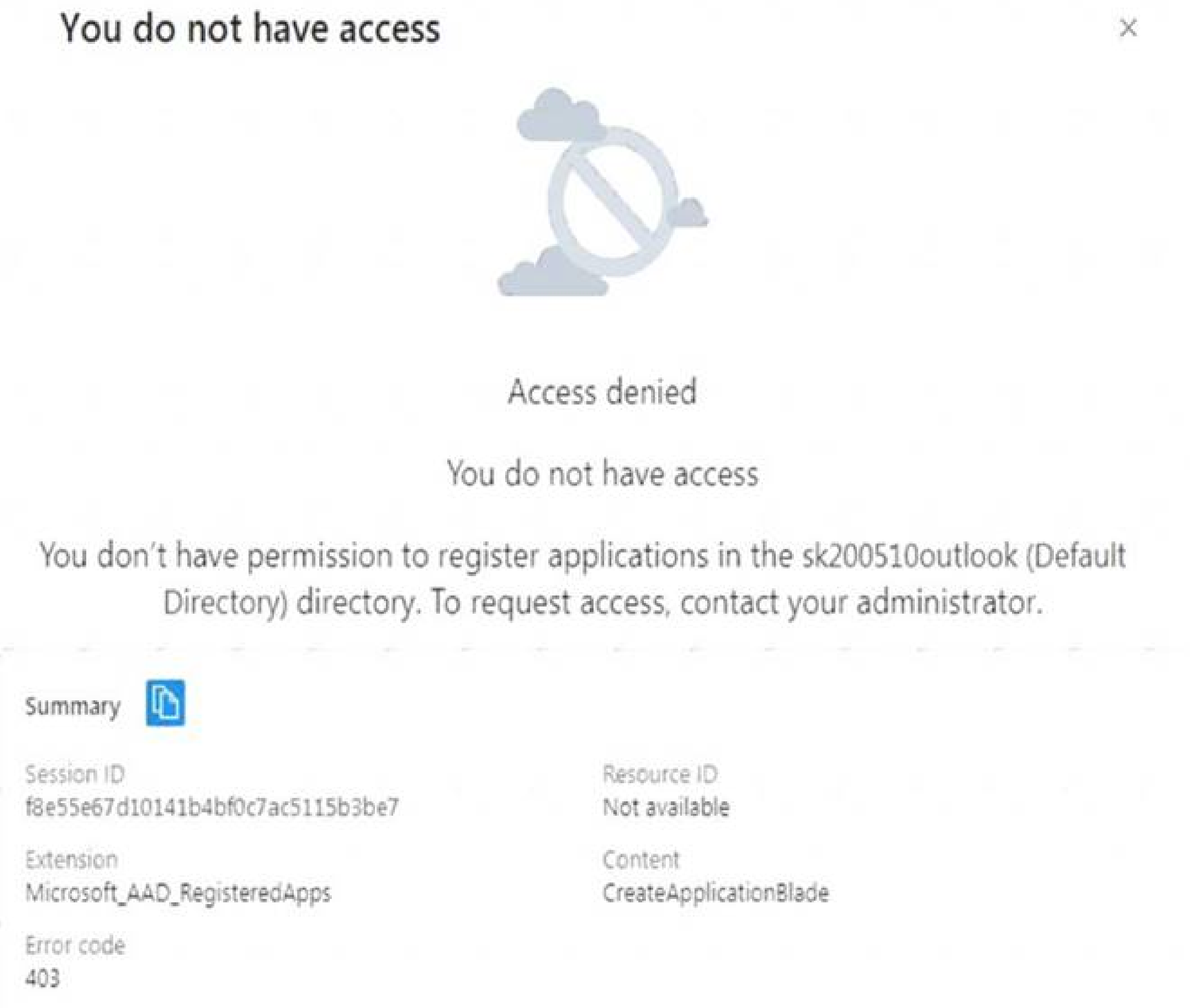
A. an Azure Active Directory (Azure AD) Privileged identity Management (PIM) role assignment.
B. a just in time (JIT) VM access policy in Azure Security Center
C. an azure policy assigned to RG1.
D. an Azure Bastion host on VNET1.

Answer: B

Explanation:

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

NEW QUESTION 225
- (Exam Topic 4)
You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant.
When a developer attempts to register an app named App1 in the tenant, the developer receives the error message shown in the following exhibit.



You do not have access ×

Access denied

You do not have access

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

Summary

Session ID
f8e55e67d10141b4bf0c7ac5115b3be7

Resource ID
Not available

Extension
Microsoft_AAD_RegisteredApps

Content
CreateApplicationBlade

Error code
403

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

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

Answer: A

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

NEW QUESTION 228
- (Exam Topic 4)
You have an Azure subscription that contains an Azure Files share named share1 and a user named User1. Identity-based authentication is configured for share1. User1 attempts to access share1 from a Windows 10 device by using SMB. Which type of token will Azure Files use to authorize the request?

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

Answer: C

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

NEW QUESTION 231
- (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: Userl -28681041@ExamUsers.com
Azure Password: GpOAe4@lDg
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 232
- (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: Userl -28681041@ExamUsers.com
Azure Password: GpOAe4@lDg
If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only: Lab Instance: 28681041
Task 10
You need to create a new Azure AD directory named 28681041.onmicrosoft.com. The new directory must contain a new user named user1@28681041.onmicrosoft.com.

A. Mastered
B. Not Mastered

Answer: A

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

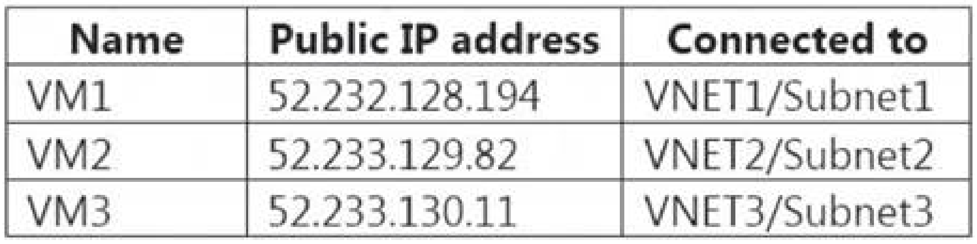
- In the Azure portal, search for and select Azure Active Directory.
- In the left pane, select Domains.
- Select Add domain.
- In the Add a custom domain pane, enter the following information:
- Domain name: Enter the domain name you want to use. For example, 28681041.onmicrosoft.com.
- Add domain: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

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

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

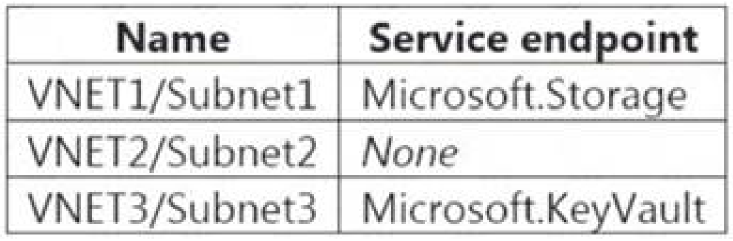
NEW QUESTION 234

- (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.

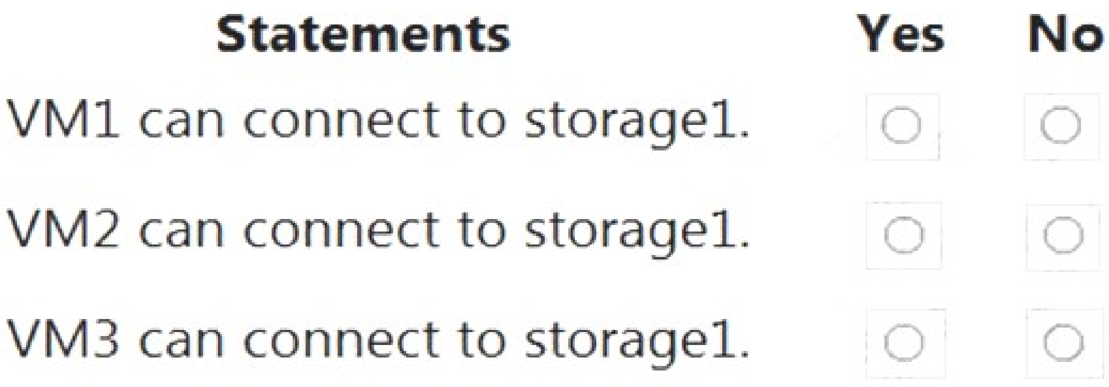


Name	Service endpoint
VNET1/Subnet1	Microsoft.Storage
VNET2/Subnet2	*None*
VNET3/Subnet3	Microsoft.KeyVault

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.	○	○
VM2 can connect to storage1.	○	○
VM3 can connect to storage1.	○	○

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 238
- (Exam Topic 4)
You have an Azure subscription that contains an Azure key vault and an Azure Storage account. The key vault contains customer-managed keys. The storage account is configured to use the customer-managed keys stored In the key vault.
You plan to store data in Azure by using the following services:
* Azure Files
* Azure Blob storage
* Azure Log Analytics
* Azure Table storage
* Azure Queue storage
Which two services data encryption by using the keys stored in the key vault? Each correct answer present a complete solution.
NOTE: Each correct selection is worth one point.

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

Answer: AC

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

NEW QUESTION 241
- (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.

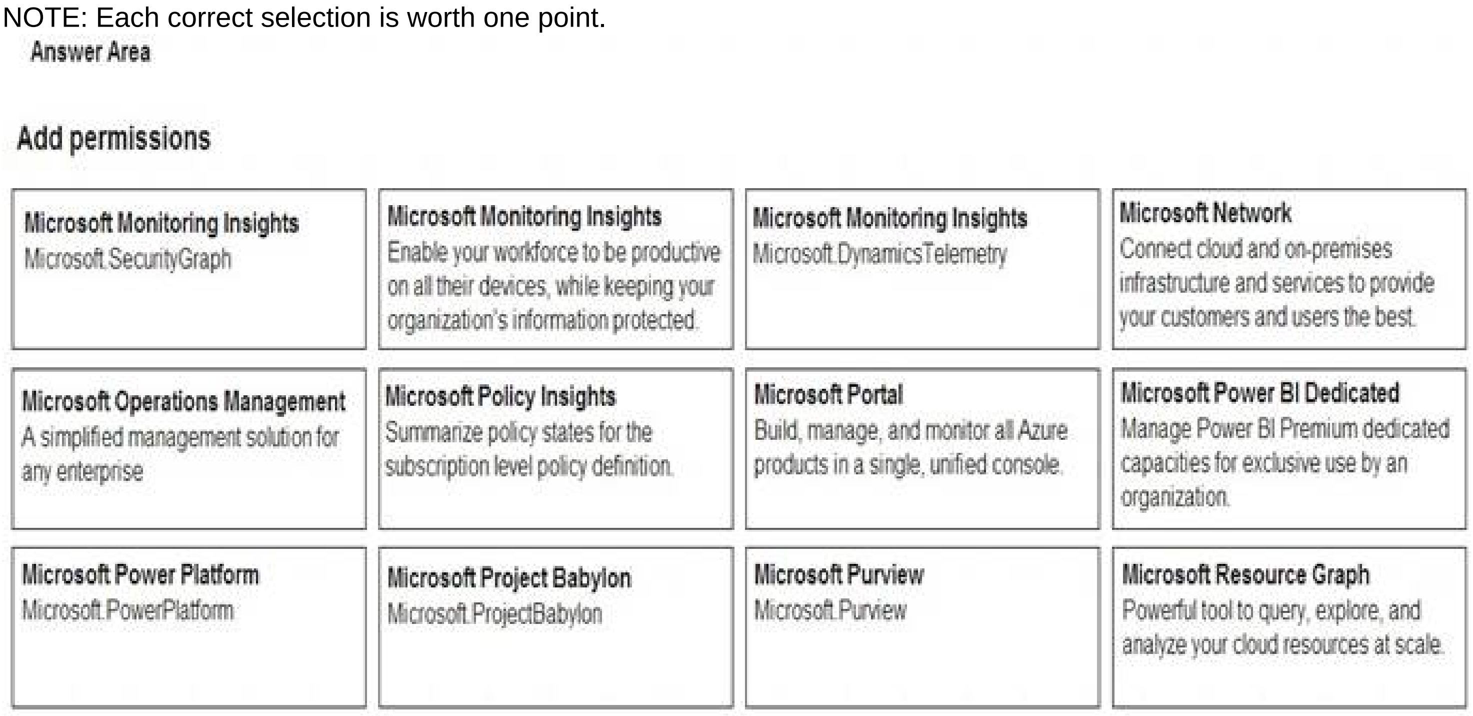
You use Azure Security Center for the centralized policy management of three Azure subscriptions. You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create a policy initiative and 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 243
- (Exam Topic 4)
You have an Azure subscription that contains a user named User1. User1 is assigned the Reader role for the subscription.
You plan to create a custom role named Role1 and assign Role1 to User1.
You need to ensure that User1 can create and manage application security groups by using the Azure portal. Which two permissions should you add to Role1? To answer, select the appropriate permission in the answer area.
NOTE: Each correct selection is worth one point.


Answer Area

Add permissions

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
* 1. Microsoft Portal 2. Microsoft Network
https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/azure-services-resource-providers

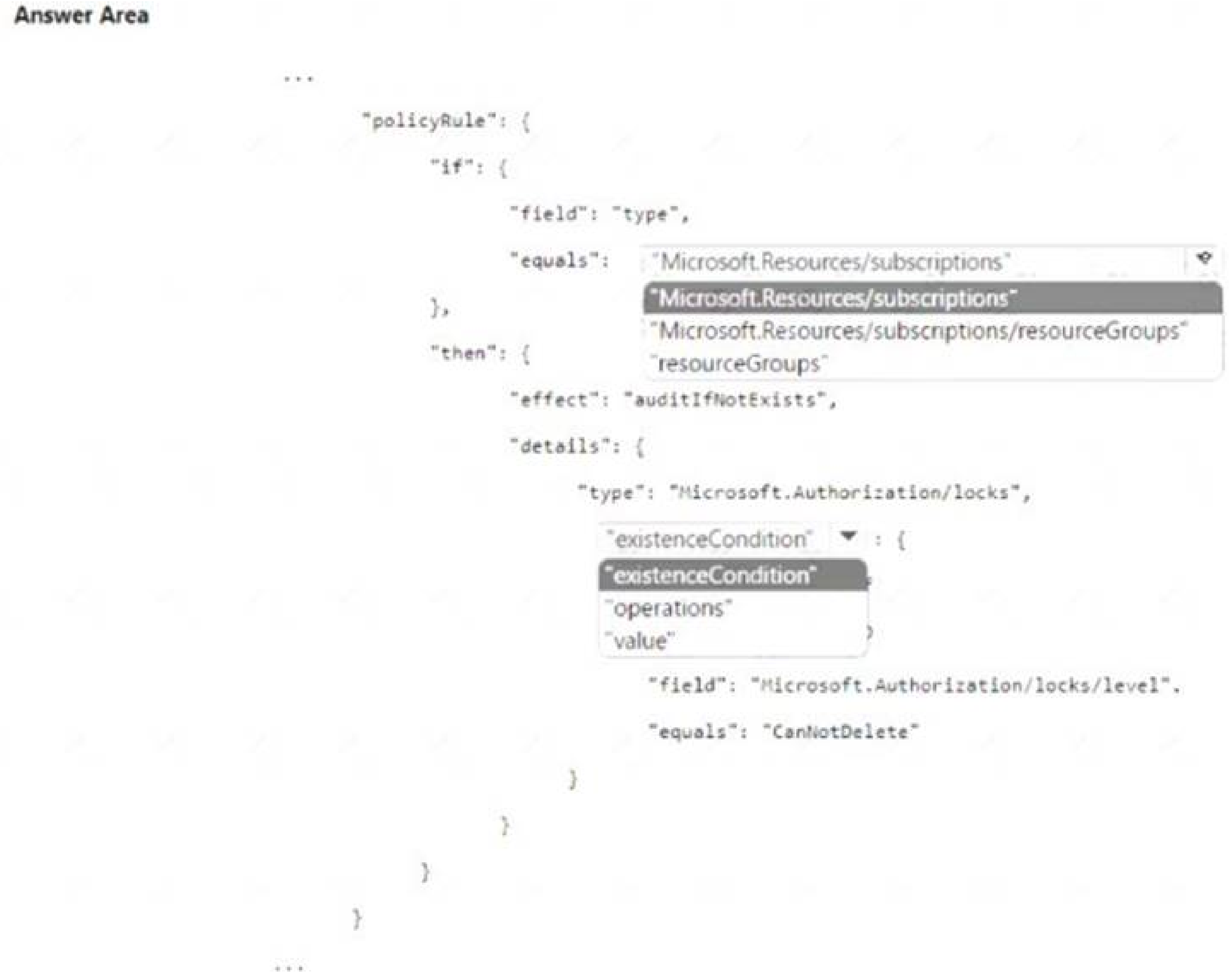
NEW QUESTION 247
- (Exam Topic 4)
Lab Task
use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password. place your cursor in the Enter password box and click on the password below. Azure Username: Userl -28681041@ExamUsers.com
Azure Password: GpOAe4@lDg
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 249
- (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.

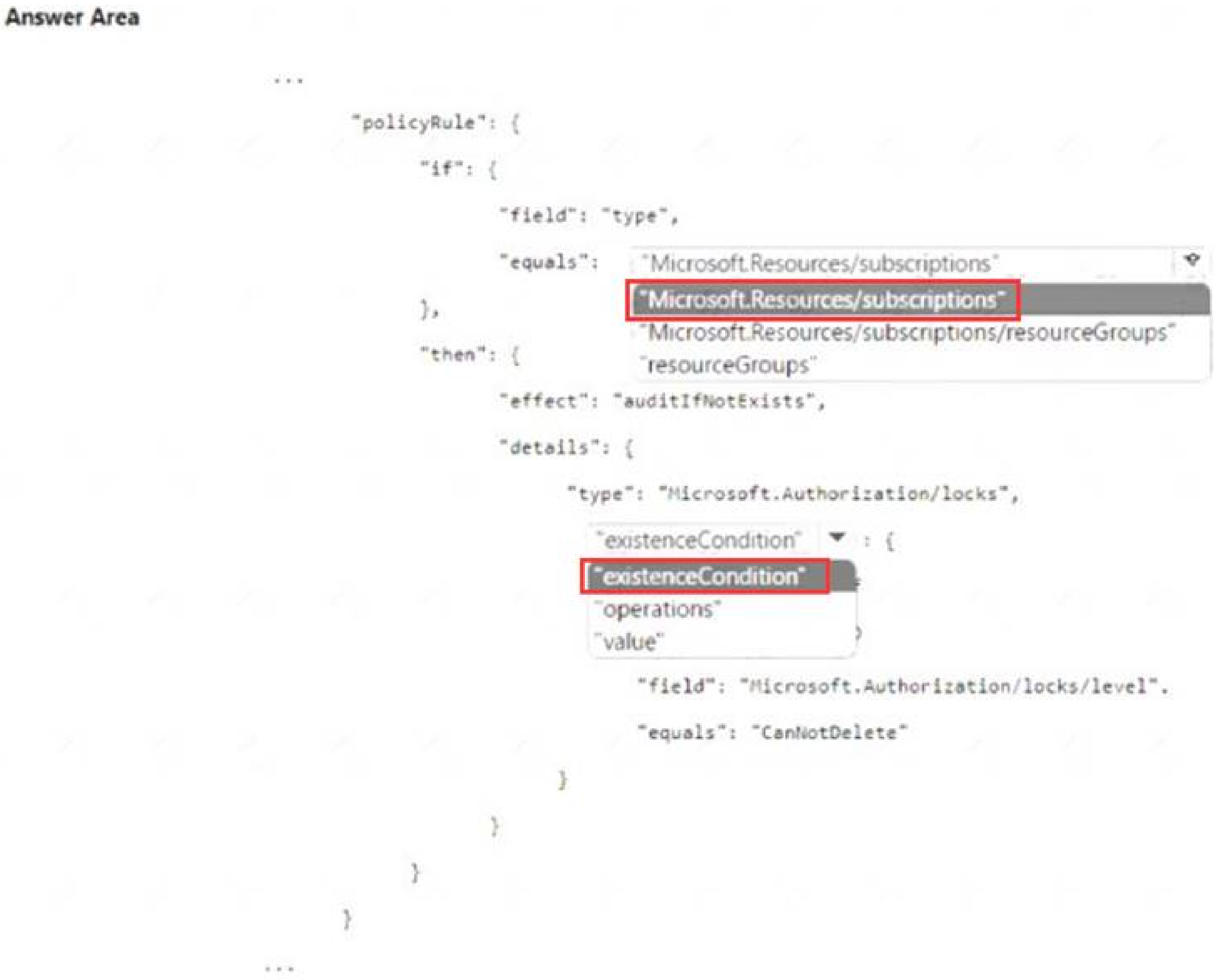

Answer Area
"Microsoft.Resources/subscriptions"
"Microsoft.Resources/subscriptions/resourceGroups"
"resourceGroups"
"existenceCondition"
"operations"
"value"

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

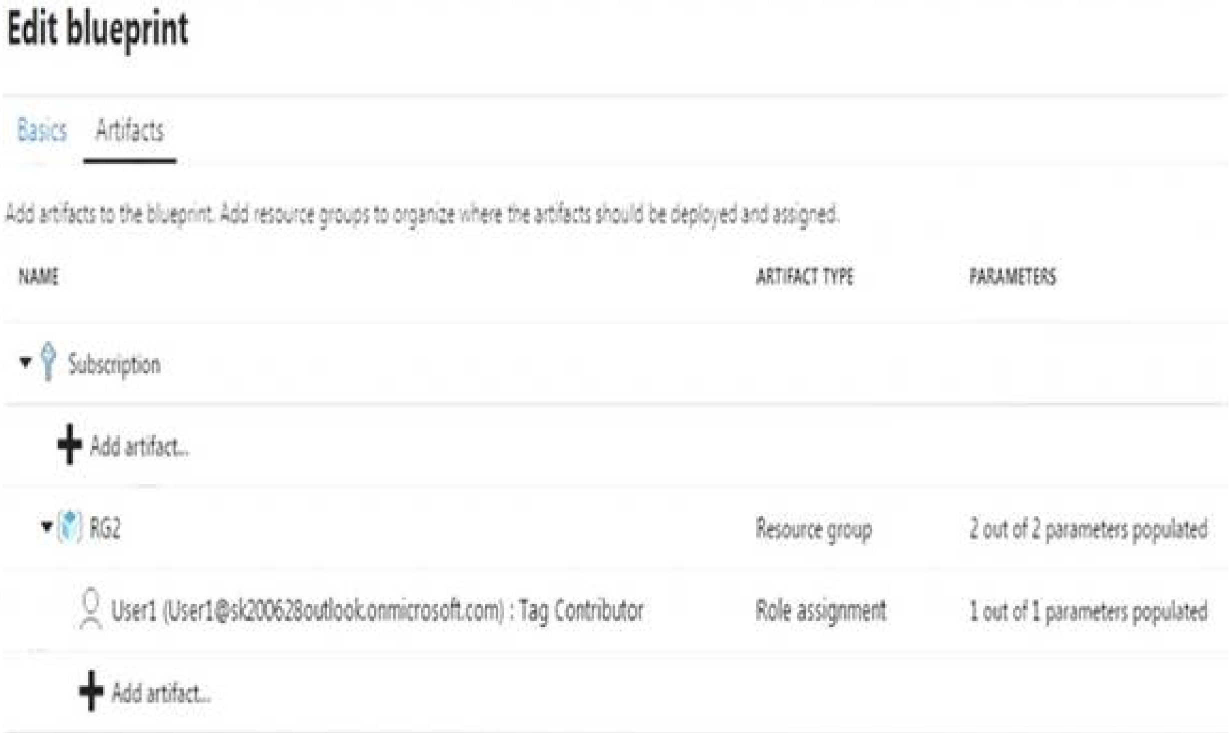
```
...
    "policyRule": {
        "if": {
            "field": "type",
            "equals": "Microsoft.Resources/subscriptions"
                      "Microsoft.Resources/subscriptions"
                      "Microsoft.Resources/subscriptions/resourceGroups"
                      "resourceGroups"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

NEW QUESTION 253

- (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

Add artifacts to the blueprint. Add resource groups to organize where the artifacts should be deployed and assigned.

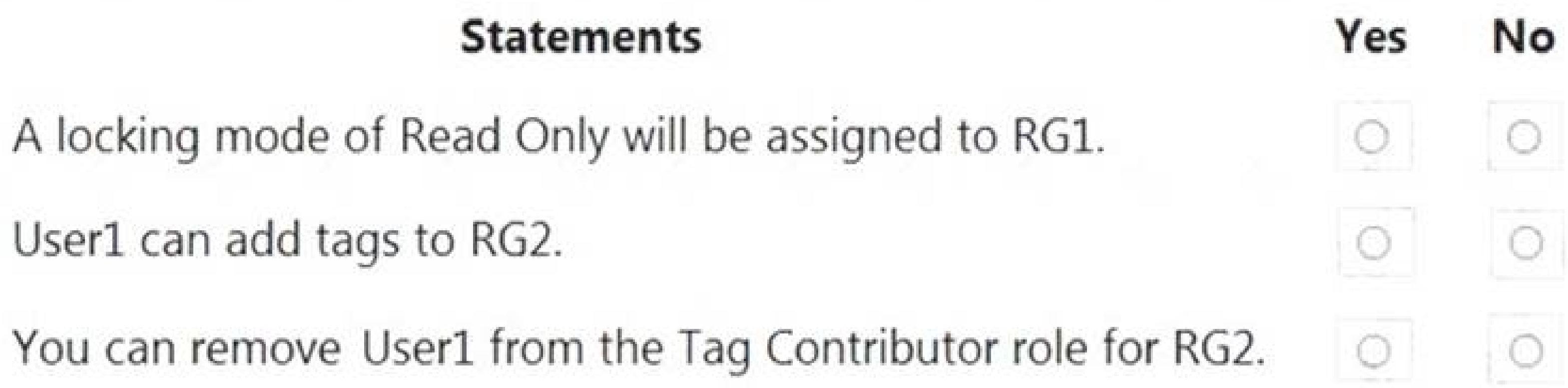
NAME	ARTIFACT TYPE	PARAMETERS
Subscription		
Add artifact...		
RG2	Resource group	2 out of 2 parameters populated
User1 (User1@sk200628outlook.onmicrosoft.com) : Tag Contributor	Role assignment	1 out of 1 parameters populated
Add artifact...		

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.	○	○
User1 can add tags to RG2.	○	○
You can remove User1 from the Tag Contributor role for RG2.	○	○

A. Mastered
B. Not Mastered

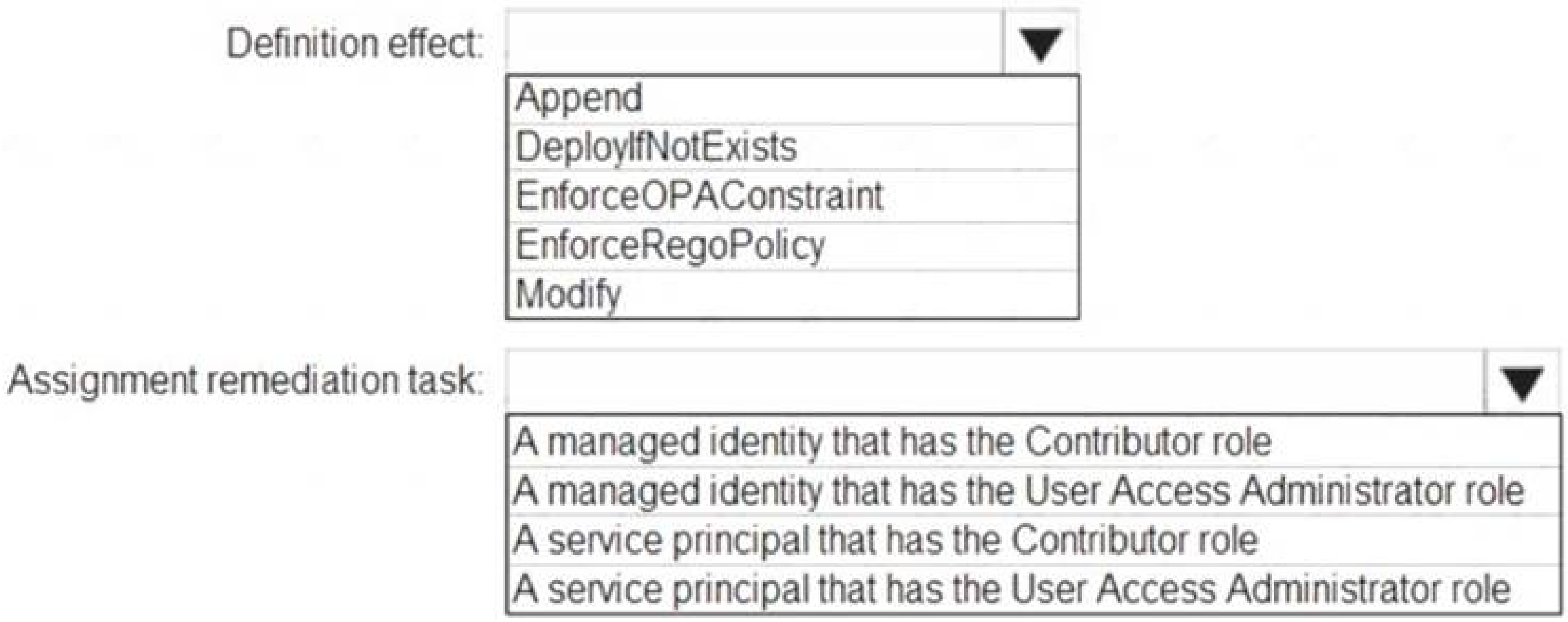
Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated
Reference:
https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking

NEW QUESTION 255
- (Exam Topic 4)
You have an Azure subscription.
You need to create and deploy an Azure policy that meets the following requirements:

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

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



Definition effect:
- Append
- DeployIfNotExists
- EnforceOPAConstraint
- EnforceRegoPolicy
- Modify

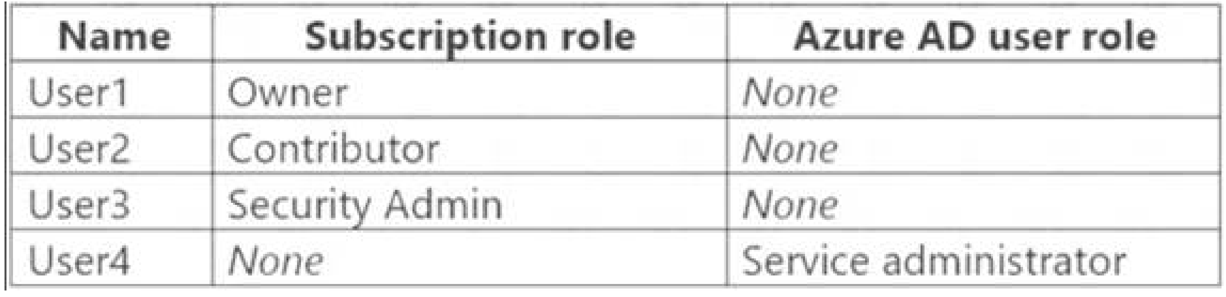
Assignment remediation task:
- A managed identity that has the Contributor role
- A managed identity that has the User Access Administrator role
- A service principal that has the Contributor role
- A service principal that has the User Access Administrator role

A. Mastered
B. Not Mastered

Answer: A

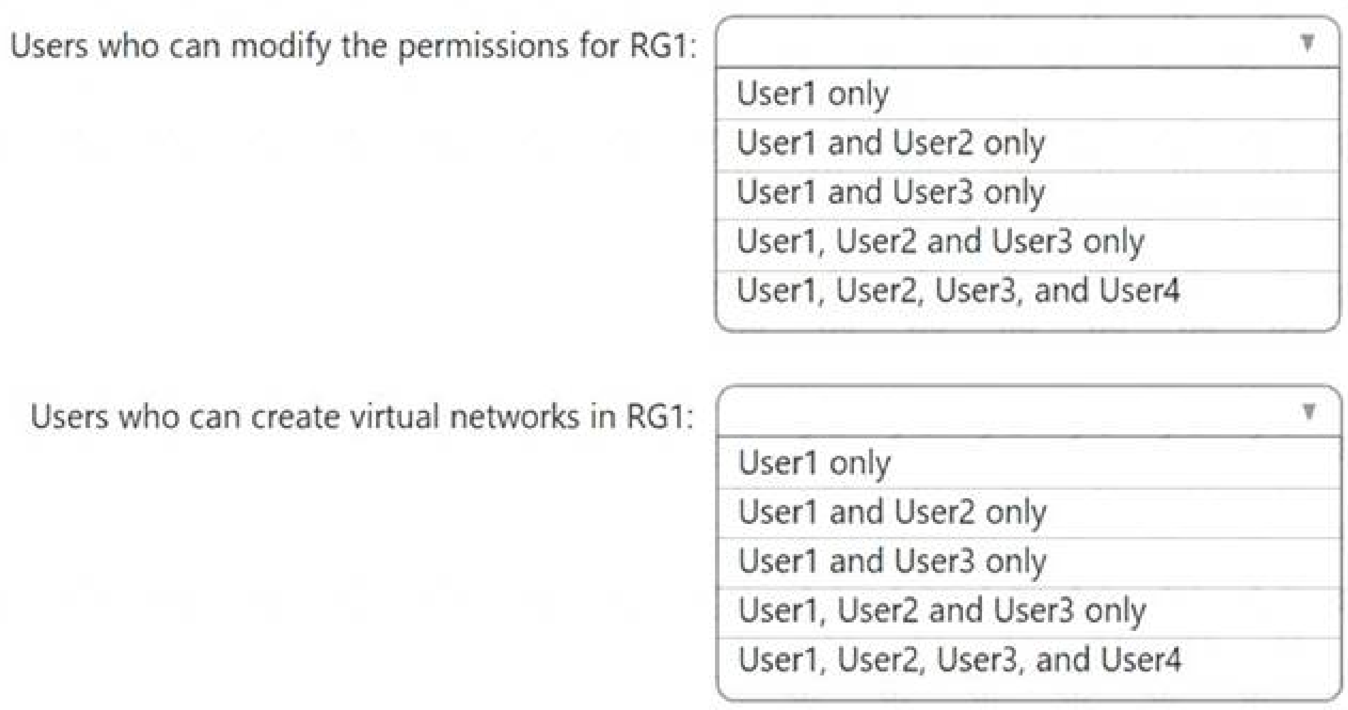
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources

NEW QUESTION 259
- (Exam Topic 4)
You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.



Name	Subscription role	Azure AD user role
User1	Owner	*None*
User2	Contributor	*None*
User3	Security Admin	*None*
User4	*None*	Service administrator

You create a resource group named RG1.
Which users can modify the permissions for RG1 and which users can create virtual networks in RG1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Users who can modify the permissions for RG1:

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

Users who can create virtual networks in RG1:

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Only an owner can change permissions on resources.
Box 2: A Contributor can create/modify/delete anything in the subscription but cannot change permissions.

NEW QUESTION 263
- (Exam Topic 4)
You are configuring and securing a network environment.
You deploy an Azure virtual machine named VM1 that is configured to analyze network traffic. You need to ensure that all network traffic is routed through VM1.
What should you configure?

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

Answer: C

Explanation:
Although the use of system routes facilitates traffic automatically for your deployment, there are cases in which you want to control the routing of packets through a virtual appliance. You can do so by creating user defined routes that specify the next hop for packets flowing to a specific subnet to go to your virtual appliance instead, and enabling IP forwarding for the VM running as the virtual appliance.
Note: User Defined Routes
For most environments you will only need the system routes already defined by Azure. However, you may need to create a route table and add one or more routes in specific cases, such as:

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

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

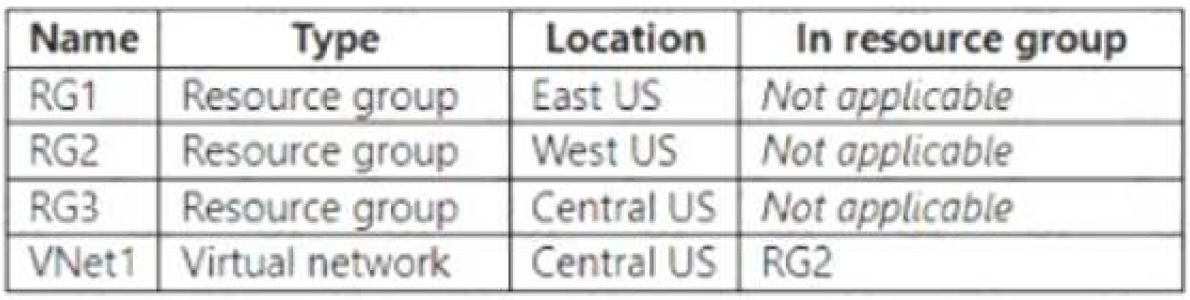
NEW QUESTION 264
- (Exam Topic 4)
You have an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry. You need to use automatically generated service principal for the AKS cluster to authenticate to the Azure
Container Registry.
What should you create?

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

Answer: B

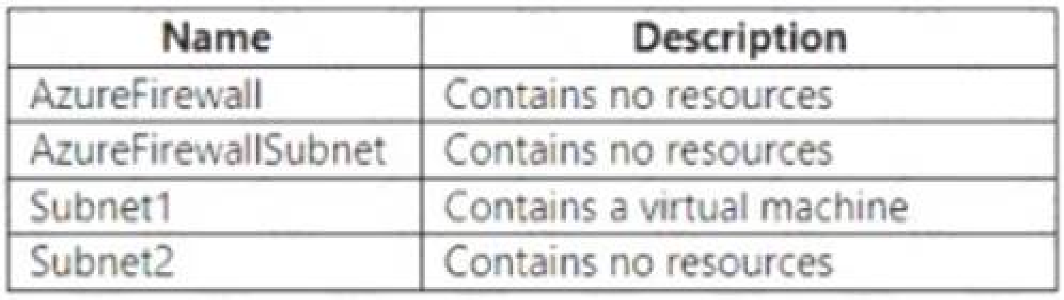
Explanation:
References:
https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal

NEW QUESTION 267
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.



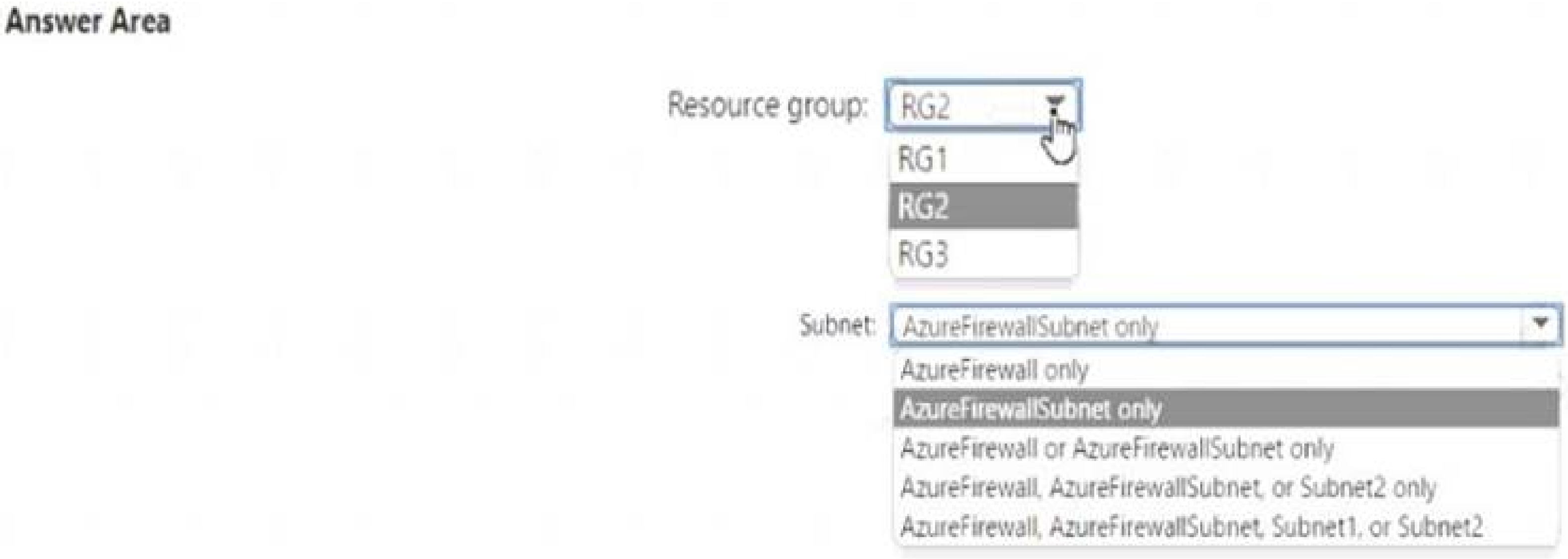
Name	Type	Location	In resource group
RG1	Resource group	East US	*Not applicable*
RG2	Resource group	West US	*Not applicable*
RG3	Resource group	Central US	*Not applicable*
VNet1	Virtual network	Central US	RG2

VNet1 contains the subnets shown in the following table.



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

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



Answer Area

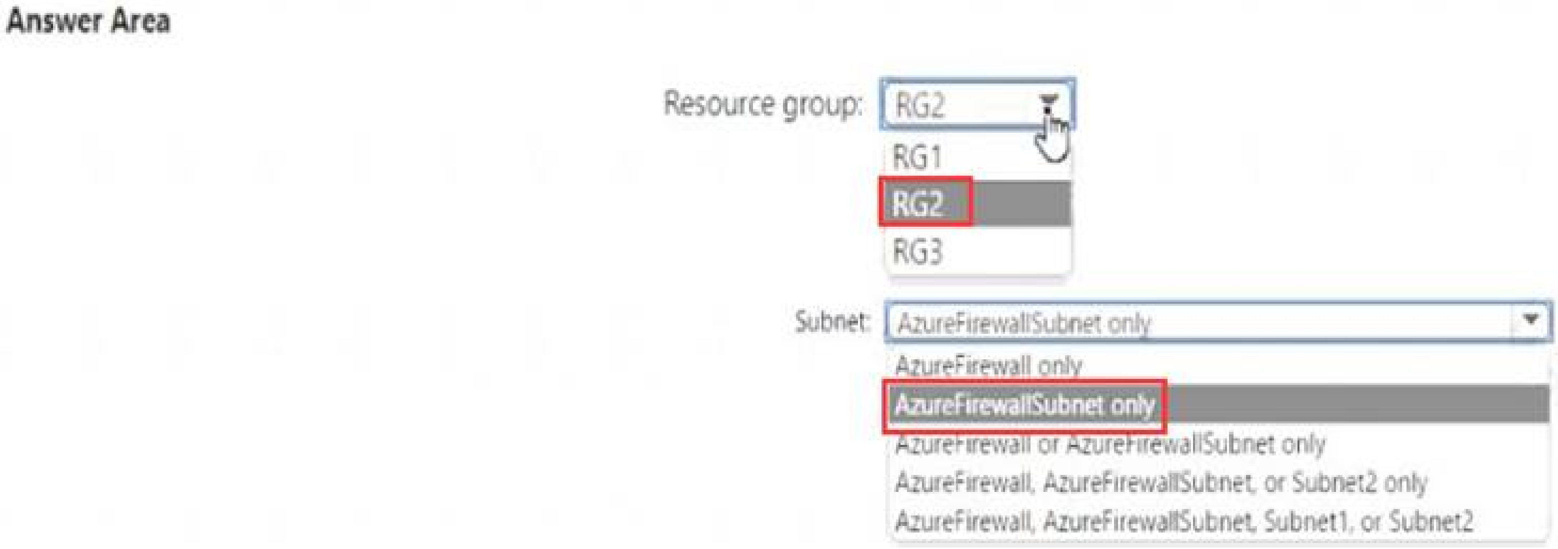
Resource group: RG2
- RG1
- RG2
- RG3

Subnet: AzureFirewallSubnet only
- AzureFirewall only
- AzureFirewallSubnet only
- AzureFirewall or AzureFirewallSubnet only
- AzureFirewall, AzureFirewallSubnet, or Subnet2 only
- AzureFirewall, AzureFirewallSubnet, Subnet1, or Subnet2

A. Mastered
B. Not Mastered

Answer: A

Explanation:

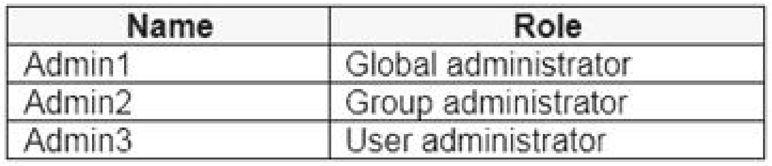


Answer Area

Resource group: RG2
- RG1
- RG2
- RG3

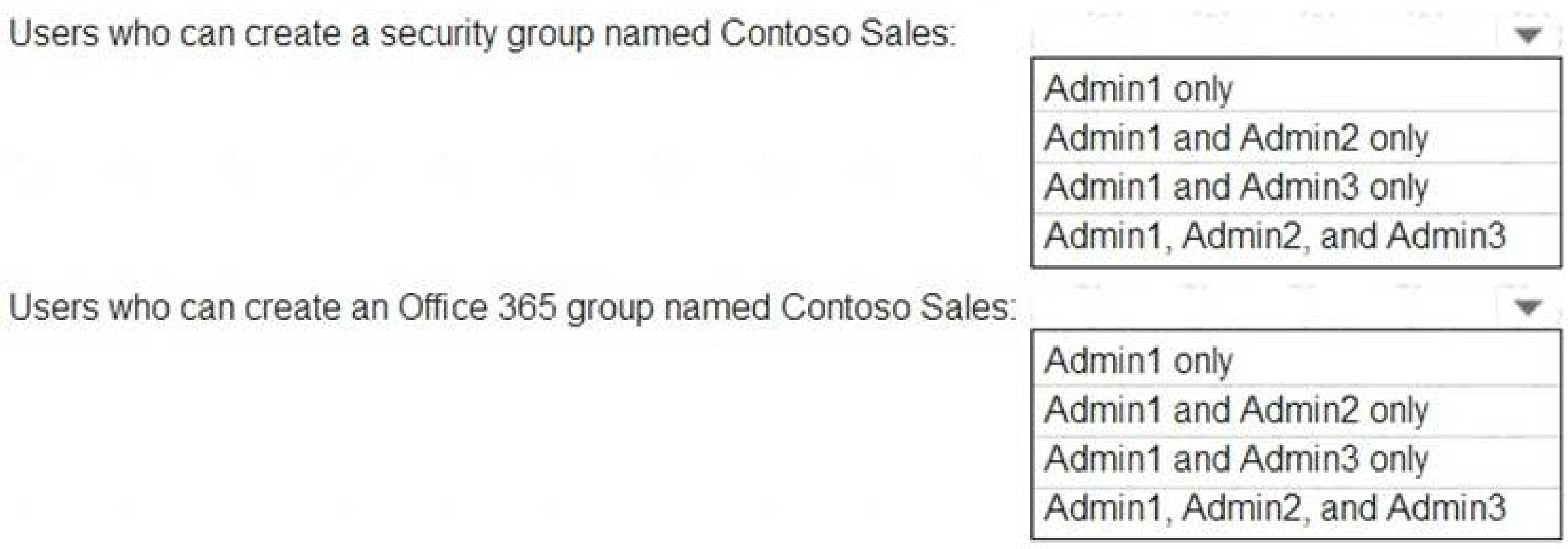
Subnet: AzureFirewallSubnet only
- AzureFirewall only
- AzureFirewallSubnet only
- AzureFirewall or AzureFirewallSubnet only
- AzureFirewall, AzureFirewallSubnet, or Subnet2 only
- AzureFirewall, AzureFirewallSubnet, Subnet1, or Subnet2

NEW QUESTION 271
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.



Name	Role
Admin1	Global administrator
Admin2	Group administrator
Admin3	User administrator

Contoso.com contains a group naming policy. The policy has a custom blocked word list rule that includes the word Contoso.
Which users can create a group named Contoso Sales in contoso.com? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Users who can create a security group named Contoso Sales:

- Admin1 only
- Admin1 and Admin2 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3

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

- Admin1 only
- Admin1 and Admin2 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 274
- (Exam Topic 4)
You have 10 virtual machines on a single subnet that has a single network security group (NSG). You need to log the network traffic to an Azure Storage account. Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

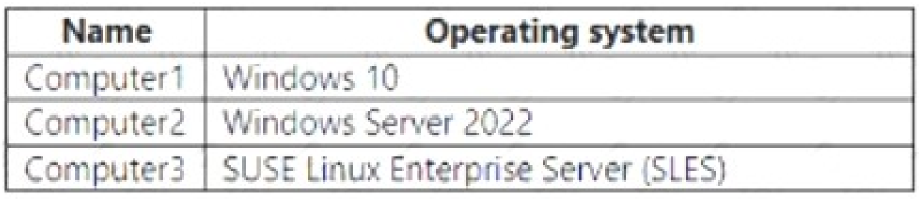
Answer: D

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

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

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

NEW QUESTION 275
- (Exam Topic 4)
You have an Azure subscription. That contains the virtual machines shown in the following table.



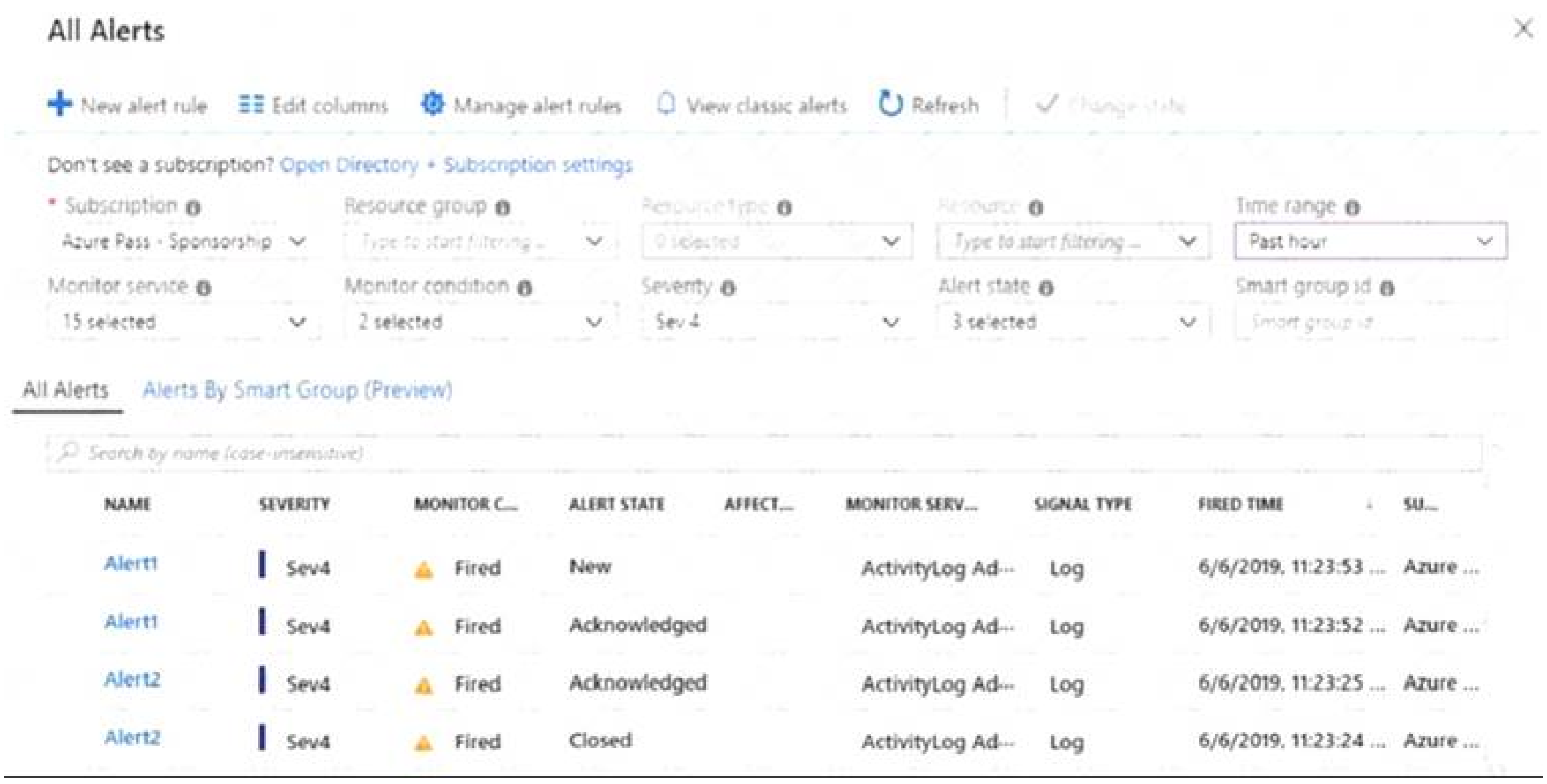
Name	Operating system
Computer1	Windows 10
Computer2	Windows Server 2022
Computer3	SUSE Linux Enterprise Server (SLES)

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

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

Answer: B

NEW QUESTION 278
- (Exam Topic 4)
You have an Azure subscription that contains the alerts shown in the following exhibit.

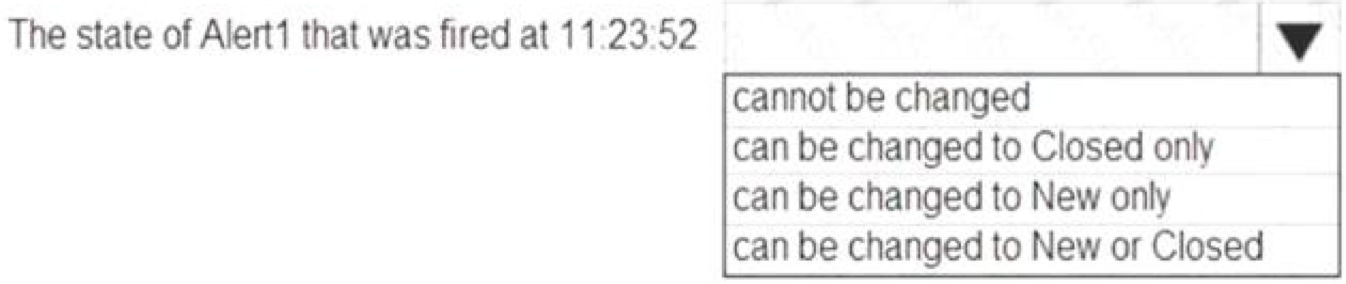


Don't see a subscription? Open Directory • Subscription settings

* Subscription	Resource group	Resource type	Resource	Time range
Azure Pass - Sponsorship	Type to start filtering ...	0 selected	Type to start filtering ...	Past hour
Monitor service	**Monitor condition**	**Severity**	**Alert state**	**Smart group id**
15 selected	2 selected	Sev 4	3 selected	Smart group id

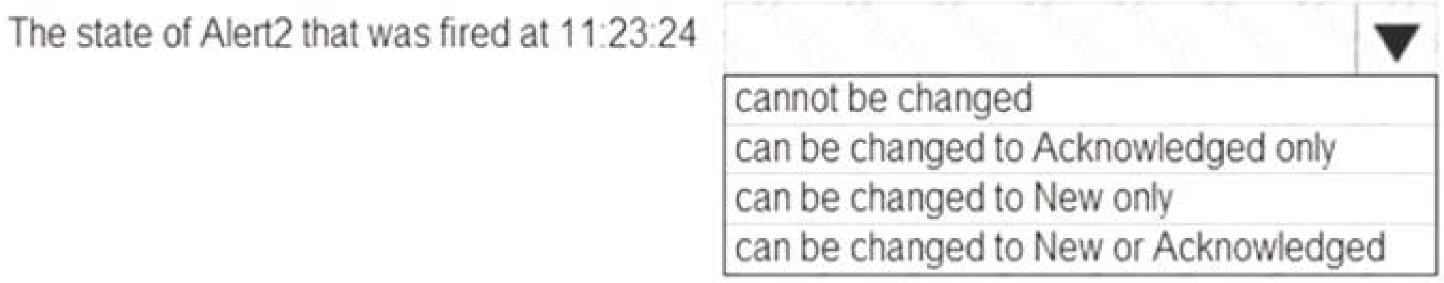
NAME	SEVERITY	MONITOR C...	ALERT STATE	AFFECT...	MONITOR SERV...	SIGNAL TYPE	FIRED TIME	SU...
Alert1	Sev4	Fired	New		ActivityLog Ad...	Log	6/6/2019, 11:23:53 ...	Azure ...
Alert1	Sev4	Fired	Acknowledged		ActivityLog Ad...	Log	6/6/2019, 11:23:52 ...	Azure ...
Alert2	Sev4	Fired	Acknowledged		ActivityLog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

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



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

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



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

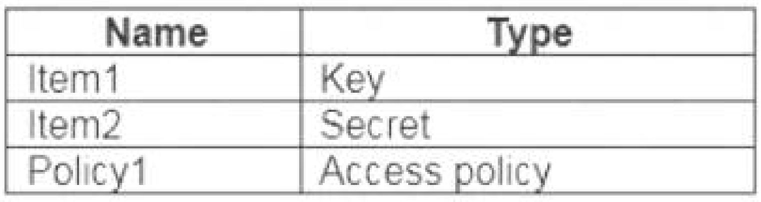
- cannot be changed
- can be changed to Acknowledged only
- can be changed to New only
- can be changed to New or Acknowledged

A. Mastered
B. Not Mastered

Answer: A

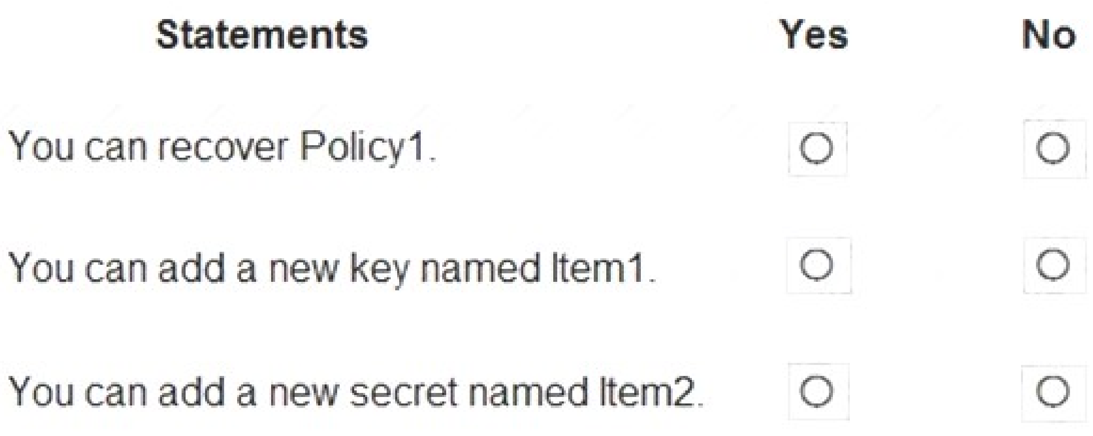
Explanation:
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-overview

NEW QUESTION 281
- (Exam Topic 4)
You have an Azure key vault named KeyVault1 that contains the items shown in the following table.



Name	Type
Item1	Key
Item2	Secret
Policy1	Access policy

In KeyVault1 the following events occur in sequence:
• item is deleted.
• Item2 and Policy1 are deleted.
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

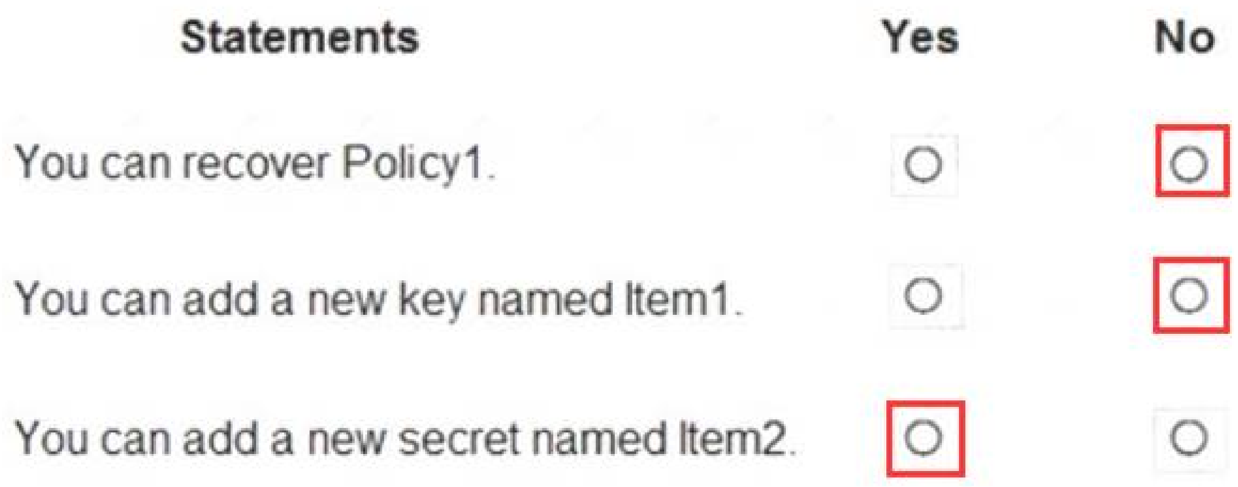


Statements	Yes	No
You can recover Policy1.	○	○
You can add a new key named Item1.	○	○
You can add a new secret named Item2.	○	○

A. Mastered
B. Not Mastered

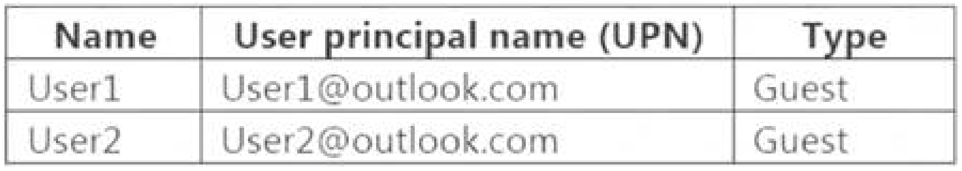
Answer: A

Explanation:



Statements	Yes	No
You can recover Policy1.	○	[✓ ○]
You can add a new key named Item1.	○	[✓ ○]
You can add a new secret named Item2.	[✓ ○]	○

NEW QUESTION 282
- (Exam Topic 4)
You have an Azure subscription named Subscription1 that contains a resource group named RG1 and the users shown in the following table.



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

You perform the following tasks:

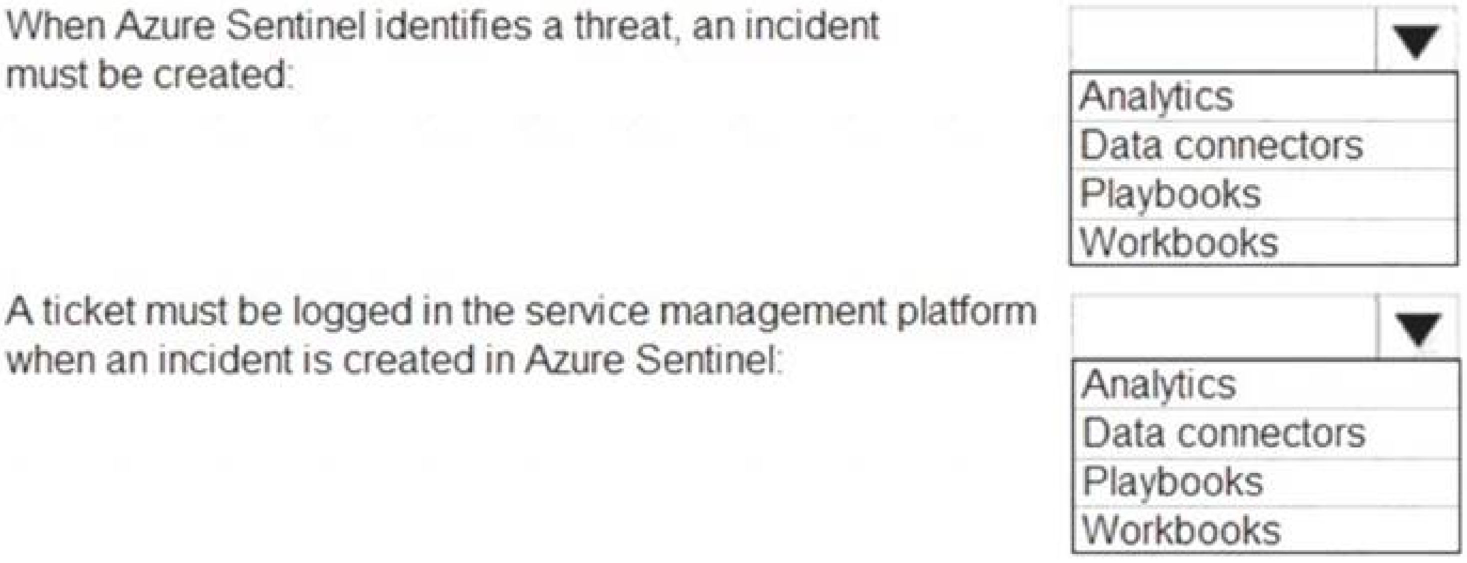
- Assign User1 the Network Contributor role for Subscription1.
- Assign User2 the Contributor role for RG1.

To Subscription1 and RG1, you assign the following policy definition: External accounts with write permissions should be removed from your subscription.
What is the Compliance State of the policy assignments?

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

Answer: A

NEW QUESTION 285
- (Exam Topic 4)
You have an Azure subscription that contains a Microsoft Sentinel workspace.
Microsoft Sentinel is configured to ingest logs from several Azure workloads. A third-party service management platform is used to manage incidents.
You need to identify which Microsoft Sentinel components to configure to meet the following requirements:
• When Microsoft Sentinel identifies a threat an incident must be created.
• A ticket must be logged in the service management platform when an incident is created in Microsoft Sentinel.
Which component should you identify for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



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

- Analytics
- Data connectors
- Playbooks
- Workbooks

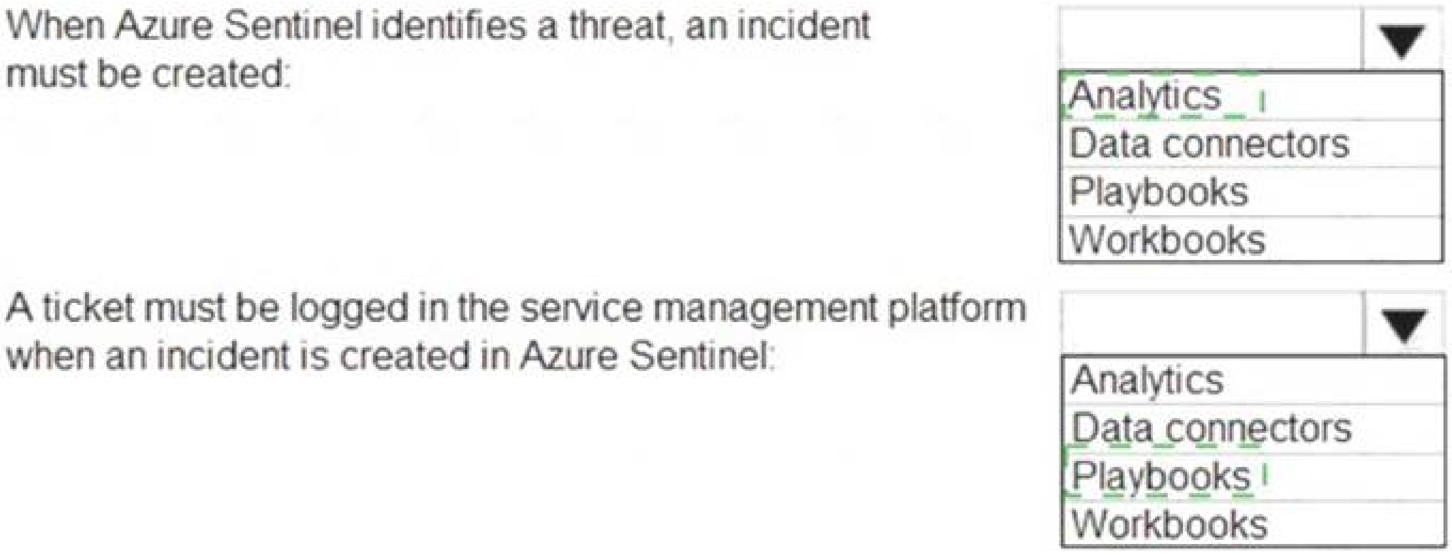
A ticket must be logged in the service management platform when an incident is created in Azure Sentinel:

- Analytics
- Data connectors
- Playbooks
- Workbooks

A. Mastered
B. Not Mastered

Answer: A

Explanation:



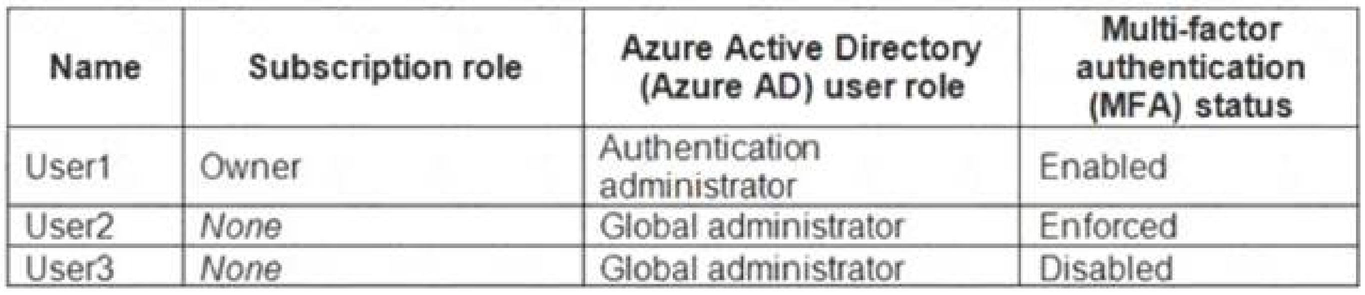
When Azure Sentinel identifies a threat, an incident must be created:

- [✓ Analytics]
- Data connectors
- Playbooks
- Workbooks

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

- Analytics
- Data connectors
- [✓ Playbooks]
- Workbooks

NEW QUESTION 288
- (Exam Topic 4)
You have an Azure subscription that contains the users shown in the following table.



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

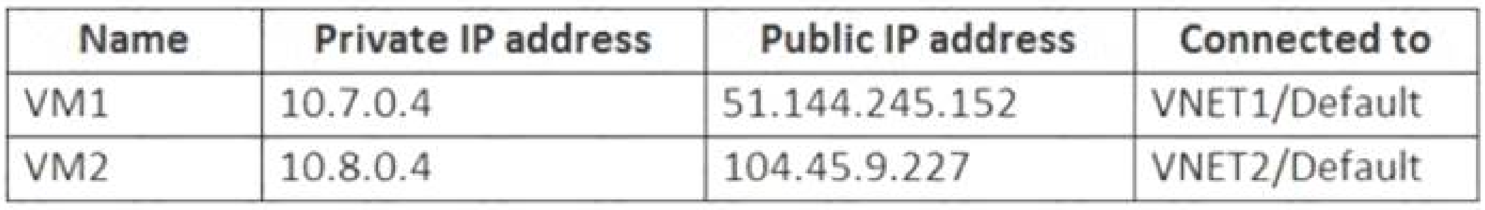
Which users can enable Azure AD Privileged Identity Management (PIM)?

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

Answer: B

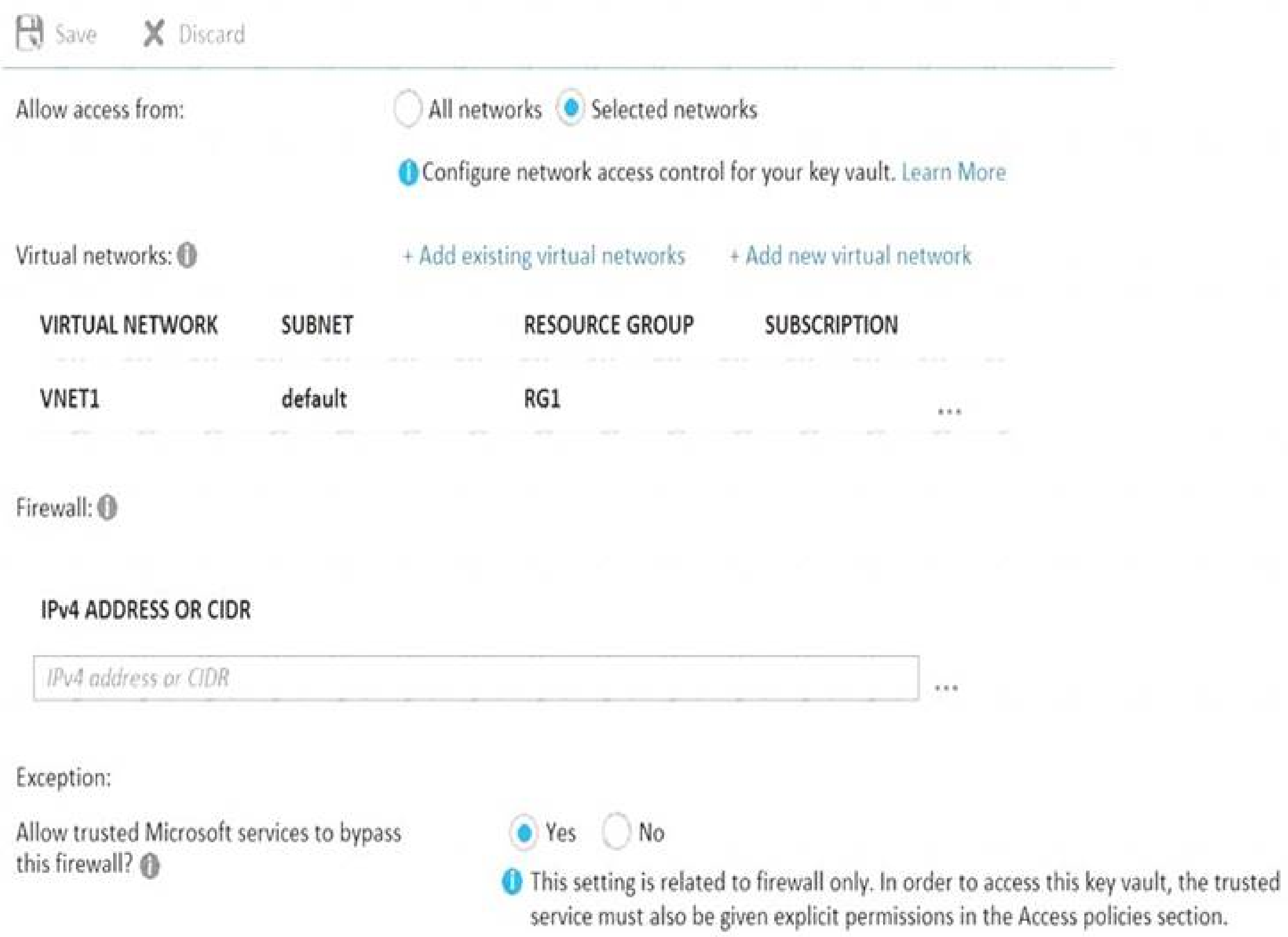
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan

NEW QUESTION 292
- (Exam Topic 4)
You have an Azure subscription that contains an Azure key vault named KeyVault1 and the virtual machines shown in the following table.



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

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



Allow access from: ○ All networks ● Selected networks

Configure network access control for your key vault. Learn More

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

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

Firewall:

IPv4 ADDRESS OR CIDR

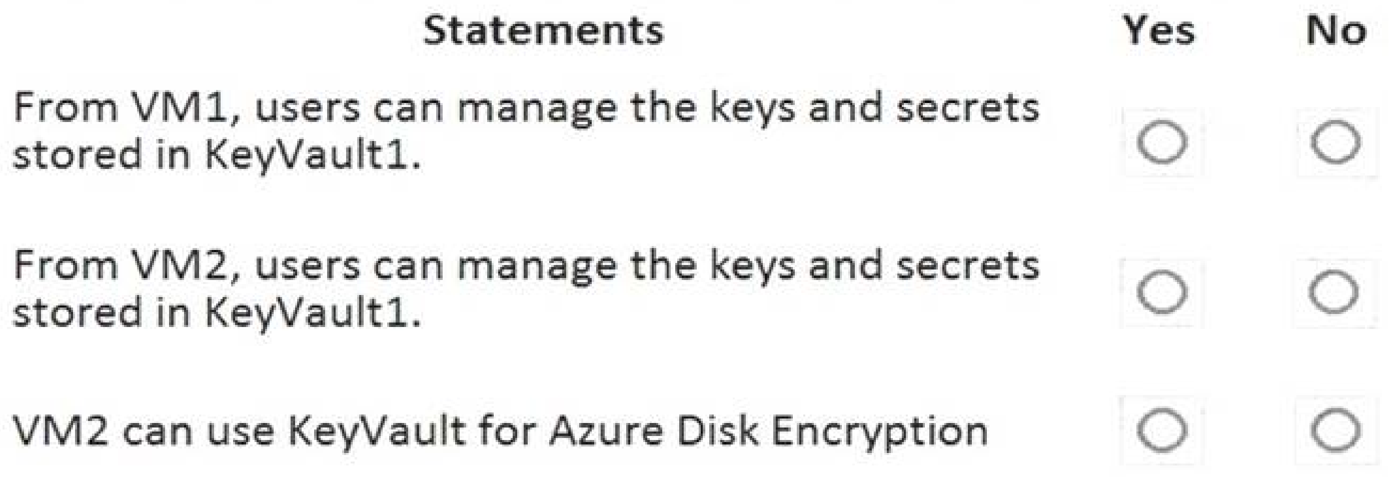
IPv4 address or CIDR ...

Exception:

Allow trusted Microsoft services to bypass this firewall? ● Yes ○ No

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

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

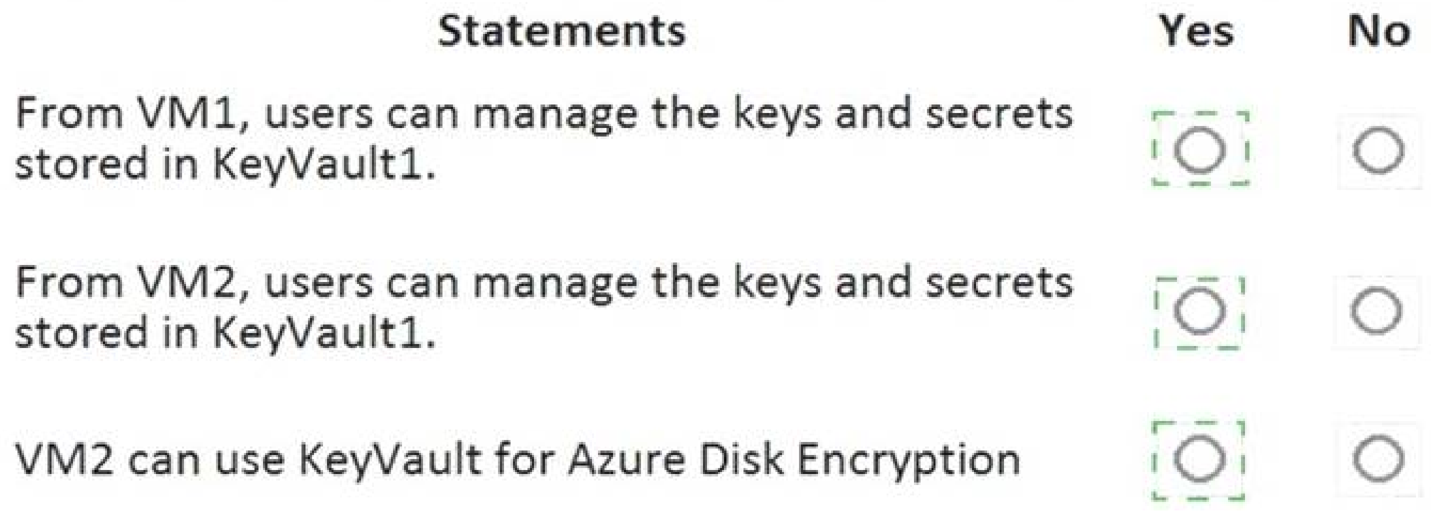


Statements	Yes	No
From VM1, users can manage the keys and secrets stored in KeyVault1.	○	○
From VM2, users can manage the keys and secrets stored in KeyVault1.	○	○
VM2 can use KeyVault for Azure Disk Encryption	○	○

A. Mastered
B. Not Mastered

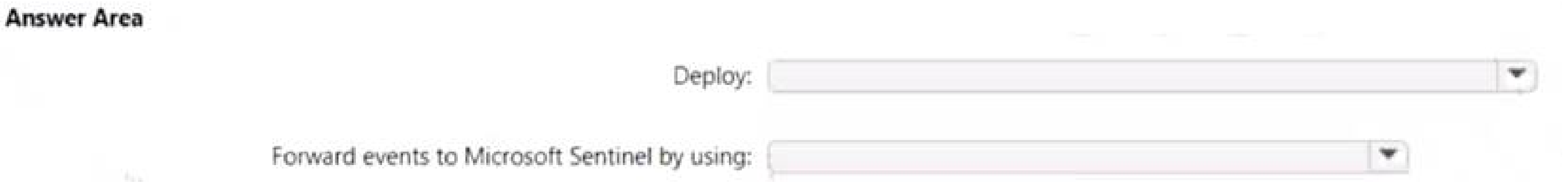
Answer: A

Explanation:



Statements	Yes	No
From VM1, users can manage the keys and secrets stored in KeyVault1.	[✓ ○]	○
From VM2, users can manage the keys and secrets stored in KeyVault1.	[✓ ○]	○
VM2 can use KeyVault for Azure Disk Encryption	[✓ ○]	○

NEW QUESTION 293
- (Exam Topic 4)
You have a Microsoft Sentinel deployment.
You need to connect a third-party security solution to the deployment. The third-party solution will send Common Event Format (CER-formatted messages.
What should you include in the solution? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

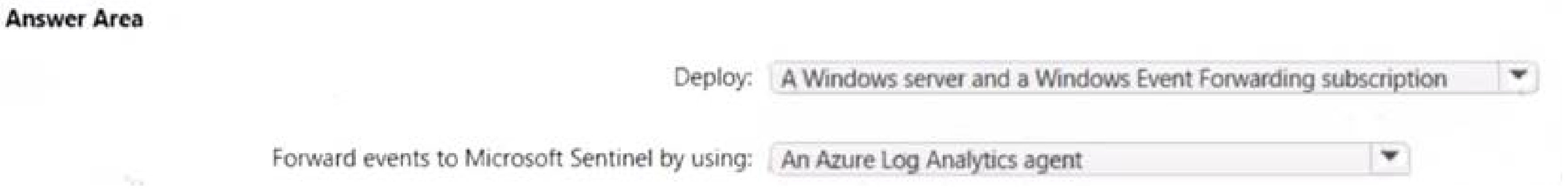
Deploy:

Forward events to Microsoft Sentinel by using:

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Deploy: A Windows server and a Windows Event Forwarding subscription

Forward events to Microsoft Sentinel by using: An Azure Log Analytics agent

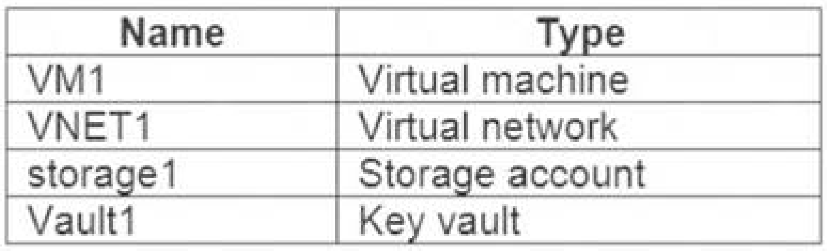
NEW QUESTION 296
- (Exam Topic 4)
Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
Your company has an Active Directory forest with a single domain, named weylandindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.
You have been tasked with integrating Active Directory and the Azure AD tenant. You intend to deploy Azure AD Connect.
Your strategy for the integration must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.
Solution: You recommend the use of federation with Active Directory Federation Services (AD FS). Does the solution meet the goal?

A. Yes
B. No

Answer: B

Explanation:
A federated authentication system relies on an external trusted system to authenticate users. Some companies want to reuse their existing federated system investment with their Azure AD hybrid identity solution. The maintenance and management of the federated system falls outside the control of Azure AD. It's up to the organization by using the federated system to make sure it's deployed securely and can handle the authentication load.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

NEW QUESTION 300
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following Table.



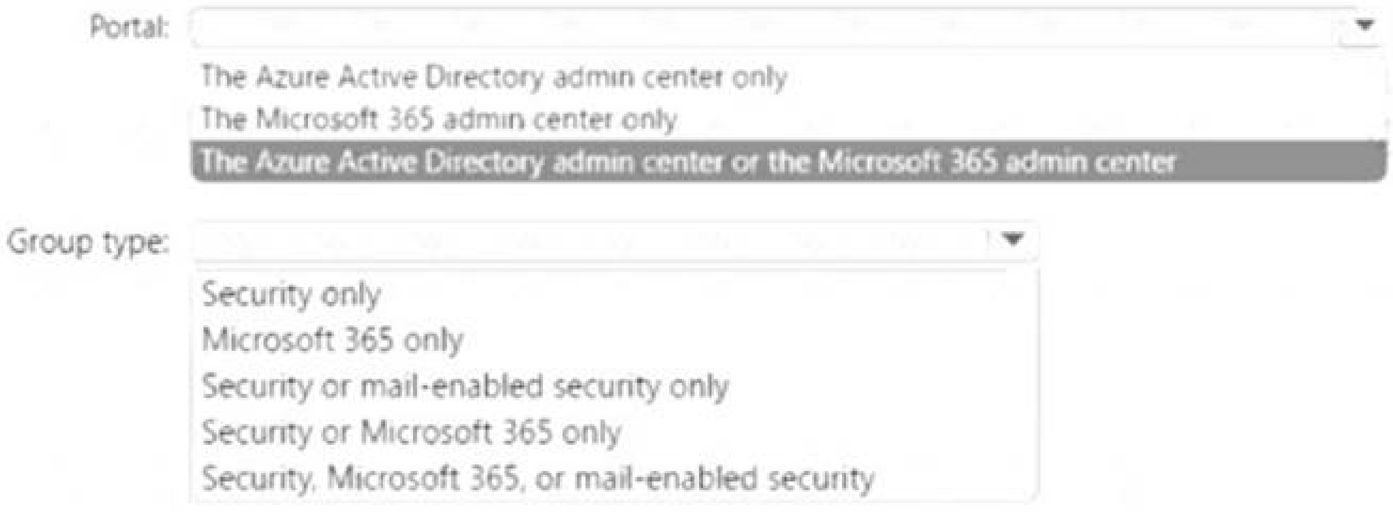
Name	Type
VM1	Virtual machine
VNET1	Virtual network
storage1	Storage account
Vault1	Key vault

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

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

Answer: C

NEW QUESTION 305
- (Exam Topic 4)
You have an Azure AD tenant named contoso.com that has Azure AD Premium P1 licenses. You need to create a group named Group1 that will be assigned the Global reader role.
Which portal should you use to create Group1 and which type of group should you create? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point



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

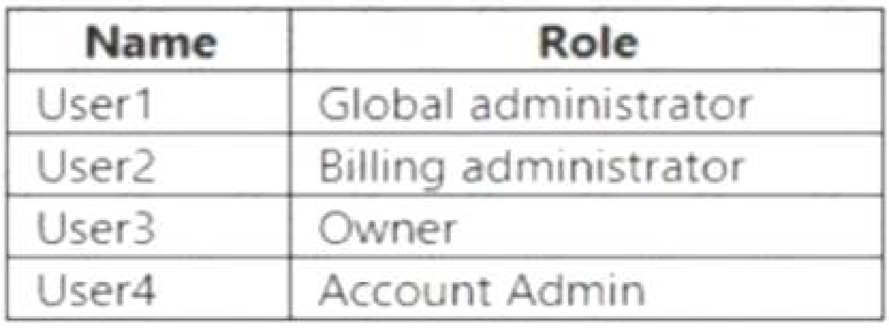
Group type:
- Security only
- Microsoft 365 only
- Security or mail-enabled security only
- Security or Microsoft 365 only
- Security, Microsoft 365, or mail-enabled security

A. Mastered
B. Not Mastered

Answer: A

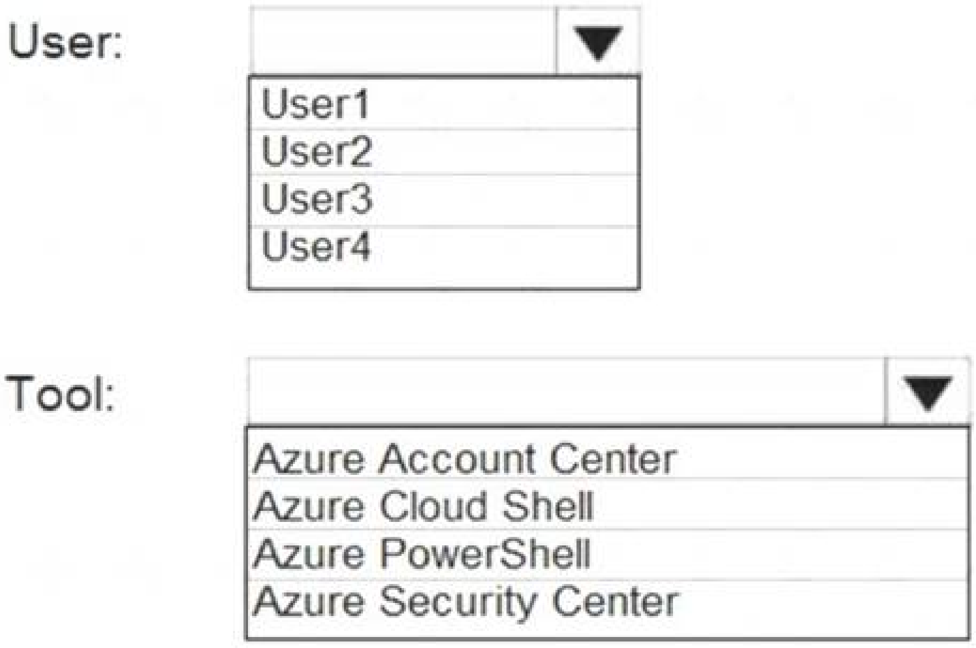
Explanation:
https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-create-eligible

NEW QUESTION 310
- (Exam Topic 4)
HOTSPOT
Your company has an Azure subscription named Subscription1 that contains the users shown in the following table.



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

The company is sold to a new owner.
The company needs to transfer ownership of Subscription1.
Which user can transfer the ownership and which tool should the user use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



User:
- User1
- User2
- User3
- User4

Tool:
- Azure Account Center
- Azure Cloud Shell
- Azure PowerShell
- Azure Security Center

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1; User2
Billing Administrator
Select Transfer billing ownership for the subscription that you want to transfer.
Enter the email address of a user who's a billing administrator of the account that will be the new owner for the subscription.
Box 2: Azure Account Center Azure Account Center can be used. Reference:
https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transfer-billing-ownership-of-an-azu

NEW QUESTION 313
- (Exam Topic 4)
You have an Azure web app named webapp1.

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

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

Answer: B

NEW QUESTION 316
- (Exam Topic 4)
You have an Azure subscription that contains an Azure key vault named Vault1. In Vault1, you create a secret named Secret1.
An application developer registers an application in Azure Active Directory (Azure AD). You need to ensure that the application can use Secret1.
What should you do?

A. In Azure AD, create a role.
B. In Azure Key Vault, create a key.
C. In Azure Key Vault, create an access policy.
D. In Azure AD, enable Azure AD Application Proxy.

Answer: C

Explanation:
"You may need to configure the target resource to allow access from your application. For example, if you request a token to Key Vault, you need to make sure you have added an access policy that includes your application's identity. Otherwise, your calls to Key Vault will be rejected, even if they include the token"
https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity?tabs=dotnet

NEW QUESTION 320
- (Exam Topic 4)
You have an Azure subscription that contains a web app named Appl. App1 provides users with product images and videos. Users access App1 by using a URL of HTTPS://appl.contoso.com. You deploy two server pools named Pool! and Pool2. Pool1 hosts product images. Pool2 hosts product videos. You need to optimize The performance of Appl. The solution must meet the following requirements:
• Minimize the performance impact of TLS connections on Pool1 and Pool2.
• Route user requests to the server pools based on the requested URL path. What should you include in the solution?

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

Answer: C

NEW QUESTION 324
- (Exam Topic 4)
You have an Azure subscription named Sub1.
In Azure Security Center, you have a security playbook named Play1. Play1 is configured to send an email message to a user named User1.
You need to modify Play1 to send email messages to a distribution group named Alerts. What should you use to modify Play1?

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

Answer: D

Explanation:
You can change an existing playbook in Security Center to add an action, or conditions. To do that you just need to click on the name of the playbook that you want to change, in the Playbooks tab, and Logic App Designer opens up.
References:
https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks

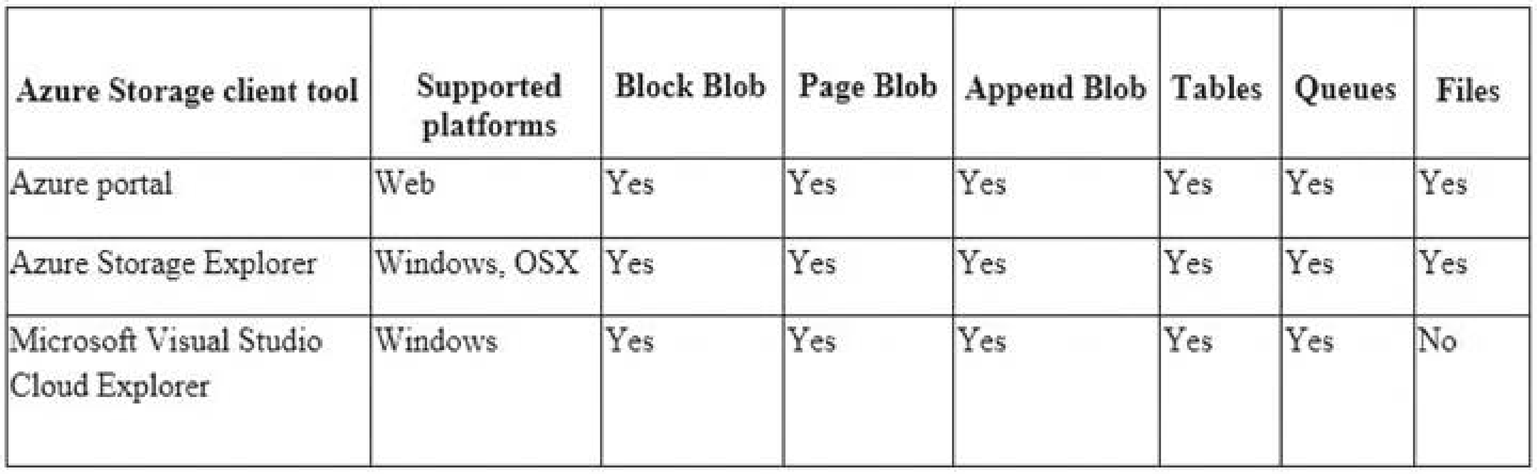
NEW QUESTION 328
- (Exam Topic 4)
You are troubleshooting a security issue for an Azure Storage account. You enable the diagnostic logs for the storage account.
What should you use to retrieve the diagnostics logs?

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

Answer: A

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

table are free.



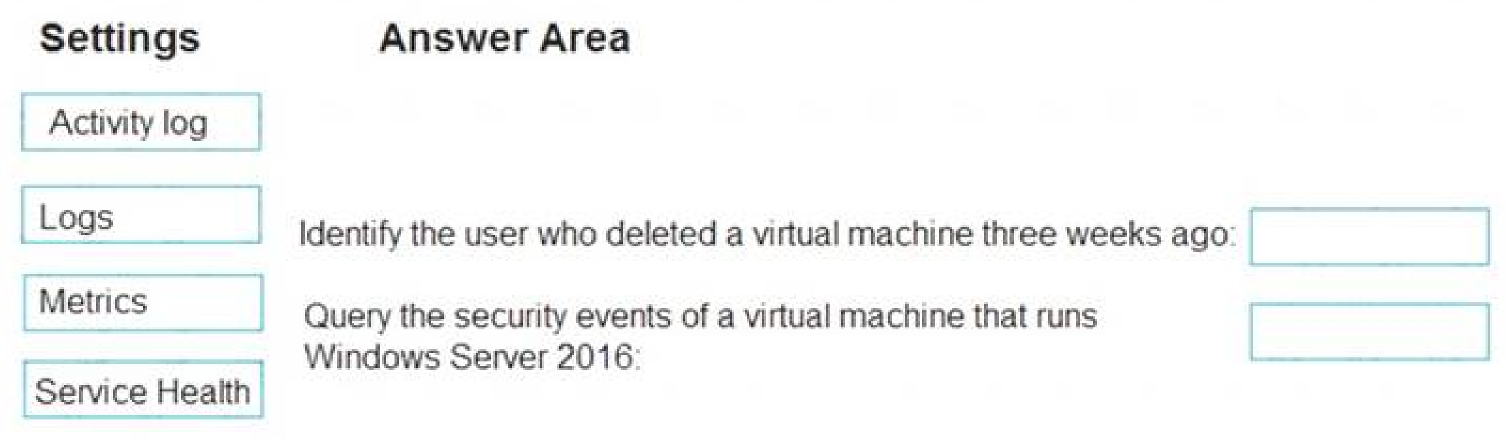
Azure Storage client tool	Supported platforms	Block Blob	Page Blob	Append Blob	Tables	Queues	Files
Azure portal	Web	Yes	Yes	Yes	Yes	Yes	Yes
Azure Storage Explorer	Windows, OSX	Yes	Yes	Yes	Yes	Yes	Yes
Microsoft Visual Studio Cloud Explorer	Windows	Yes	Yes	Yes	Yes	Yes	No

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

NEW QUESTION 333
- (Exam Topic 4)
You have an Azure subscription that contains 100 virtual machines. Azure Diagnostics is enabled on all the virtual machines.
You are planning the monitoring of Azure services in the subscription. You need to retrieve the following details:

- Identify the user who deleted a virtual machine three weeks ago.
- Query the security events of a virtual machine that runs Windows Server 2016.

What should you use in Azure Monitor? To answer, drag the appropriate configuration settings to the correct details. Each configuration setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Settings

Activity log

Logs

Metrics

Service Health

Answer Area

Identify the user who deleted a virtual machine three weeks ago:

Query the security events of a virtual machine that runs Windows Server 2016:

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box1: Activity log
Azure activity logs provide insight into the operations that were performed on resources in your subscription. Activity logs were previously known as “audit logs” or “operational logs,” because they report control-plane events for your subscriptions.
Activity logs help you determine the “what, who, and when” for write operations (that is, PUT, POST, or DELETE).
Box 2: Logs
Log Integration collects Azure diagnostics from your Windows virtual machines, Azure activity logs, Azure Security Center alerts, and Azure resource provider logs. This integration provides a unified dashboard for all your assets, whether they're on-premises or in the cloud, so that you can aggregate, correlate, analyze, and alert for security events.
References:
https://docs.microsoft.com/en-us/azure/security/azure-log-audit

NEW QUESTION 334
......