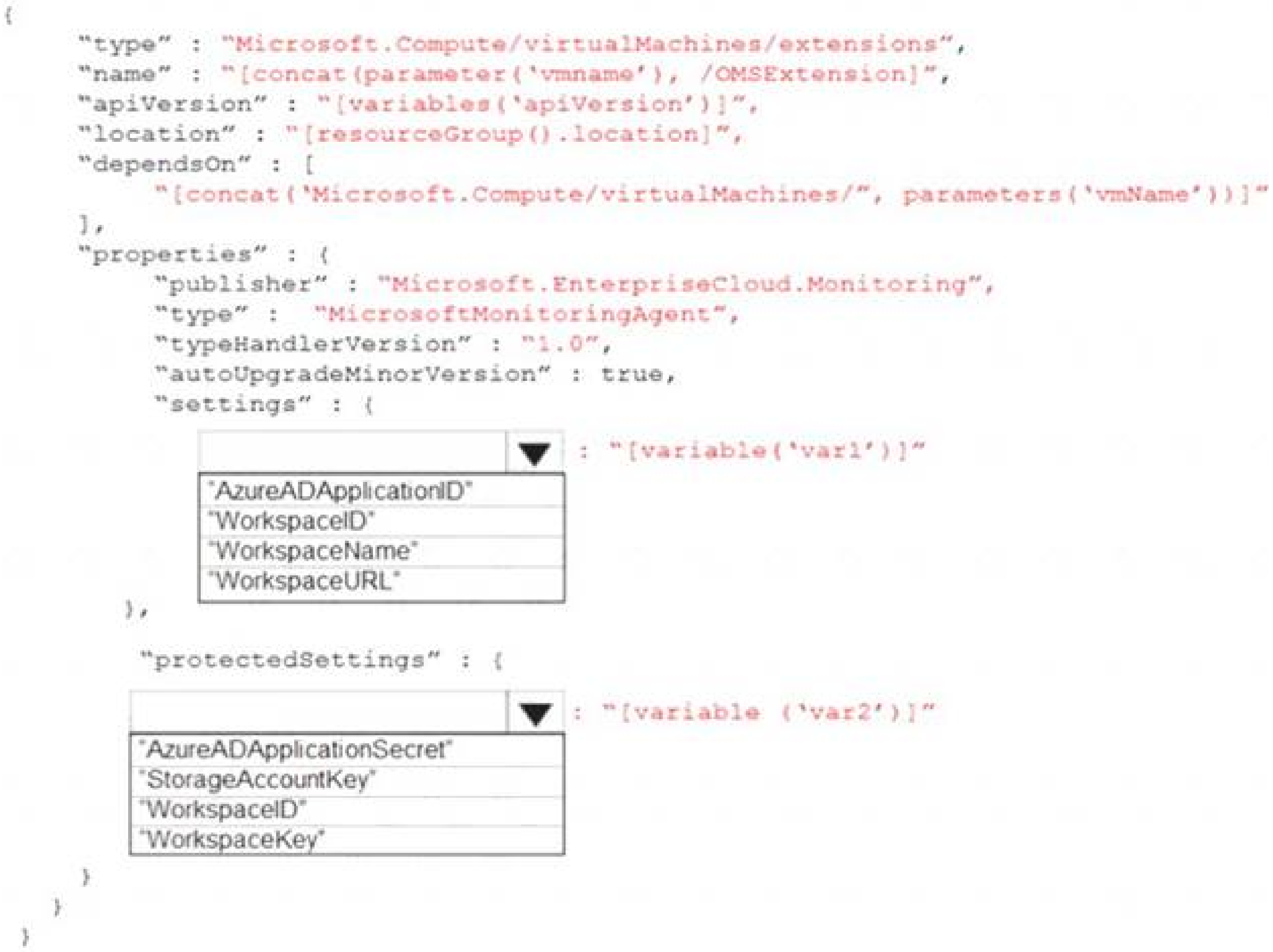
Microsoft

Exam Questions az-500

Microsoft Azure Security Technologies

NEW QUESTION 1
- (Exam Topic 4)
You plan to use Azure Log Analytics to collect logs from 200 servers that run Windows Server 2016.
You need to automate the deployment of the Microsoft Monitoring Agent to all the servers by using an Azure Resource Manager template.
How should you complete the template? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



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

          "protectedSettings" : {
          [               ▼] : "[variable ('var2')]"
          "AzureADApplicationSecret"
          "StorageAccountKey"
          "WorkspaceID"
          "WorkspaceKey"
       }
    }
 }
```

A. Mastered
B. Not Mastered

Answer: A

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

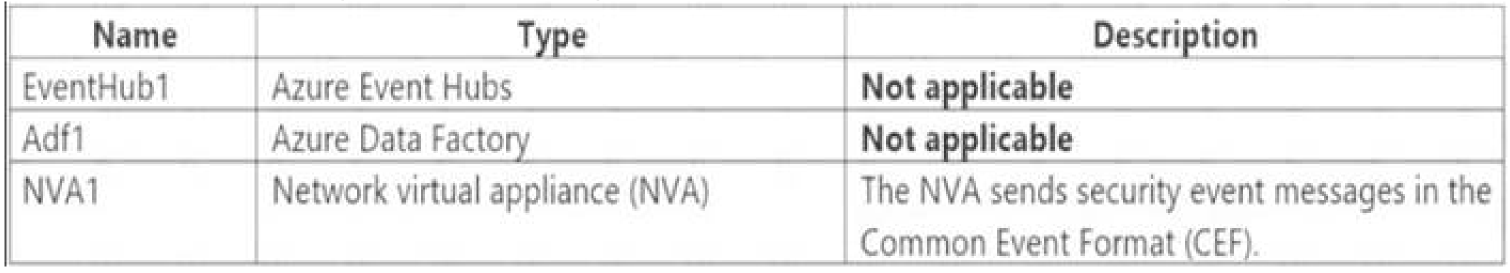
NEW QUESTION 2
- (Exam Topic 4)
You have an Azure subscription.
You configure the subscription to use a different Azure Active Directory (Azure AD) tenant. What are two possible effects of the change? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Role assignments at the subscription level are lost.
B. Virtual machine managed identities are lost.
C. Virtual machine disk snapshots are lost.
D. Existing Azure resources are deleted.

Answer: AB

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-subscriptions-associ

NEW QUESTION 3
- (Exam Topic 4)
You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

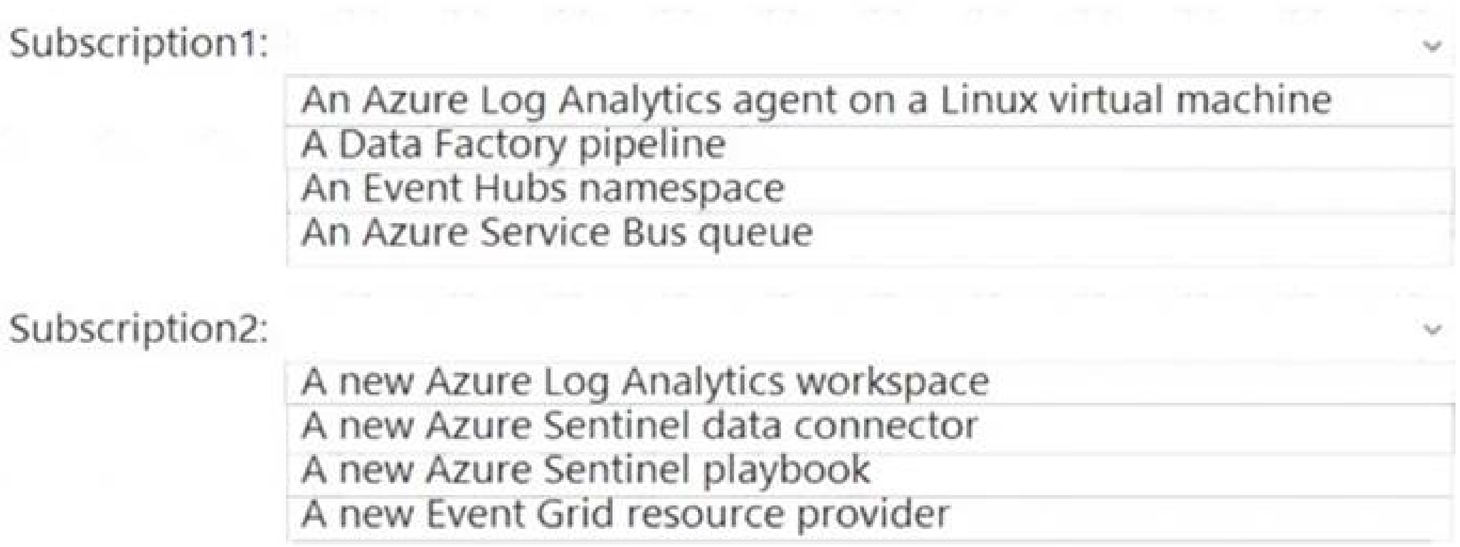


Name	Type	Description
EventHub1	Azure Event Hubs	**Not applicable**
Adf1	Azure Data Factory	**Not applicable**
NVA1	Network virtual appliance (NVA)	The NVA sends security event messages in the Common Event Format (CEF).

You have an Azure subscription named Subscription2 that contains the following resources:
- An Azure Sentinel workspace
- An Azure Event Grid instance

You need to ingest the CEF messages from the NVAs to Azure Sentinel.
What should you configure for each subscription? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Subscription1:

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

Subscription2:

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

A. Mastered
B. Not Mastered

Answer: A

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

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

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

Answer: C

NEW QUESTION 5
- (Exam Topic 4)
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 6
- (Exam Topic 4)
Lab Task
Task 5
A user named Debbie has the Azure app installed on her mobile device.
You need to ensure that debbie@contoso.com is alerted when a resource lock is deleted.

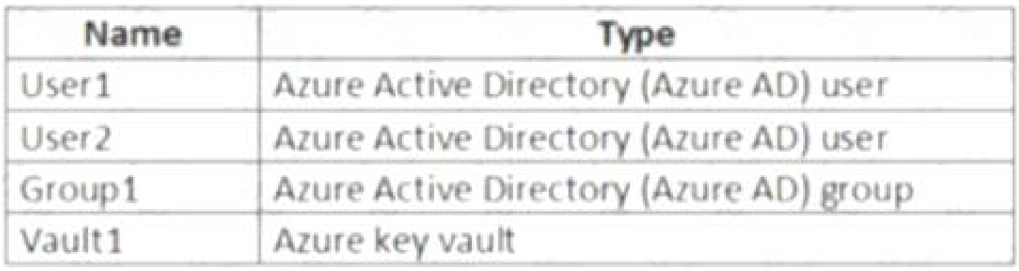
A. Mastered
B. Not Mastered

Answer: A

Explanation:

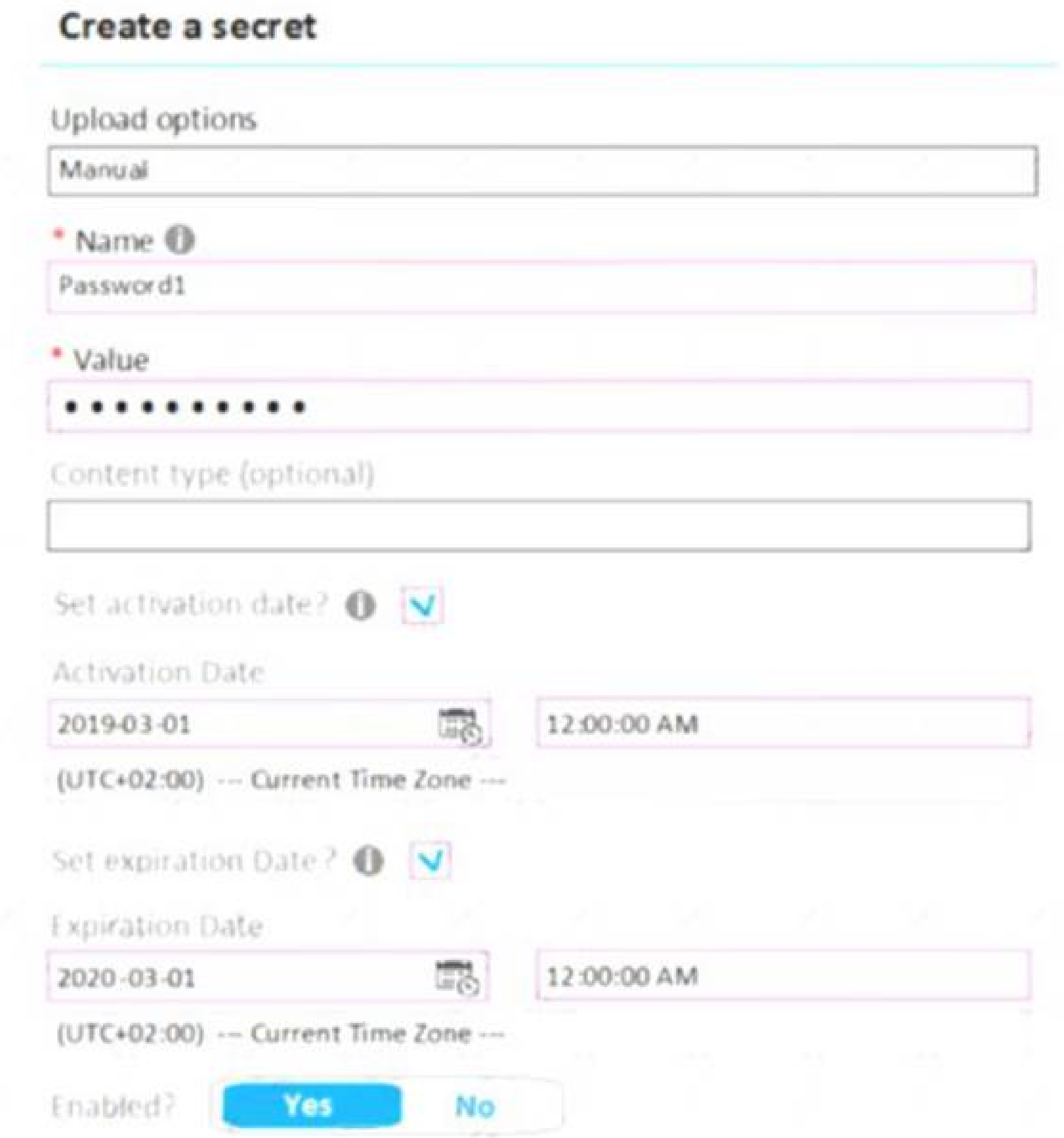
Create an Azure Resource Manager service principal. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to specify a name and a role for the service principal, such as Contributor.
Grant permission to the service principal to access the secrets in the key vault. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to assign the Key Vault Secrets User role to the service principal at the scope of the key vault or individual secrets.
Enable template deployment for the key vault. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to set the enabledForTemplateDeployment property of the key vault to true.
Reference the secrets in the template by using their resource ID. You can use the listSecrets function to get the resource ID of a secret in the key vault. You need to specify the name of the key vault and the name of the secret as parameters.
Deploy the template by using Azure PowerShell, Azure CLI, or REST API. You can use the New-AzResourceGroupDeployment cmdlet, the az deployment group create command, or the Deployments - Create Or Update REST API to do this. You need to provide the template file or URI and any required parameters. You also need to provide the credentials of the service principal.

NEW QUESTION 7
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.



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

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



Create a secret

Upload options
Manual

* Name
Password1

* Value
••••••••••

Content type (optional)

Set activation date? ☑

Activation Date
2019-03-01 12:00:00 AM
(UTC+02:00) --- Current Time Zone ---

Set expiration Date? ☑

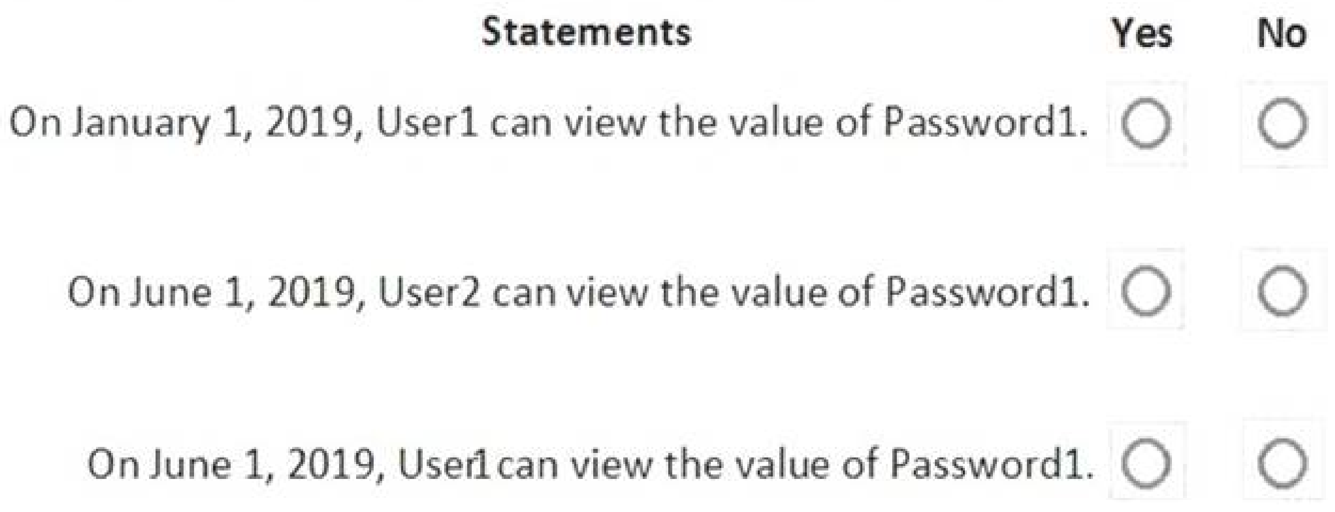
Expiration Date
2020-03-01 12:00:00 AM
(UTC+02:00) --- Current Time Zone ---

Enabled? [✓ Yes] No

User2 is assigned an access policy to Vault1. The policy has the following configurations:
- Key Management Operations: Get, List, and Restore
- Cryptographic Operations: Decrypt and Unwrap Key
- Secret Management Operations: Get, List, and Restore

Group1 is assigned an access to Vault1. The policy has the following configurations:
- Key Management Operations: Get and Recover
- Secret Management Operations: List, Backup, and Recover

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

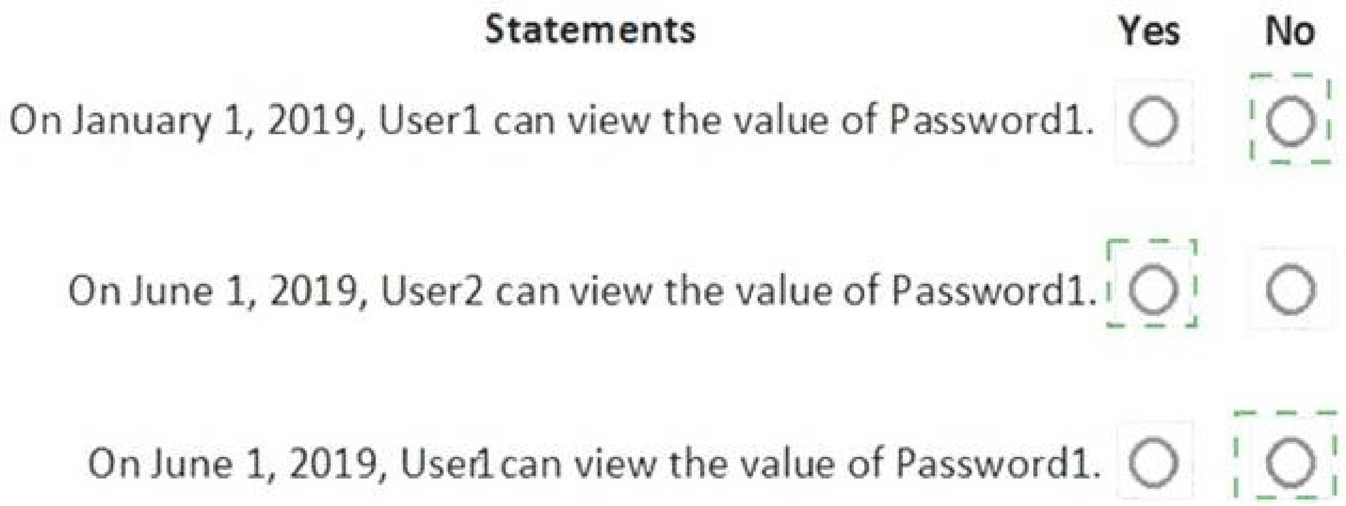


Statements	Yes	No
On January 1, 2019, User1 can view the value of Password1.	○	○
On June 1, 2019, User2 can view the value of Password1.	○	○
On June 1, 2019, User1 can view the value of Password1.	○	○

A. Mastered
B. Not Mastered

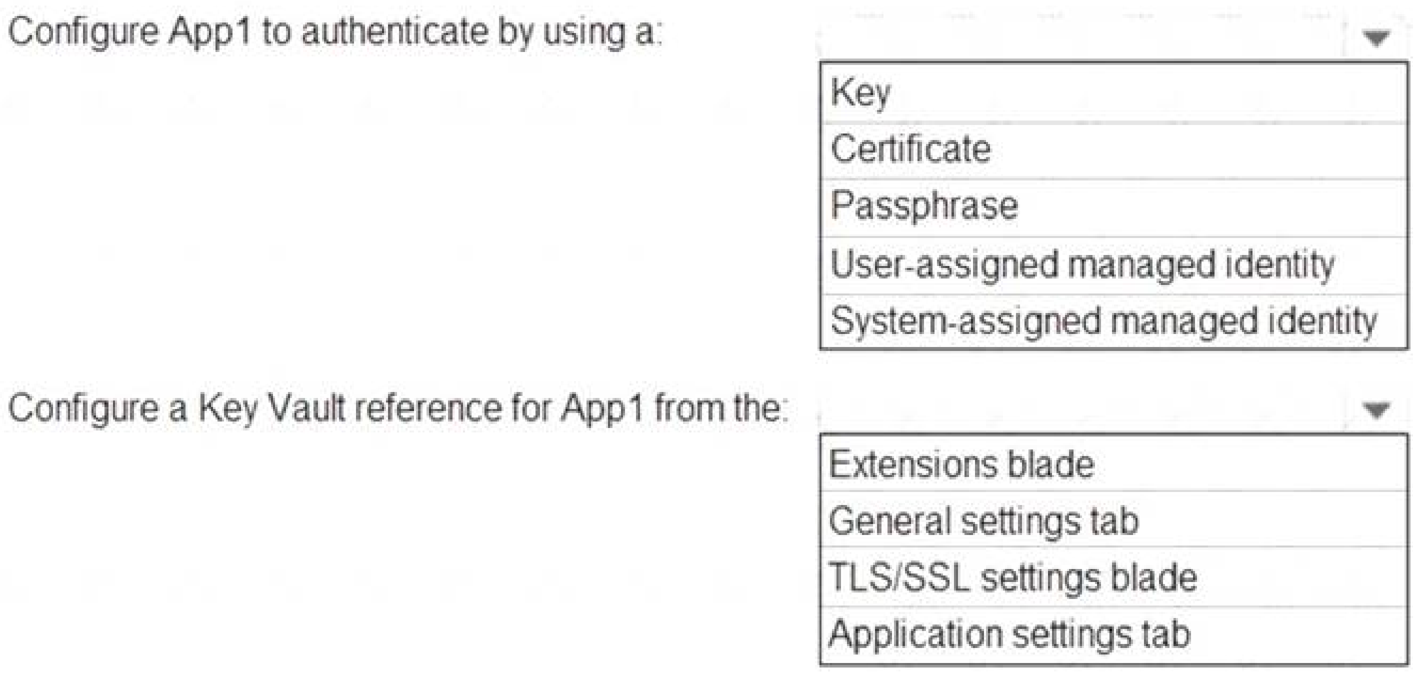
Answer: A

Explanation:



Statements	Yes	No
On January 1, 2019, User1 can view the value of Password1.	○	[✓ ○]
On June 1, 2019, User2 can view the value of Password1.	[✓ ○]	○
On June 1, 2019, User1 can view the value of Password1.	○	[✓ ○]

NEW QUESTION 8
- (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 9
- (Exam Topic 4)
You have multiple development teams that will create apps in Azure.

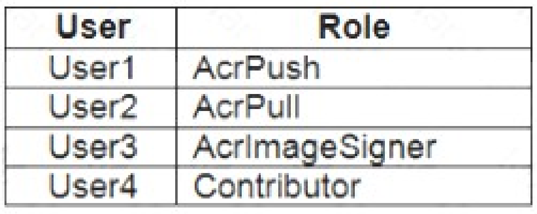
You plan to create a standard development environment that will be deployed for each team.
You need to recommend a solution that will enforce resource locks across the development environments and ensure that the locks are applied in a consistent manner.
What should you include in the recommendation?

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

Answer: D

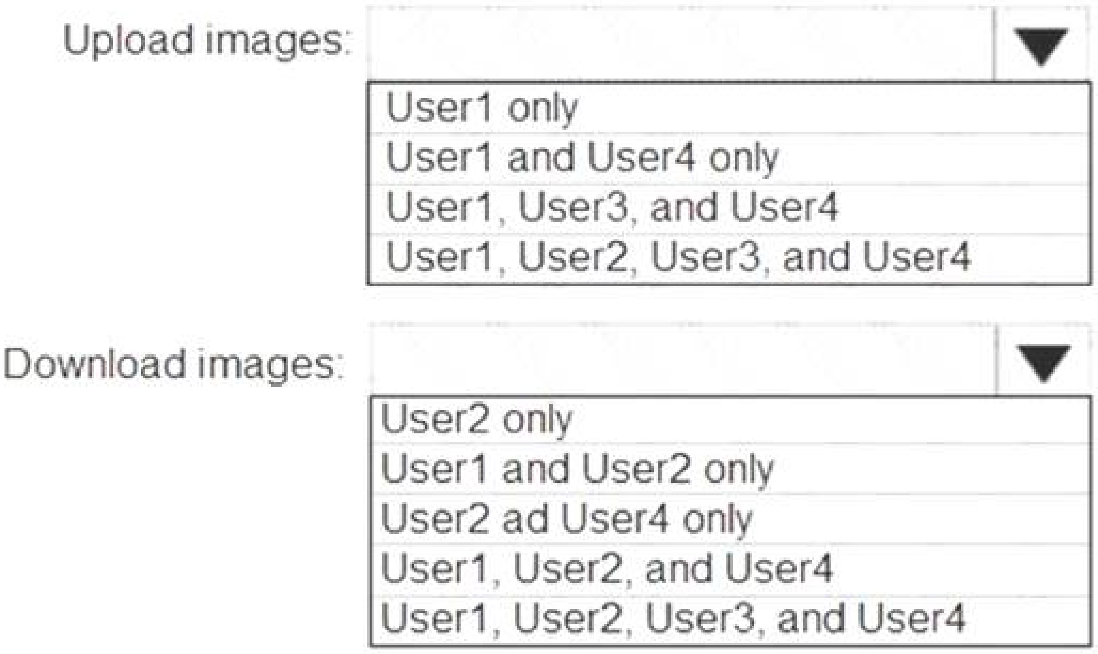
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking

NEW QUESTION 10
- (Exam Topic 4)
You have an Azure 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.



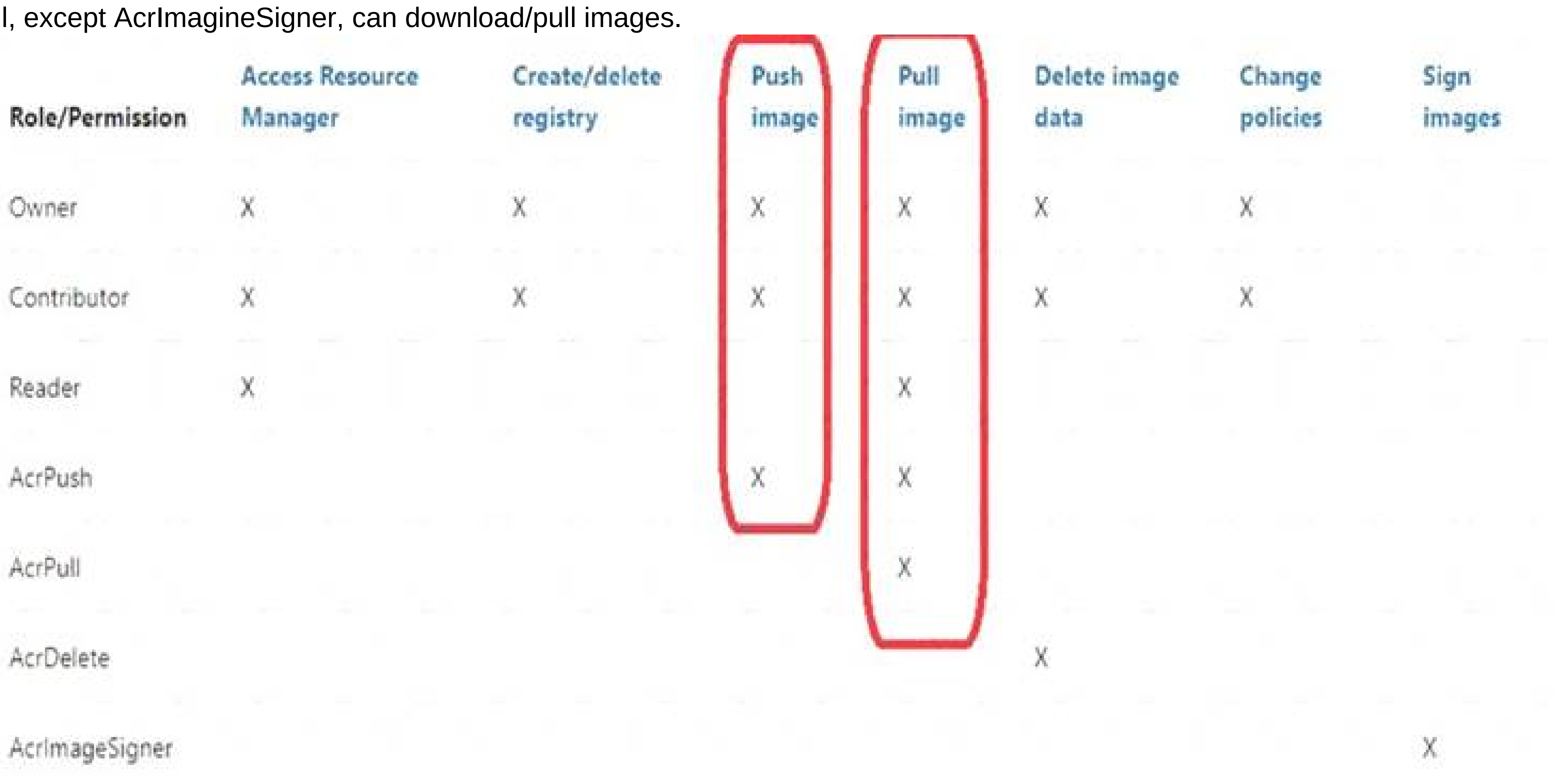
Upload images:
- User1 only
- User1 and User4 only
- User1, User3, and User4
- User1, User2, User3, and User4

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

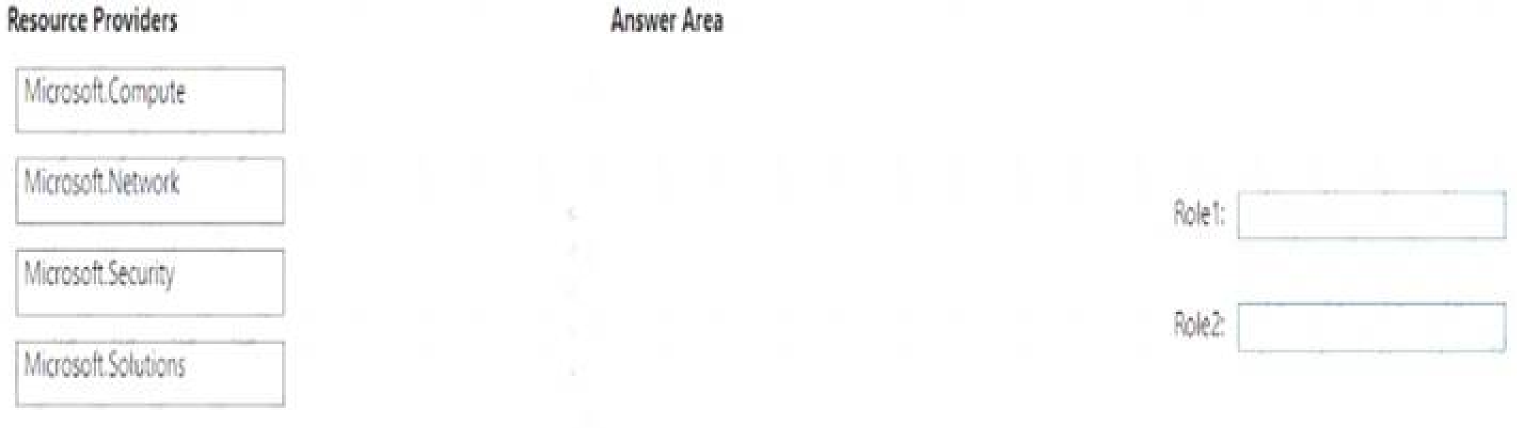
Explanation:
Box 1: User1 and User4 only
Owner, Contributor and AcrPush can push images. Box 2: User1, User2, and User4
All, except AcrImagineSigner, can download/pull images.



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 10
- (Exam Topic 4)
You have an Azure subscription.
You plan to create two custom roles named Role1 and Role2.
The custom roles will be used to perform the following tasks:
• Members of Role1 will manage application security groups.
• Members of Role2 will manage Azure Bastion. You need to add permissions to the custom roles.
Which resource provider should you use for each role? To answer, drag the appropriate resource providers to the correct roles. Each resource provider may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content



Resource Providers

Microsoft.Compute

Microsoft.Network

Microsoft.Security

Microsoft.Solutions

Answer Area

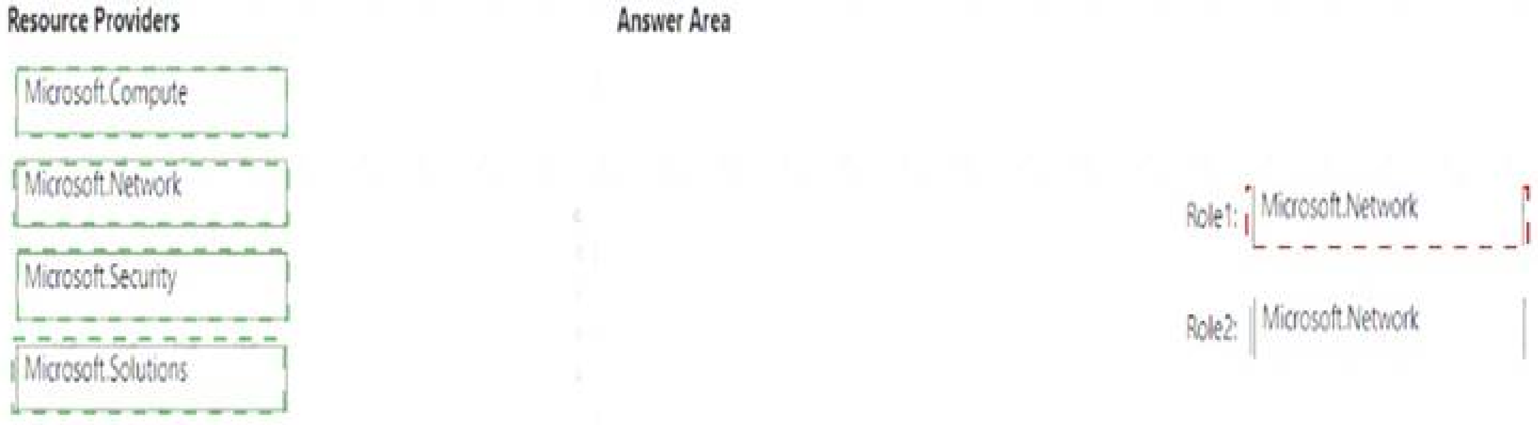
Role1:

Role2:

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Resource Providers

Microsoft.Compute

Microsoft.Network

Microsoft.Security

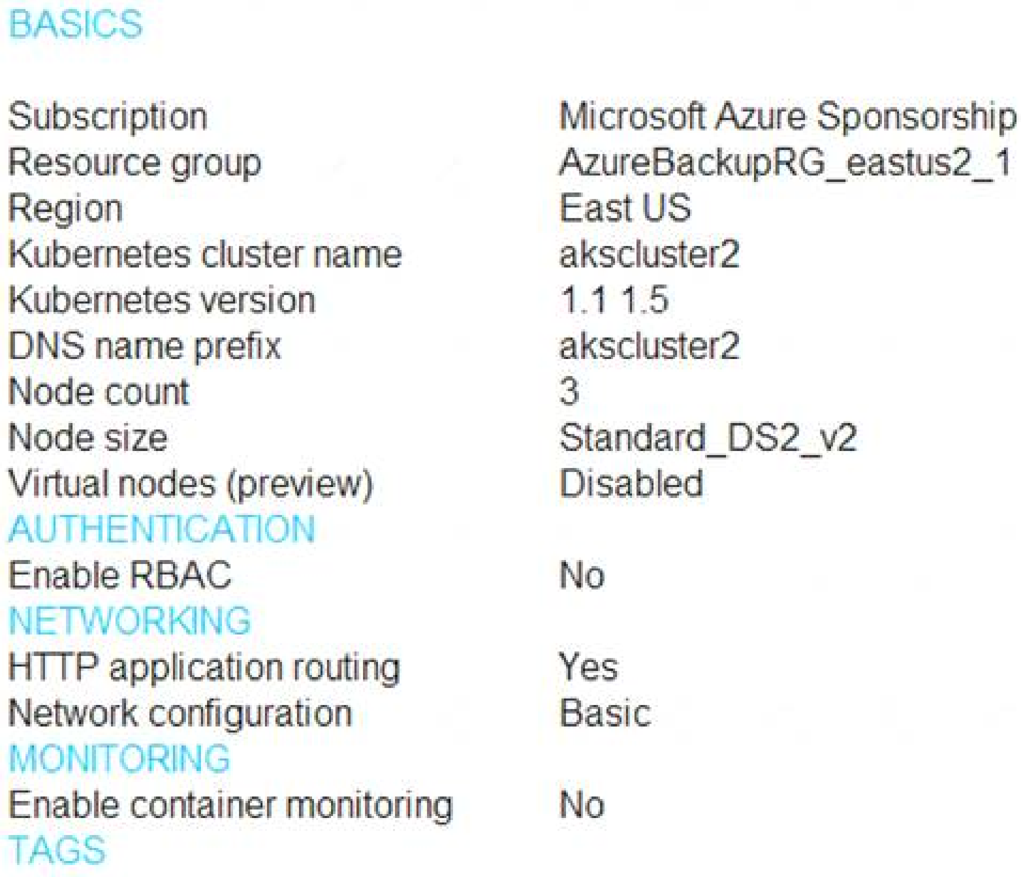
Microsoft.Solutions

Answer Area

Role1: Microsoft.Network

Role2: Microsoft.Network

NEW QUESTION 12
- (Exam Topic 4)
You are testing an Azure Kubernetes Service (AKS) cluster. The cluster is configured as shown in the exhibit. (Click the Exhibit tab.)



BASICS

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

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

A. Create an AKS Ingress controller.

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

Answer: A

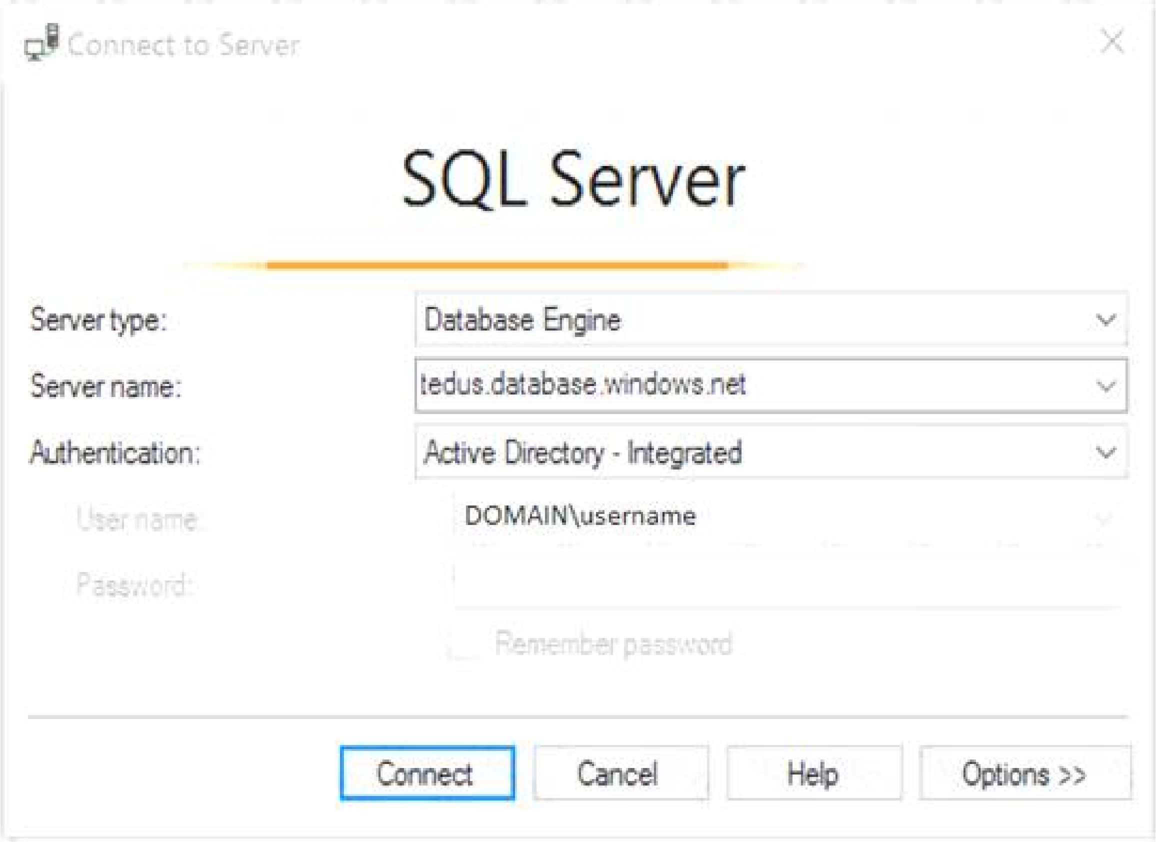
Explanation:
An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services.
References:
https://docs.microsoft.com/en-us/azure/aks/ingress-tls

NEW QUESTION 16
- (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.



Connect to Server

SQL Server

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

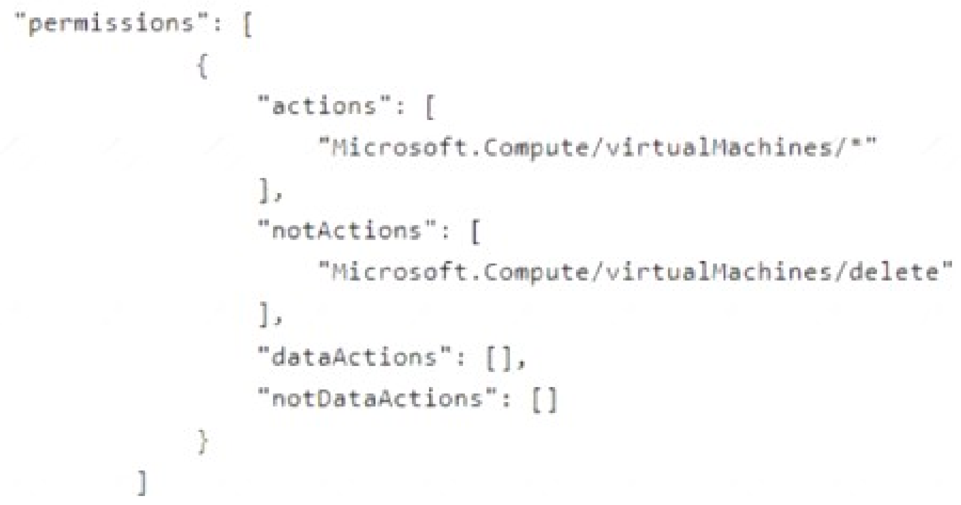
NEW QUESTION 19
- (Exam Topic 4)
You have an Azure subscription named Subscription1.
You need to view which security settings are assigned to Subscription1 by default. Which Azure policy or initiative definition should you review?

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

Answer: B

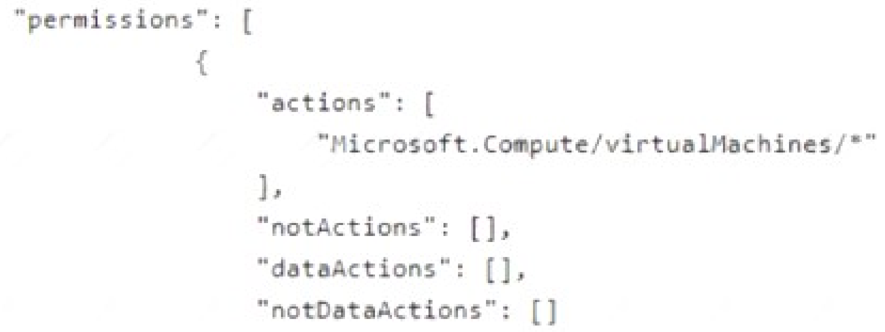
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/tutorial-security-policy https://docs.microsoft.com/en-us/azure/security-center/policy-reference

NEW QUESTION 21
- (Exam Topic 4)
You have an Azure subscription that contains a resource group named RG1. RG1 contains a virtual machine named VM1 that uses Azure Active Directory (Azure AD) authentication.
You have two custom Azure roles named Role1 and Role2 that are scoped to RG1.
The permissions for Role1 are shown in the following JSON code.



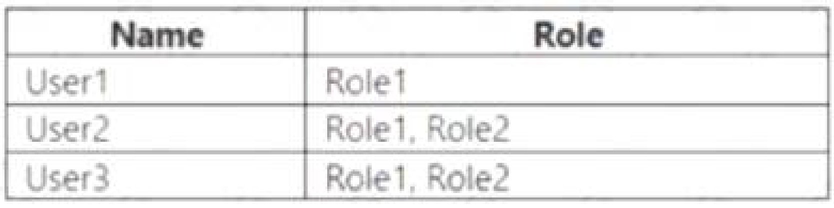
```
"permissions": [
            {
                "actions": [
                    "Microsoft.Compute/virtualMachines/*"
                ],
                "notActions": [
                    "Microsoft.Compute/virtualMachines/delete"
                ],
                "dataActions": [],
          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

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



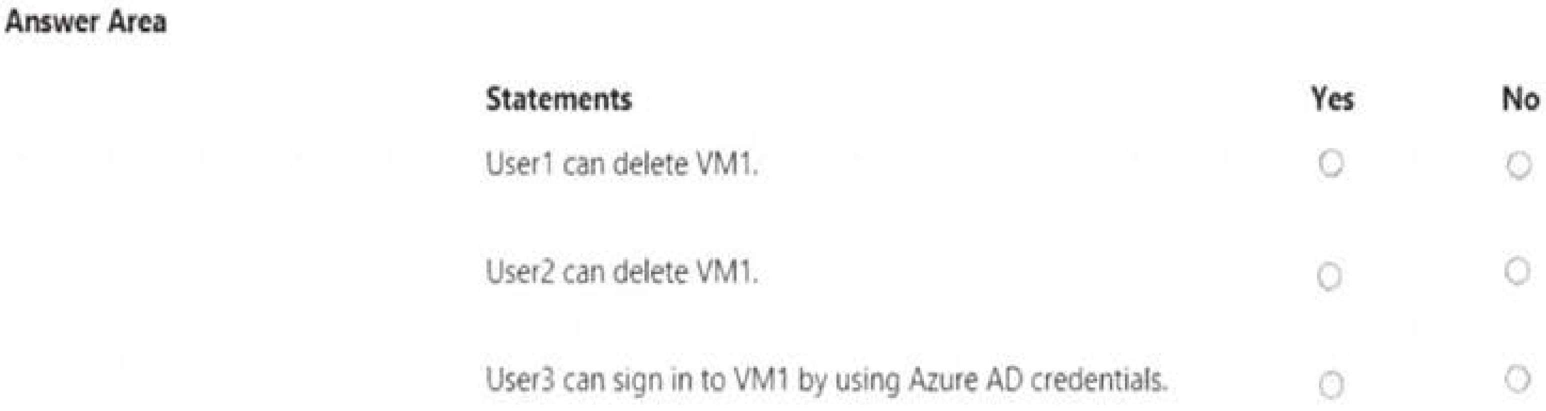
```
"permissions": [
            {
                "actions": [
                    "Microsoft.Compute/virtualMachines/*"
                ],
                "notActions": [],
                "dataActions": [],
                "notDataActions": []
```

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



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

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



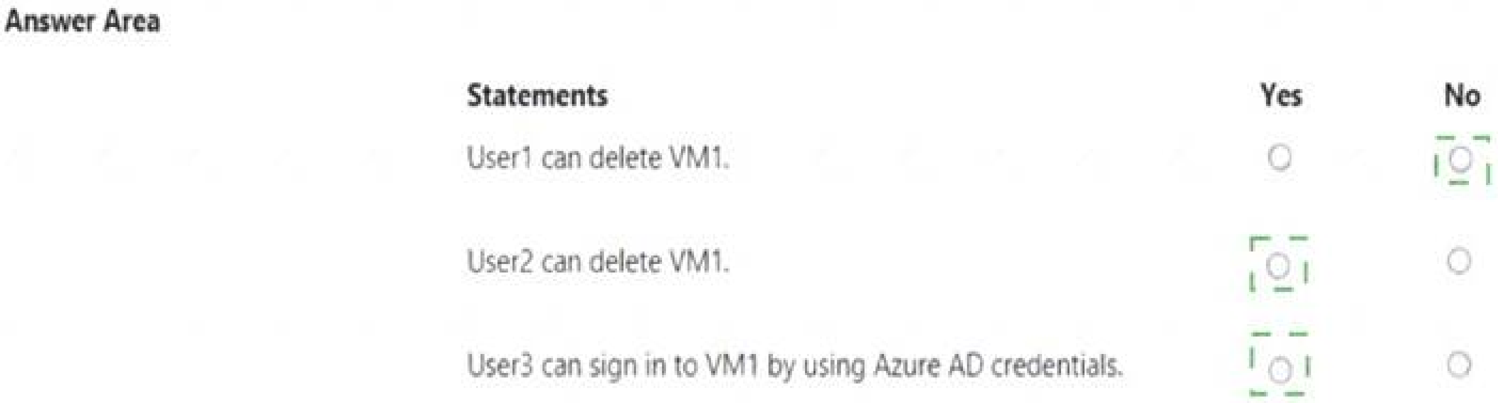
Answer Area

Statements	Yes	No
User1 can delete VM1.	○	○
User2 can delete VM1.	○	○
User3 can sign in to VM1 by using Azure AD credentials.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Statements	Yes	No
User1 can delete VM1.	○	[✓ ○]
User2 can delete VM1.	[✓ ○]	○
User3 can sign in to VM1 by using Azure AD credentials.	[✓ ○]	○

NEW QUESTION 22

- (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.

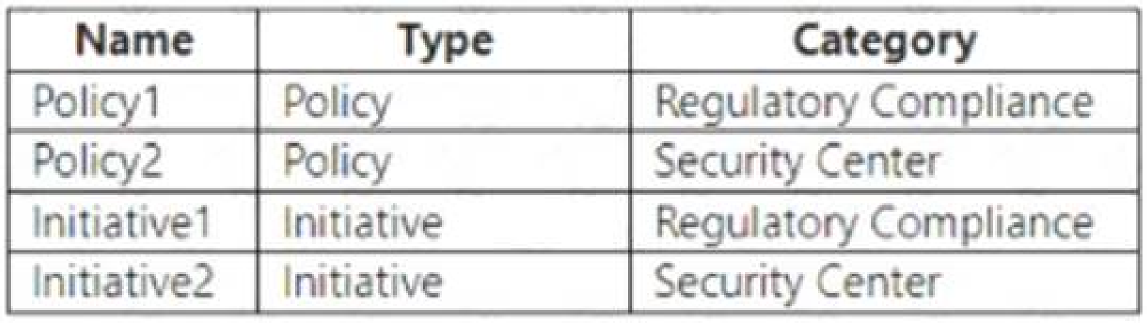
NEW QUESTION 24
- (Exam Topic 4)
From the Azure portal, you are configuring an Azure policy.
You plan to assign policies that use the DeployIfNotExist, AuditIfNotExist, Append, and Deny effects.
Which effect requires a managed identity for the assignment?

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

Answer: C

Explanation:
When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity.
References:
https://docs.microsoft.com/bs-latn-ba/azure/governance/policy/how-to/remediate-resources

NEW QUESTION 29
- (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 31
- (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.

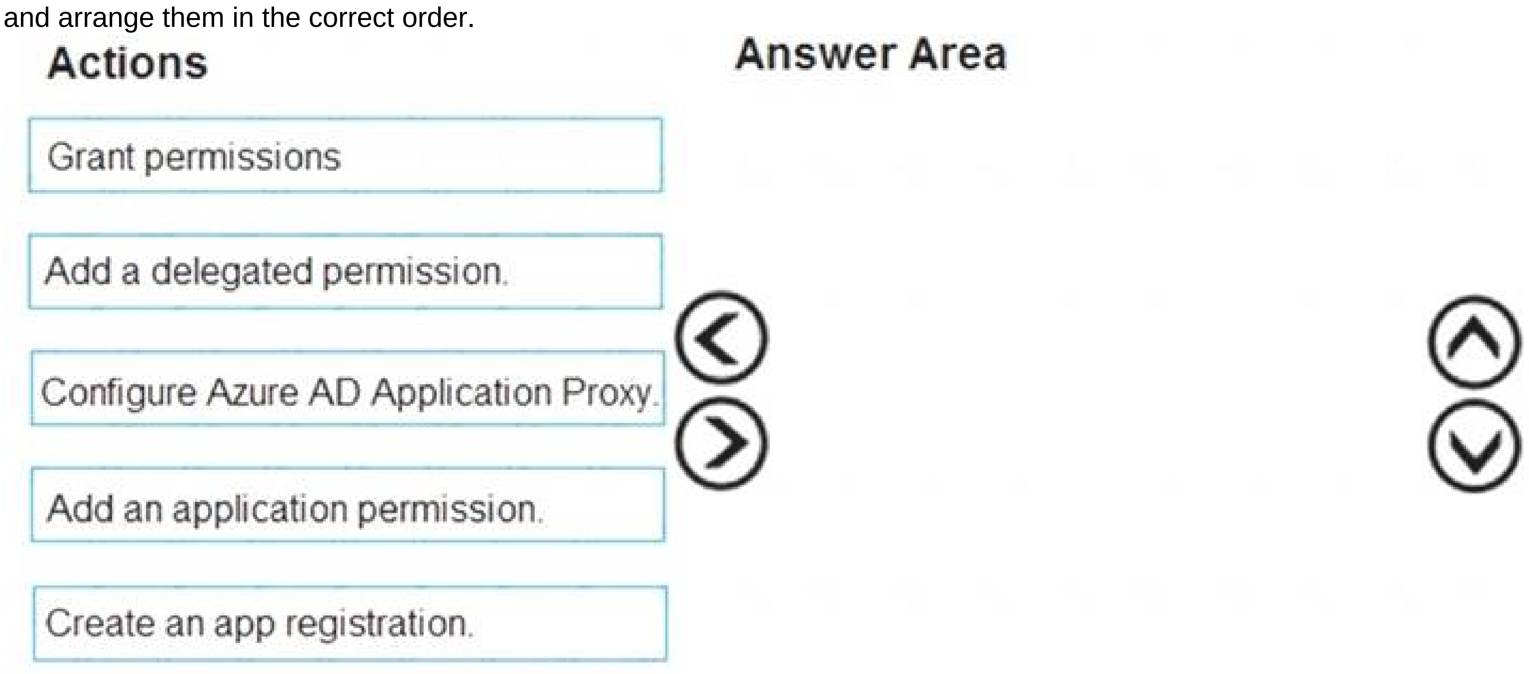
Answer: B

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 33
- (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

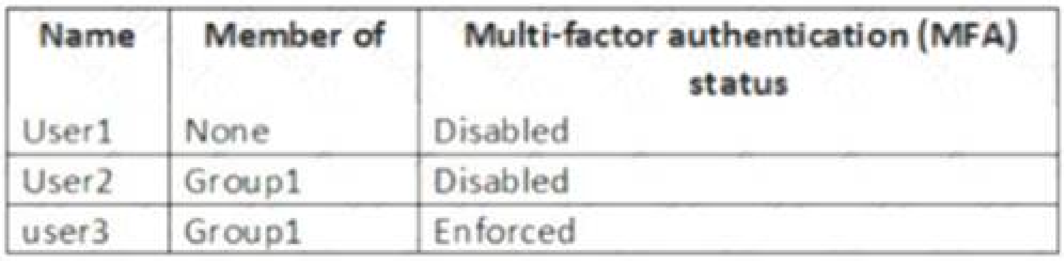
NEW QUESTION 38
- (Exam Topic 4)
You are troubleshooting a security issue for an Azure Storage account.
You enable the diagnostic logs for the storage account. What should you use to retrieve the diagnostics logs?

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 41
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

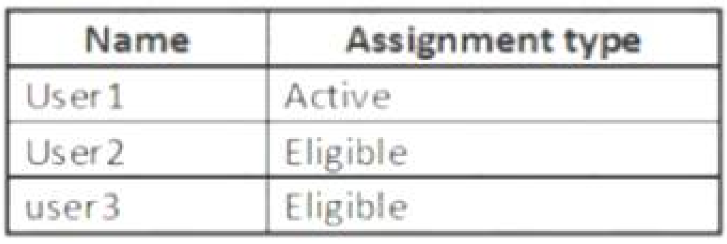


Name	Member of	Multi-factor authentication (MFA) status
User1	None	Disabled
User2	Group1	Disabled
user3	Group1	Enforced

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

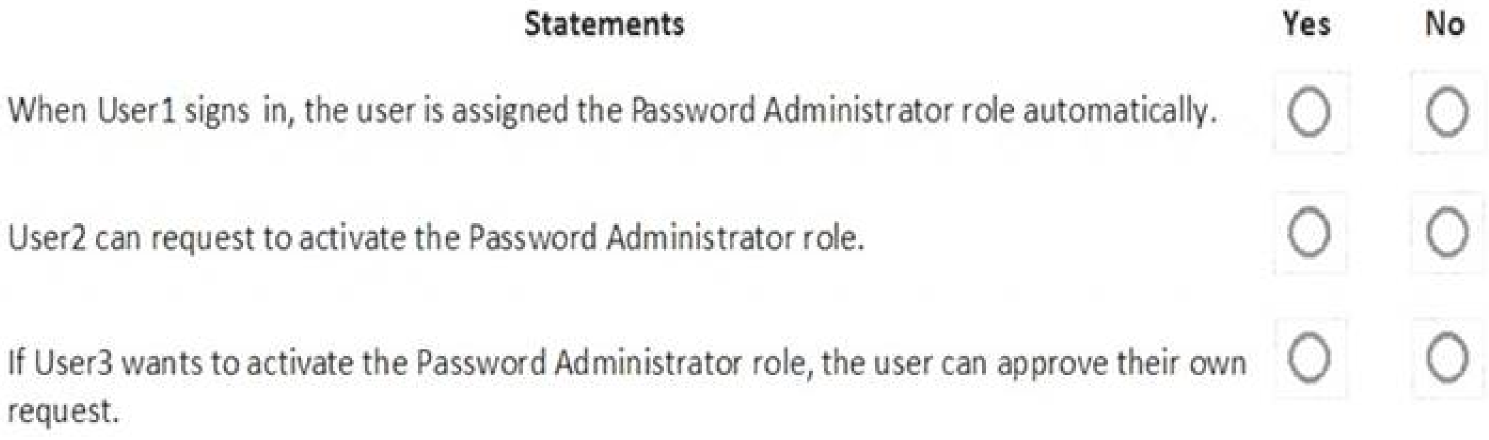
- Maximum activation duration (hours): 2
- Send email notifying admins of activation: Disable
- Require incident/request ticket number during activation: Disable
- Require Azure Multi-Factor Authentication for activation: Enable
- Require approval to activate this role: Enable
- Selected approver: Group1

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



Name	Assignment type
User1	Active
User2	Eligible
user3	Eligible

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



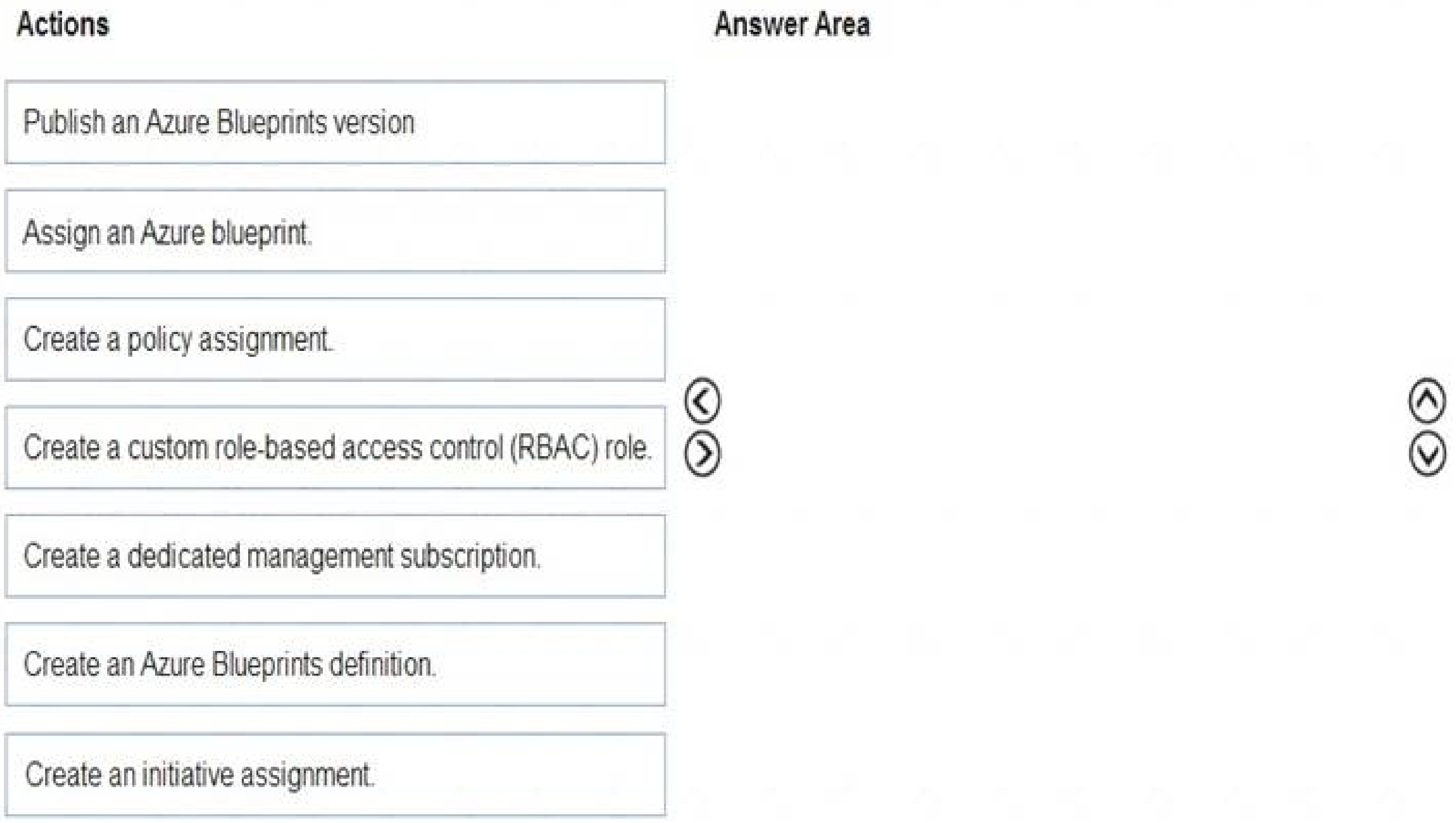
Statements	Yes	No
When User1 signs in, the user is assigned the Password Administrator role automatically.	○	○
User2 can request to activate the Password Administrator role.	○	○
If User3 wants to activate the Password Administrator role, the user can approve their own request.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
YES (Already active)
YES (The user will be prompted for MFA regardless the MFA Status of the user) NO (Even the user is included in the group, a user can't approve itself)
https://docs.microsoft.com/es-es/azure/active-directory/privileged-identity-management/pim-deployment-plan (Require approval section)

NEW QUESTION 46
- (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.

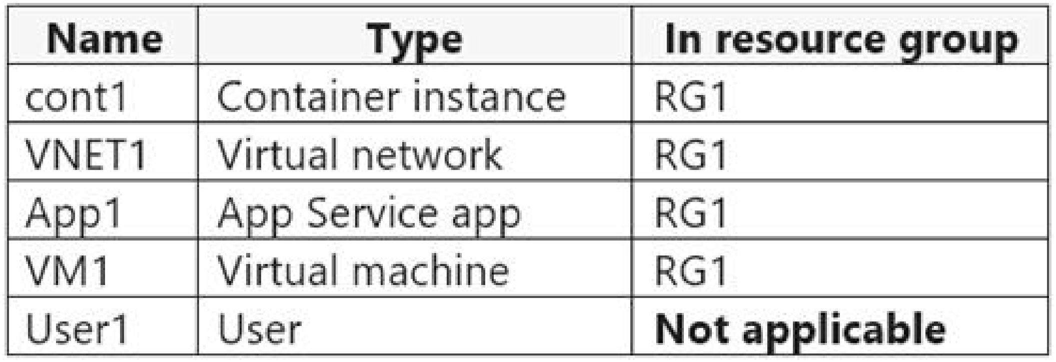
Answer Area

A. Mastered
B. Not Mastered

Answer: A

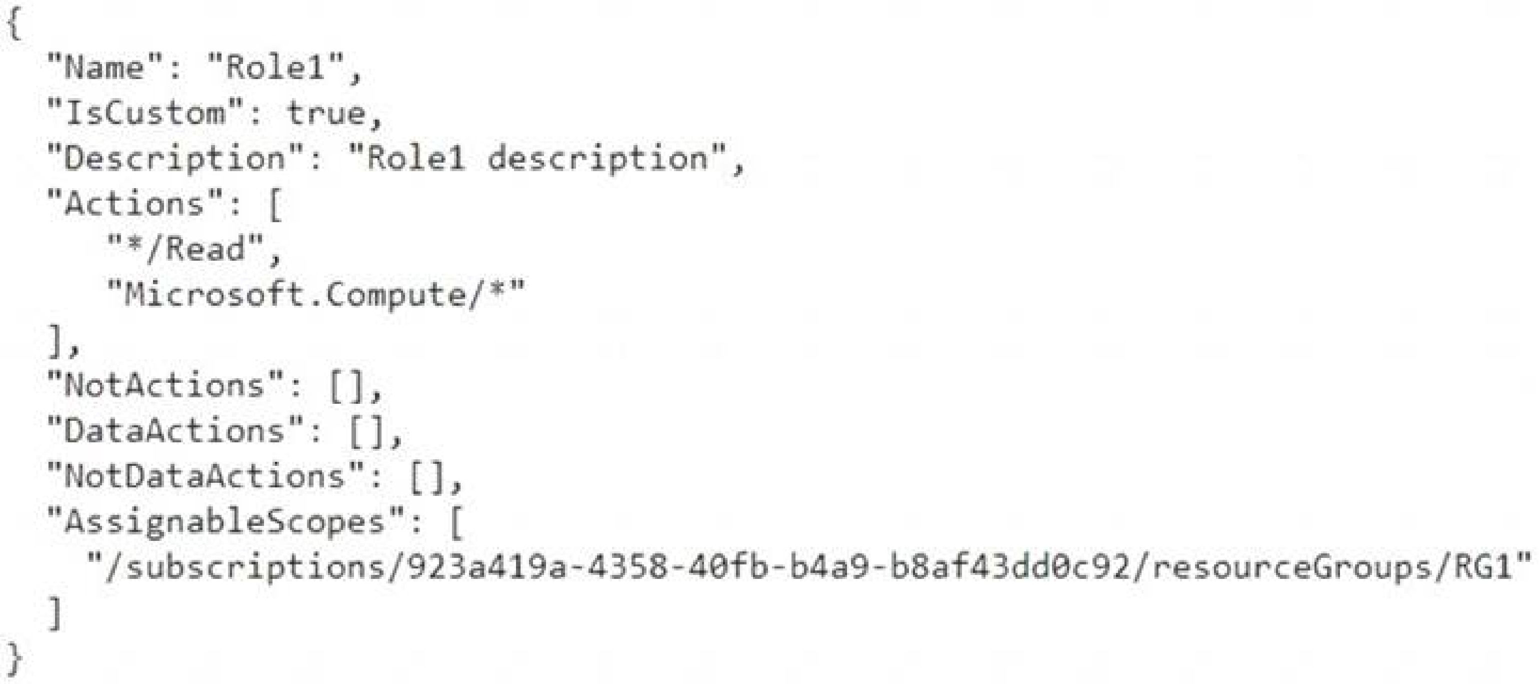
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/governance/blueprints/create-blueprint-portal https://docs.microsoft.com/en-us/azure/azure-australia/azure-policy

NEW QUESTION 48
- (Exam Topic 4)
You have an Azure subscription named Subscription1 that contains the resources shown in the following table.



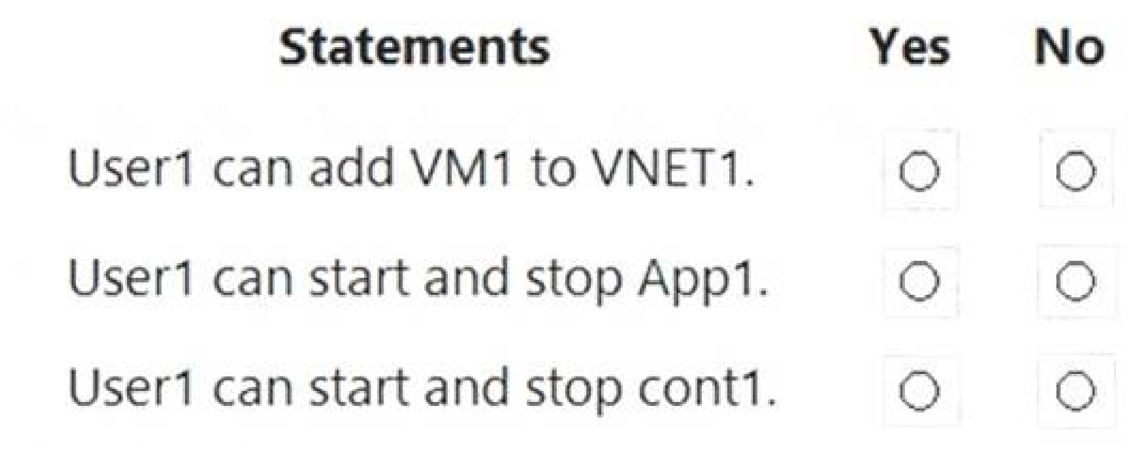
Name	Type	In resource group
cont1	Container instance	RG1
VNET1	Virtual network	RG1
App1	App Service app	RG1
VM1	Virtual machine	RG1
User1	User	**Not applicable**

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



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

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



Statements	Yes	No
User1 can add VM1 to VNET1.	○	○
User1 can start and stop App1.	○	○
User1 can start and stop cont1.	○	○

A. Mastered
B. Not Mastered

Answer: A

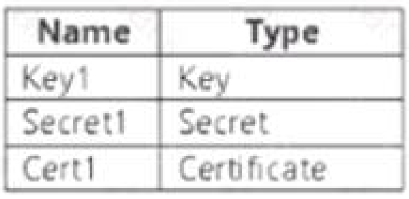
Explanation:
Text Description automatically generated
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompu

NEW QUESTION 52
- (Exam Topic 4)
You have an Azure subscription that contains an Azure key vault.
You need to configure maximum number of days for Which new keys are valid. The solution must minimize administrative effort.
What should you use?

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

Answer: B

NEW QUESTION 54
- (Exam Topic 4)
You have an Azure key vault named Vault1 that stores the resources shown in the following table.



Name	Type
Key1	Key
Secret1	Secret
Cert1	Certificate

Which resources support the creation of a rotation policy?

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

Answer: A

NEW QUESTION 55
- (Exam Topic 4)
You have an Azure subscription that contains an Azure SQL database named sql1. You plan to audit sql1.
You need to configure the audit log destination. The solution must meet the following requirements:

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

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

Answer: C

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

NEW QUESTION 56
- (Exam Topic 4)
You have an Azure subscription.
You create an Azure web app named Contoso1812 that uses an S1 App service plan.
You create a DNS record for www.contoso.com that points to the IP address of Contoso1812.
You need to ensure that users can access Contoso1812 by using the https://www.contoso.com URL. Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Turn on the system-assigned managed identity for Contoso1812.
B. Add a hostname to Contoso1812.
C. Scale out the App Service plan of Contoso1812.
D. Add a deployment slot to Contoso1812.
E. Scale up the App Service plan of Contoso1812.
F. Upload a PFX file to Contoso1812

Answer: BF

Explanation:
B: You can configure Azure DNS to host a custom domain for your web apps. For example, you can create an Azure web app and have your users access it using either www.contoso.com or contoso.com as a fully qualified domain name (FQDN). To do this, you have to create three records:
A root "A" record pointing to contoso.com A root "TXT" record for verification
A "CNAME" record for the www name that points to the A record
F: To use HTTPS, you need to upload a PFX file to the Azure Web App. The PFX file will contain the SSL certificate required for HTTPS.
References: https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom- Domain

NEW QUESTION 59
- (Exam Topic 4)
Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD). Azure AD Connect is installed on a domain member server named Server1.
You need to ensure that a domain administrator for the adatum.com domain can modify the synchronization options. The solution must use the principle of least privilege.
Which Azure AD role should you assign to the domain administrator?

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

Answer: B

Explanation:
Reference:

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

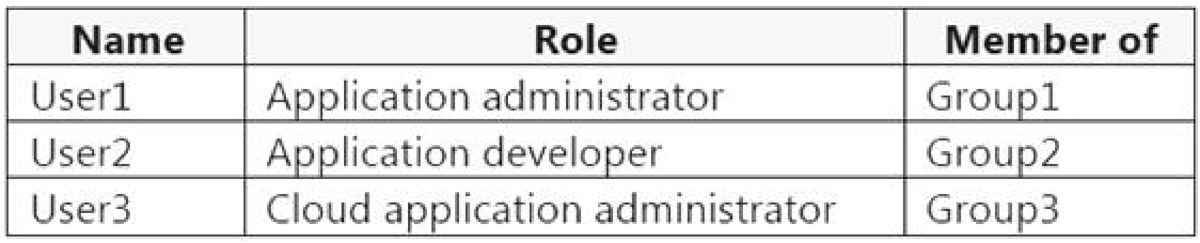
NEW QUESTION 63
- (Exam Topic 4)
You have 15 Azure virtual machines in a resource group named RG1. All virtual machines run identical applications.
You need to prevent unauthorized applications and malware from running on the virtual machines. What should you do?

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

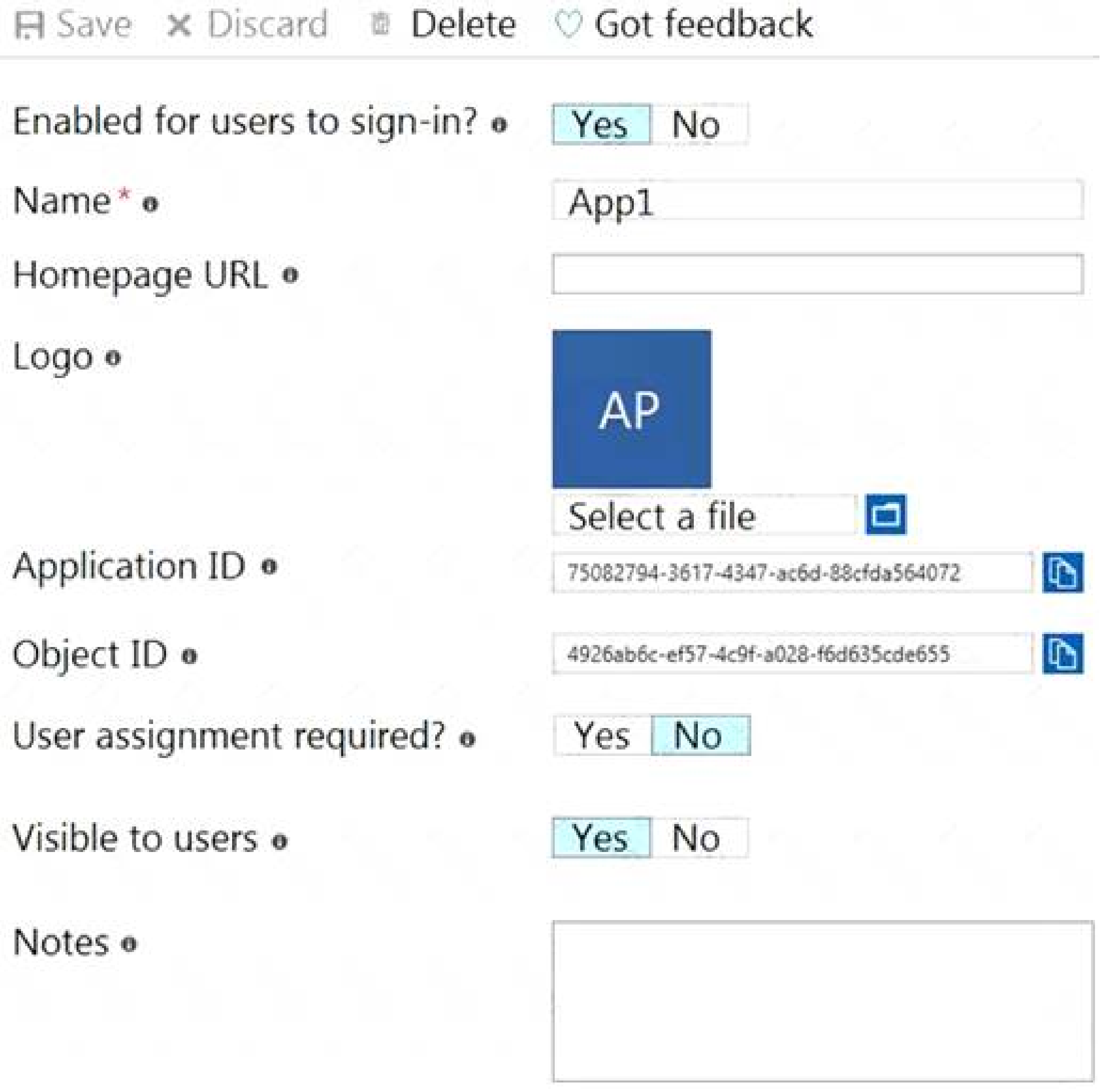
NEW QUESTION 65
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains three security groups named Group1, Group2, and Group3 and the users shown in the following table.



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
Select a file

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

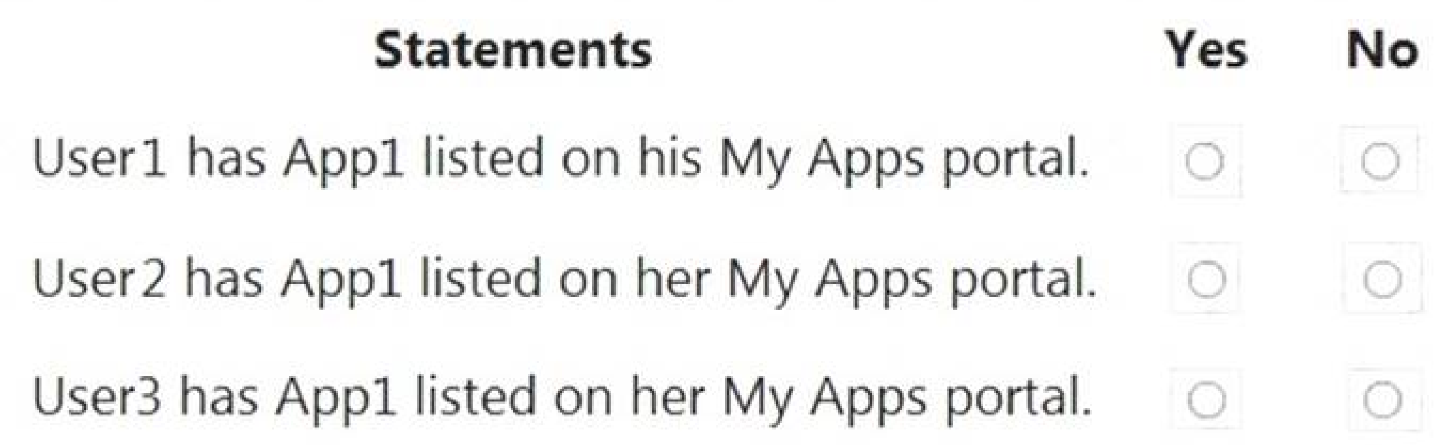
Object ID 4926ab6c-ef57-4c9f-a028-f6d635cde655

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.



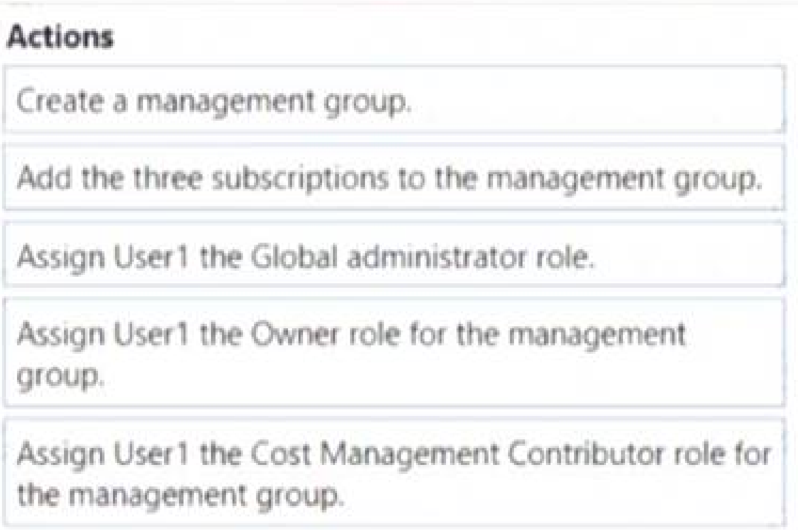
Statements	Yes	No
User1 has App1 listed on his My Apps portal.	○	○
User2 has App1 listed on her My Apps portal.	○	○
User3 has App1 listed on her My Apps portal.	○	○

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 69
- (Exam Topic 4)
You have three Azure subscriptions and a user named User1.
You need to provide User1 with the ability to manage and view costs for the resources across all three subscriptions. The solution must use the principle of least privilege.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.



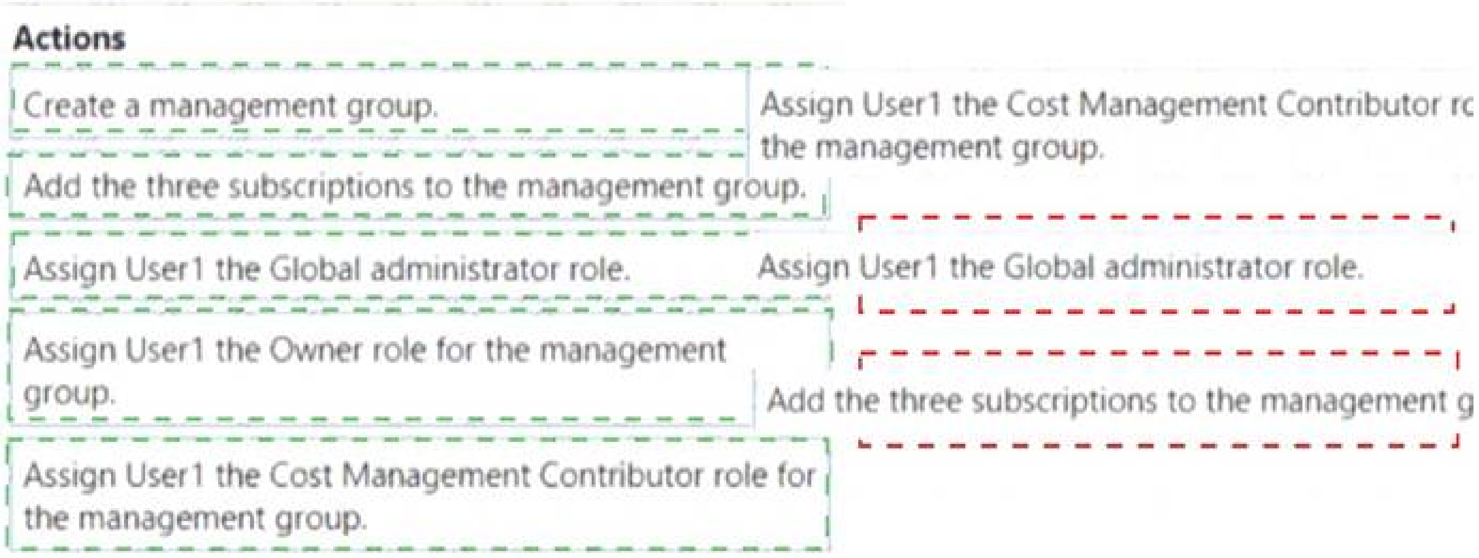
Actions

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Actions

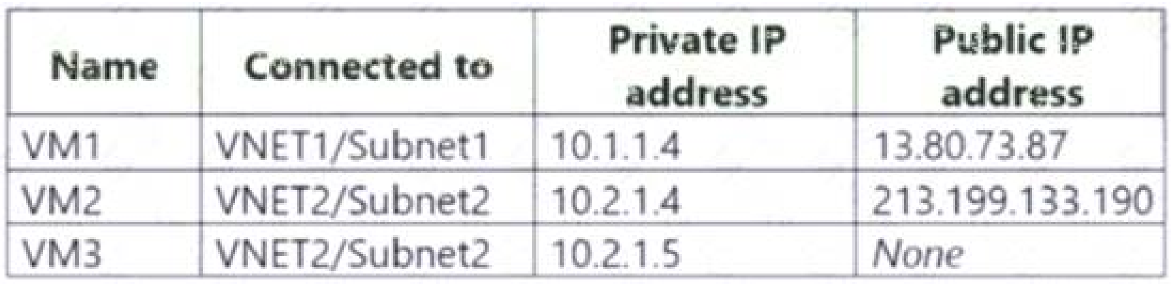
- Create a management group.
- Add the three subscriptions to the management group.
- Assign User1 the Global administrator role.
- Assign User1 the Owner role for the management group.
- Assign User1 the Cost Management Contributor role for the management group.

Assign User1 the Cost Management Contributor rc the management group.

Assign User1 the Global administrator role.

Add the three subscriptions to the management g

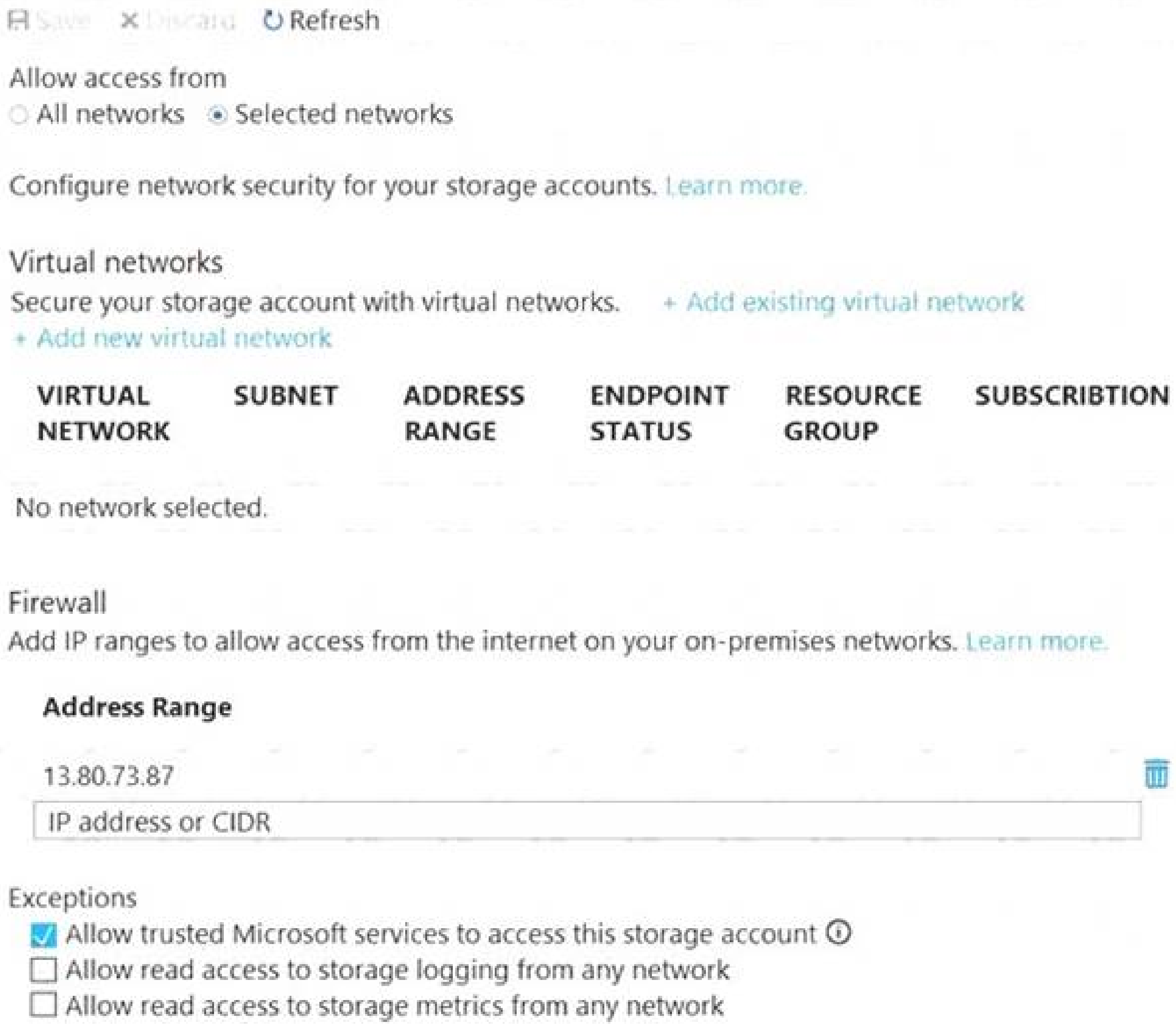
NEW QUESTION 70
- (Exam Topic 4)
You have an Azure subscription that contains the virtual machines shown in the following table.



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

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

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



Save × Discard Refresh

Allow access from
○ All networks ● Selected networks

Configure network security for your storage accounts. Learn more

Virtual networks
Secure your storage account with virtual networks. + Add existing virtual network
+ Add new virtual network

VIRTUAL NETWORK	SUBNET	ADDRESS RANGE	ENDPOINT STATUS	RESOURCE GROUP	SUBSCRIBTION

No network selected.

Firewall
Add IP ranges to allow access from the internet on your on-premises networks. Learn more

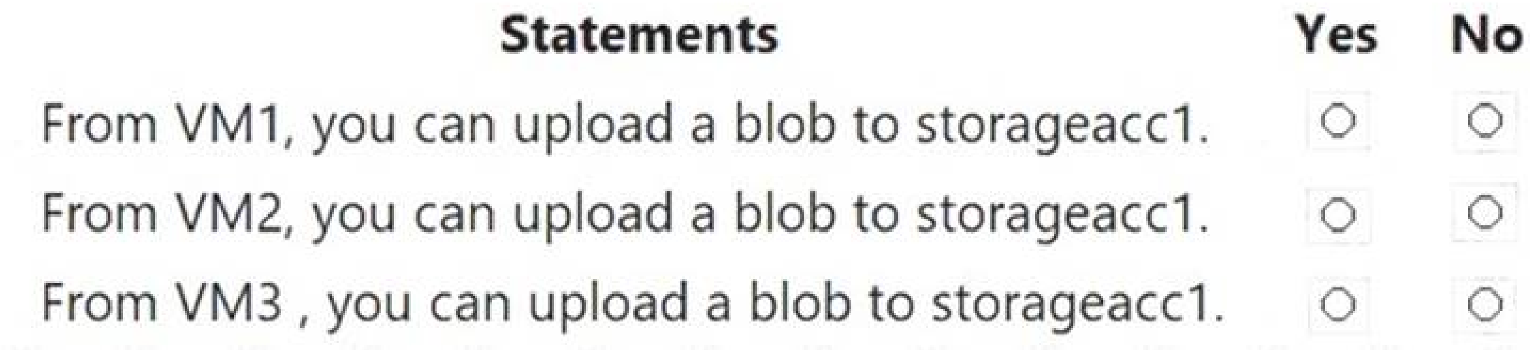
Address Range

13.80.73.87

IP address or CIDR

Exceptions
☑ Allow trusted Microsoft services to access this storage account
□ Allow read access to storage logging from any network
□ Allow read access to storage metrics from any network

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



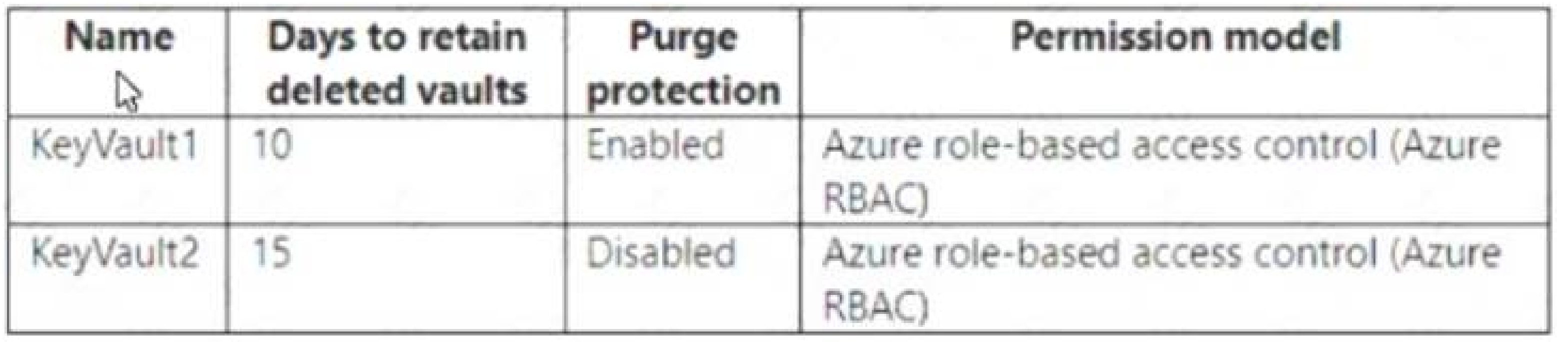
Statements	Yes	No
From VM1, you can upload a blob to storageacc1.	○	○
From VM2, you can upload a blob to storageacc1.	○	○
From VM3 , you can upload a blob to storageacc1.	○	○

A. Mastered
B. Not Mastered

Answer: A

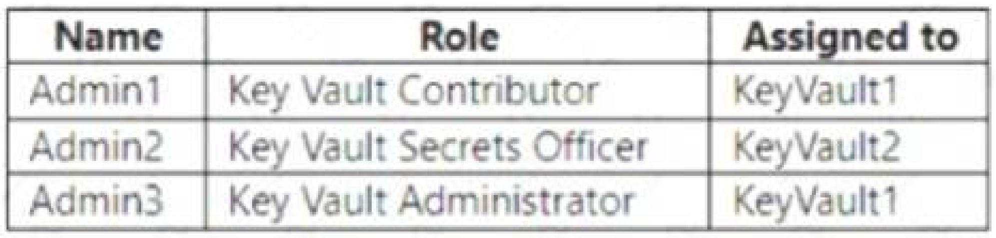
Explanation:
Box 1: Yes
The public IP of VM1 is allowed through the firewall.
Box 2: No
The allowed virtual network list is empty so VM2 cannot access storageacc1 directly. The public IP address of VM2 is not in the allowed IP list so VM2 cannot access storageacc1 over the Internet.
Box 3: No
The allowed virtual network list is empty so VM3 cannot access storageacc1 directly. VM3 does not have a public IP address so it cannot access storageacc1 over the Internet.
Reference:
https://docs.microsoft.com/en-gb/azure/storage/common/storage-network-security

NEW QUESTION 71
- (Exam Topic 4)
You have an Azure subscription that contains the key vaults shown in the following table.



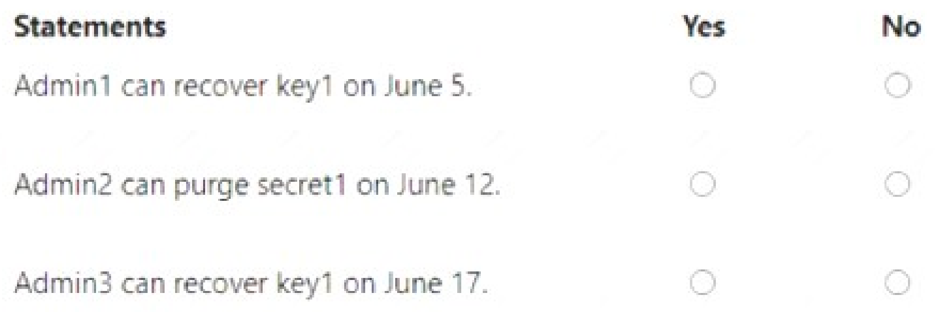
Name	Days to retain deleted vaults	Purge protection	Permission model
KeyVault1	10	Enabled	Azure role-based access control (Azure RBAC)
KeyVault2	15	Disabled	Azure role-based access control (Azure RBAC)

The subscription contains the users shown in the following table.



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

On June 1, you perform the following actions:
• Delete a key named key1 from KeyVault1.
• Delete a secret named secret 1 from KeyVault2.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.



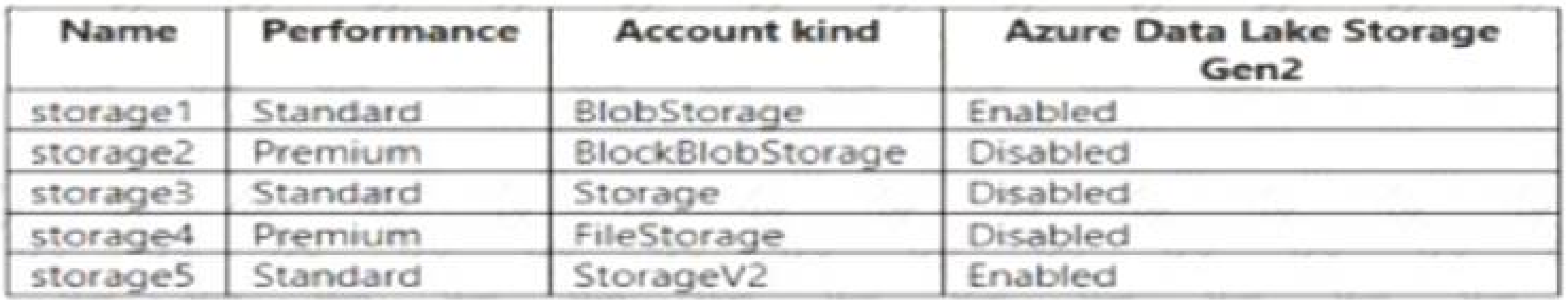
Statements	Yes	No
Admin1 can recover key1 on June 5.	○	○
Admin2 can purge secret1 on June 12.	○	○
Admin3 can recover key1 on June 17.	○	○

A. Mastered
B. Not Mastered

Answer: A

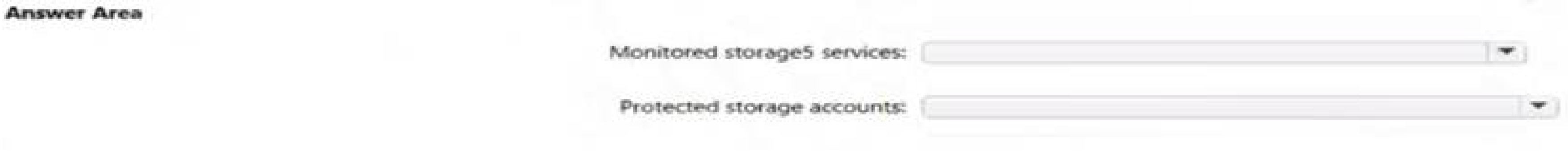
Explanation:
Yes
Yes No

NEW QUESTION 72
- (Exam Topic 4)
You have an Azure subscription that contains the storage accounts shown in the following, table.



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

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



Answer Area

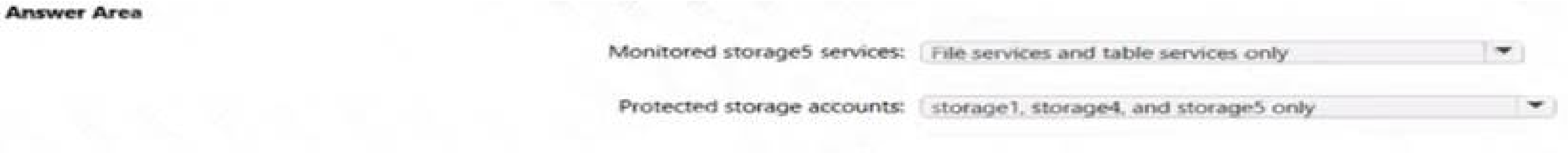
Monitored storage5 services:

Protected storage accounts:

A. Mastered
B. Not Mastered

Answer: A

Explanation:



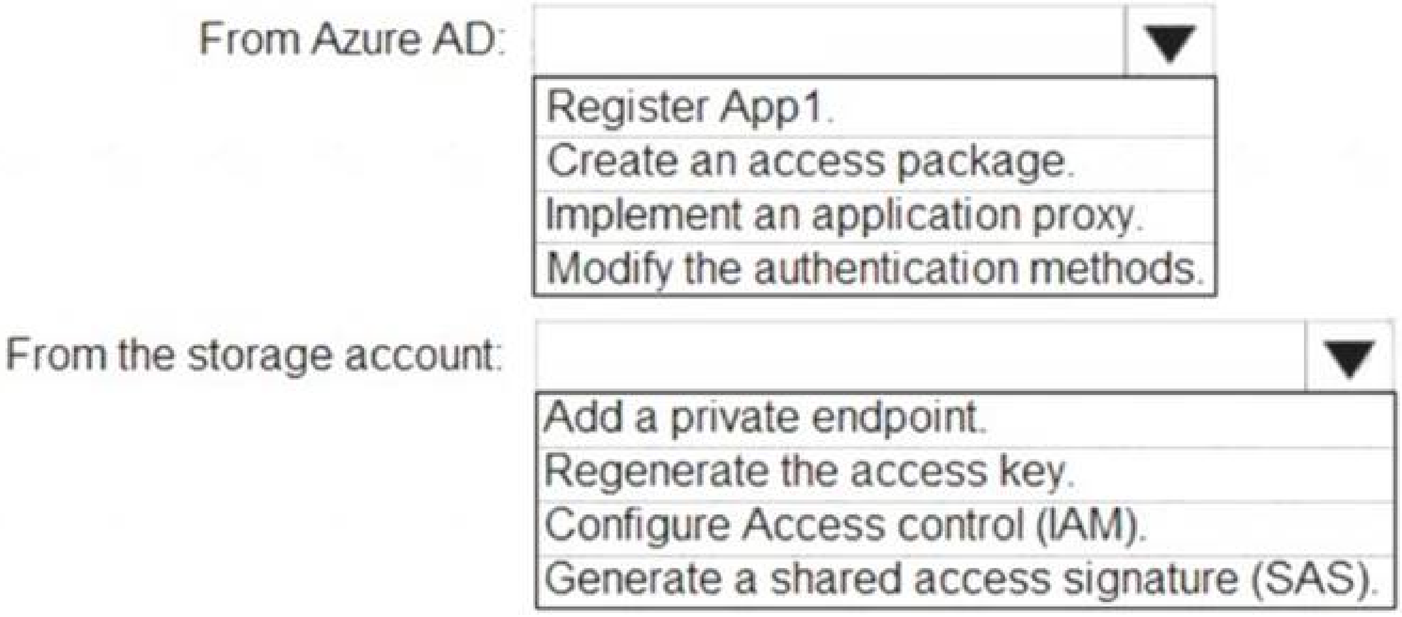
Answer Area

Monitored storage5 services: File services and table services only

Protected storage accounts: storage1, storage4, and storage5 only

NEW QUESTION 75
- (Exam Topic 4)

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



From Azure AD:
- Register App1.
- Create an access package.
- Implement an application proxy.
- Modify the authentication methods.

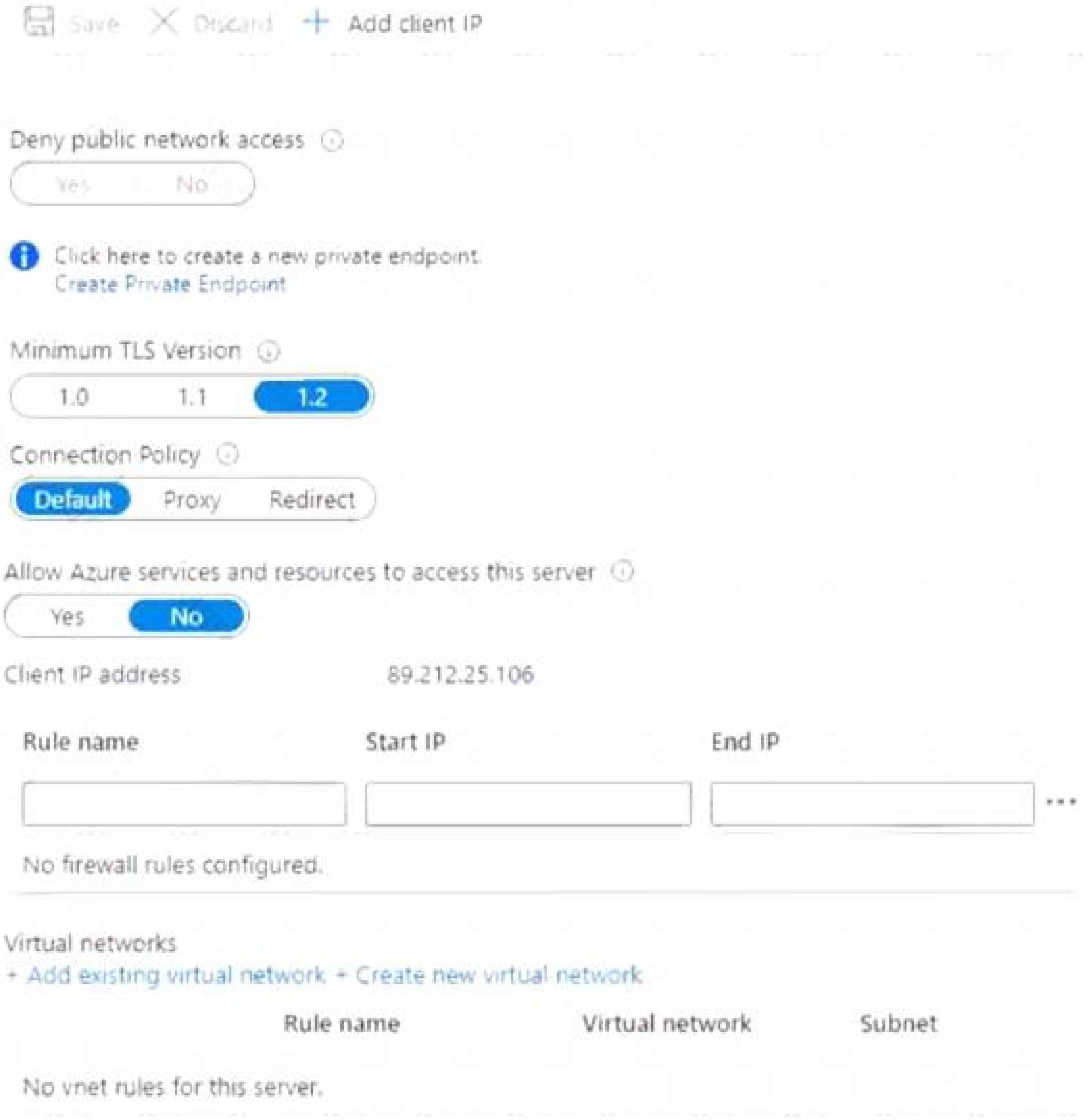
From the storage account:
- Add a private endpoint.
- Regenerate the access key.
- Configure Access control (IAM).
- Generate a shared access signature (SAS).

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 79
- (Exam Topic 4)
You have an Azure subscription that contains an Azure SQL Database logic server named SQL! and an Azure virtual machine named VM1. VM1 uses a private IP address only.
The Firewall and virtual networks settings for SQL1 are shown in the following exhibit.



Deny public network access: Yes No

Click here to create a new private endpoint.
Create Private Endpoint

Minimum TLS Version: 1.0 1.1 [✓ 1.2]

Connection Policy: [✓ Default] Proxy Redirect

Allow Azure services and resources to access this server: Yes [✓ No]

Client IP address 89.212.25.106

Rule name	Start IP	End IP

No firewall rules configured.

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

Rule name	Virtual network	Subnet

No vnet rules for this server.

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

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

Answer: C

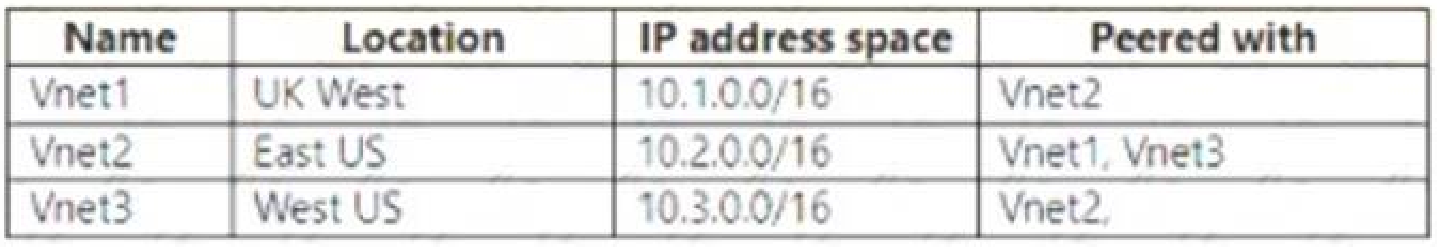
NEW QUESTION 80

- (Exam Topic 4)

You have an Azure subscription that contains the following Azure firewall:

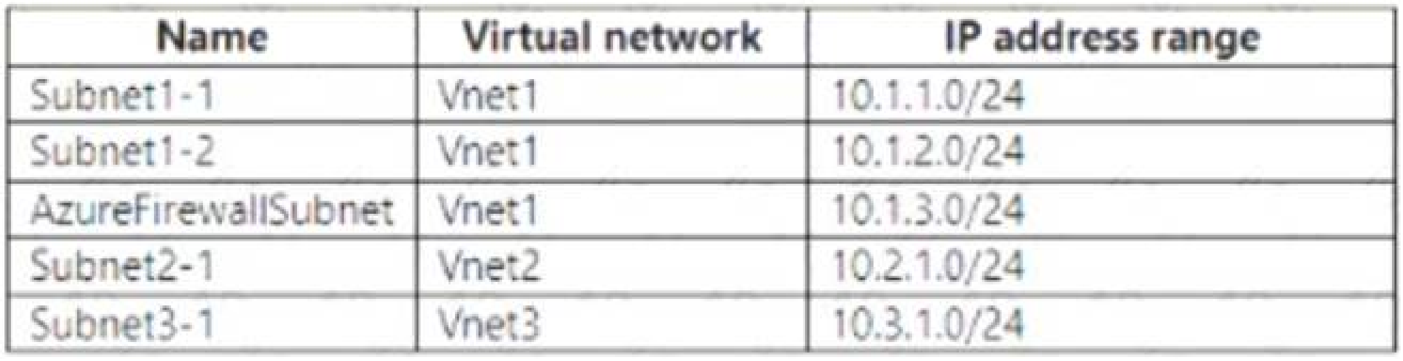
- Name: Fw1
- Azure region: UK West
- Private IP address: 10.1.3.4
- Public IP address: 23.236.62.147

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



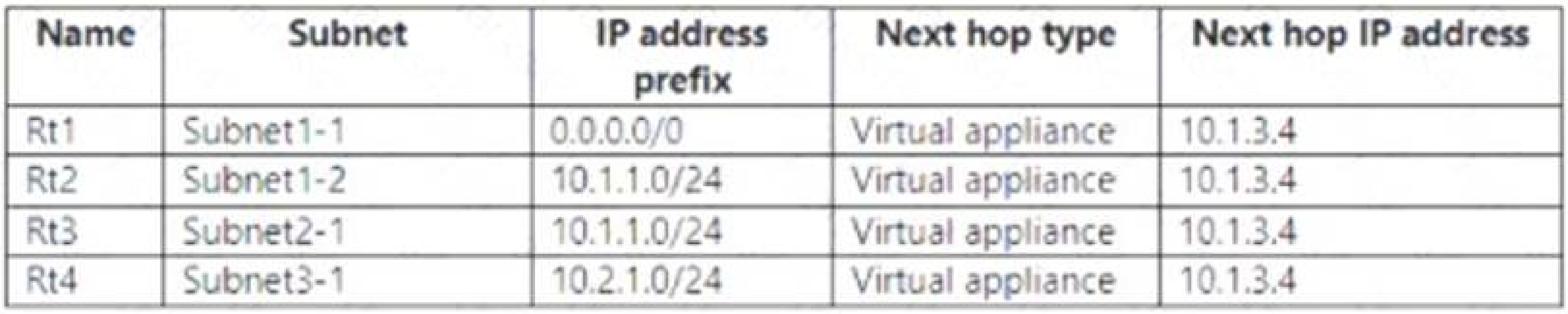
Name	Location	IP address space	Peered with
Vnet1	UK West	10.1.0.0/16	Vnet2
Vnet2	East US	10.2.0.0/16	Vnet1, Vnet3
Vnet3	West US	10.3.0.0/16	Vnet2,

The subscription contains the subnets shown in the following table.



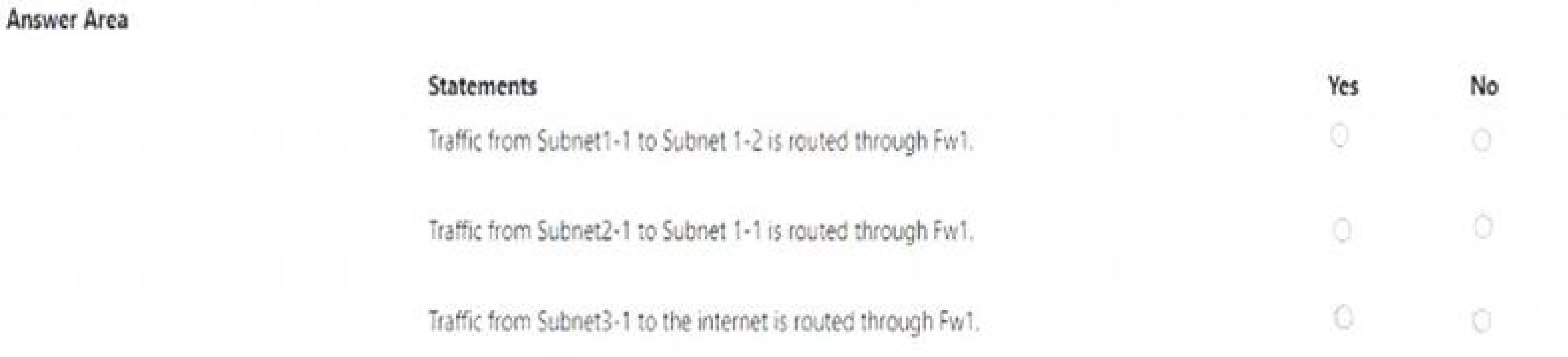
Name	Virtual network	IP address range
Subnet1-1	Vnet1	10.1.1.0/24
Subnet1-2	Vnet1	10.1.2.0/24
AzureFirewallSubnet	Vnet1	10.1.3.0/24
Subnet2-1	Vnet2	10.2.1.0/24
Subnet3-1	Vnet3	10.3.1.0/24

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.



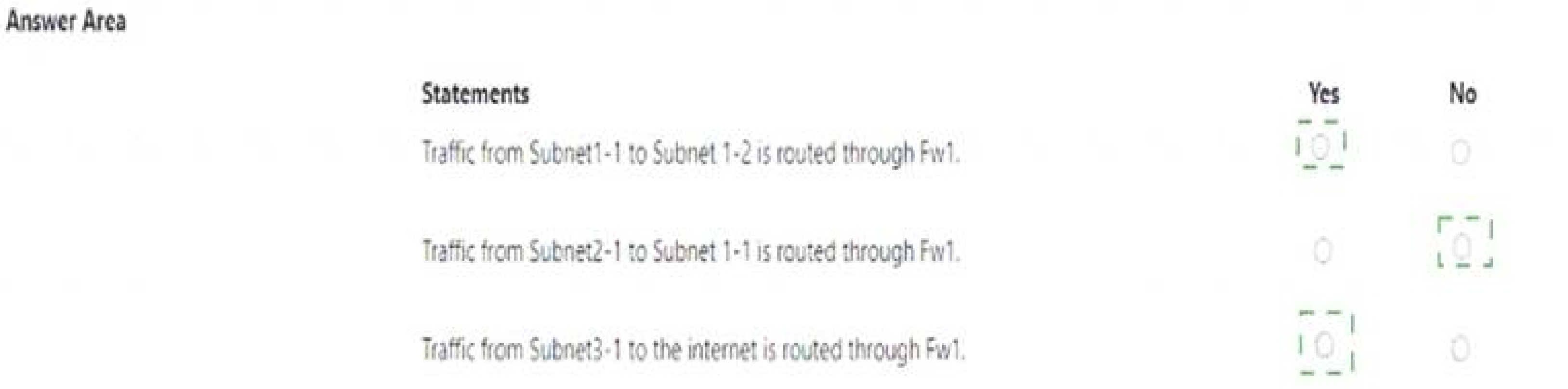
Answer Area

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 85

- (Exam Topic 4)

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

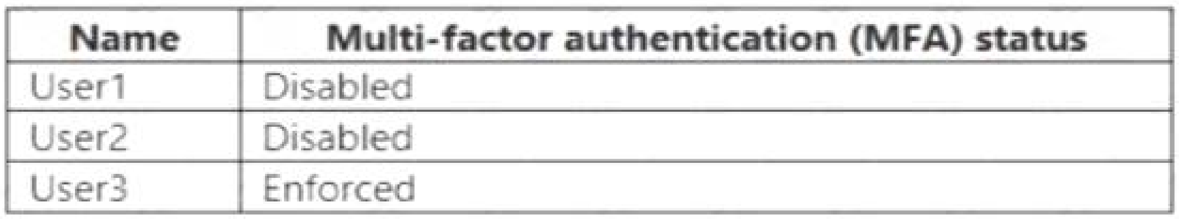
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Security Center for the centralized policy management of three Azure subscriptions. You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create an initiative and an assignment that is scoped to a management group. Does this meet the goal?

A. Yes
B. No

Answer: A

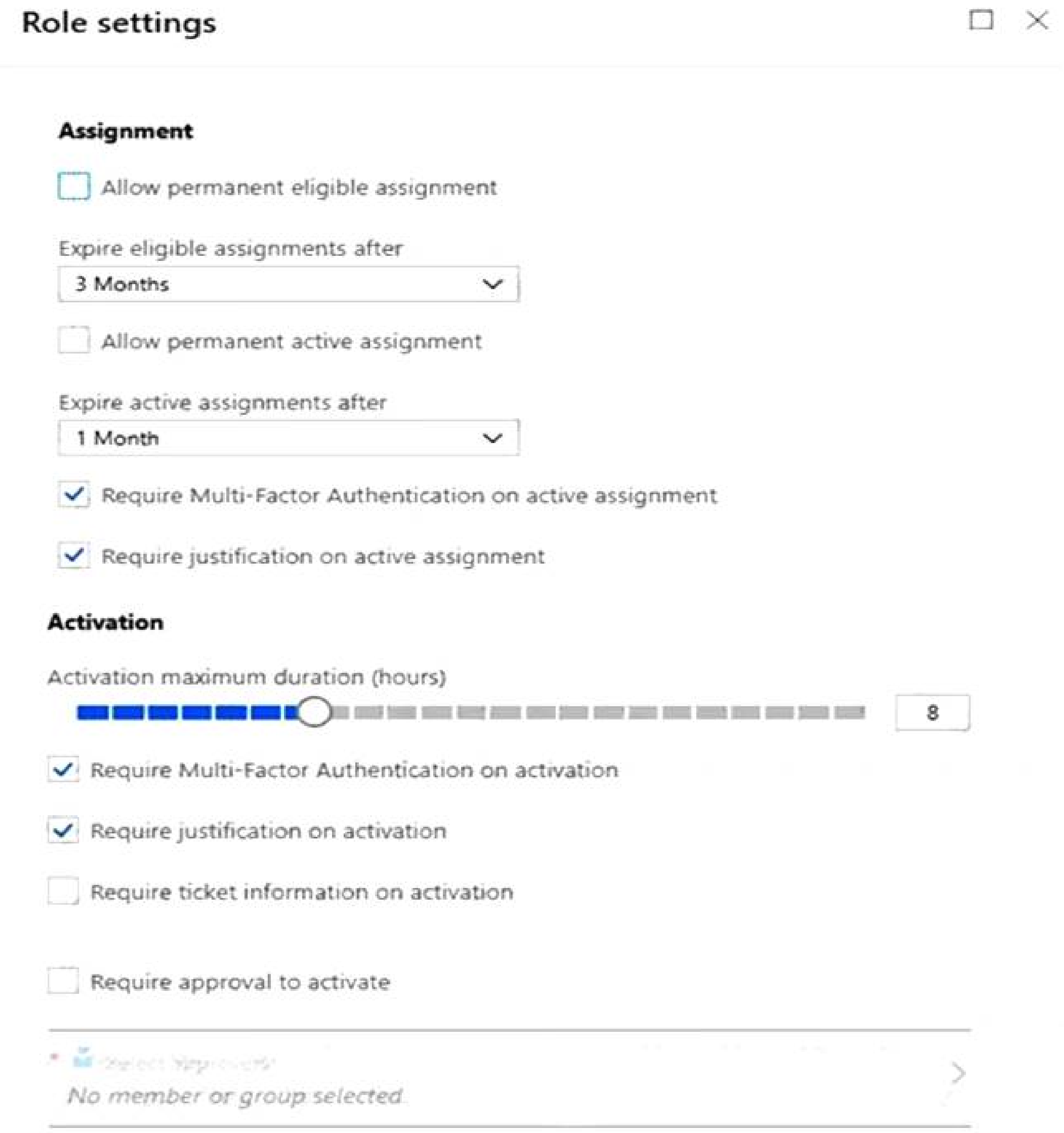
Explanation:
References:
https://docs.microsoft.com/en-us/azure/governance/policy/overview

NEW QUESTION 86
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.



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

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



Role settings

Assignment

□ Allow permanent eligible assignment

Expire eligible assignments after
3 Months

□ Allow permanent active assignment

Expire active assignments after
1 Month

☑ Require Multi-Factor Authentication on active assignment

☑ Require justification on active assignment

Activation

Activation maximum duration (hours)
8

☑ Require Multi-Factor Authentication on activation

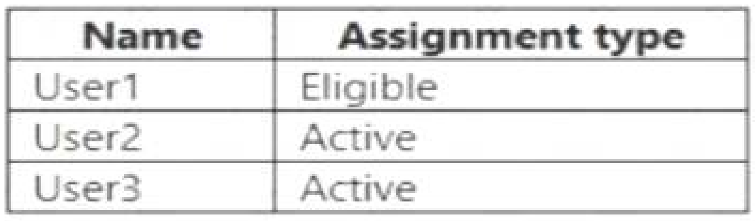
☑ Require justification on activation

□ Require ticket information on activation

□ Require approval to activate

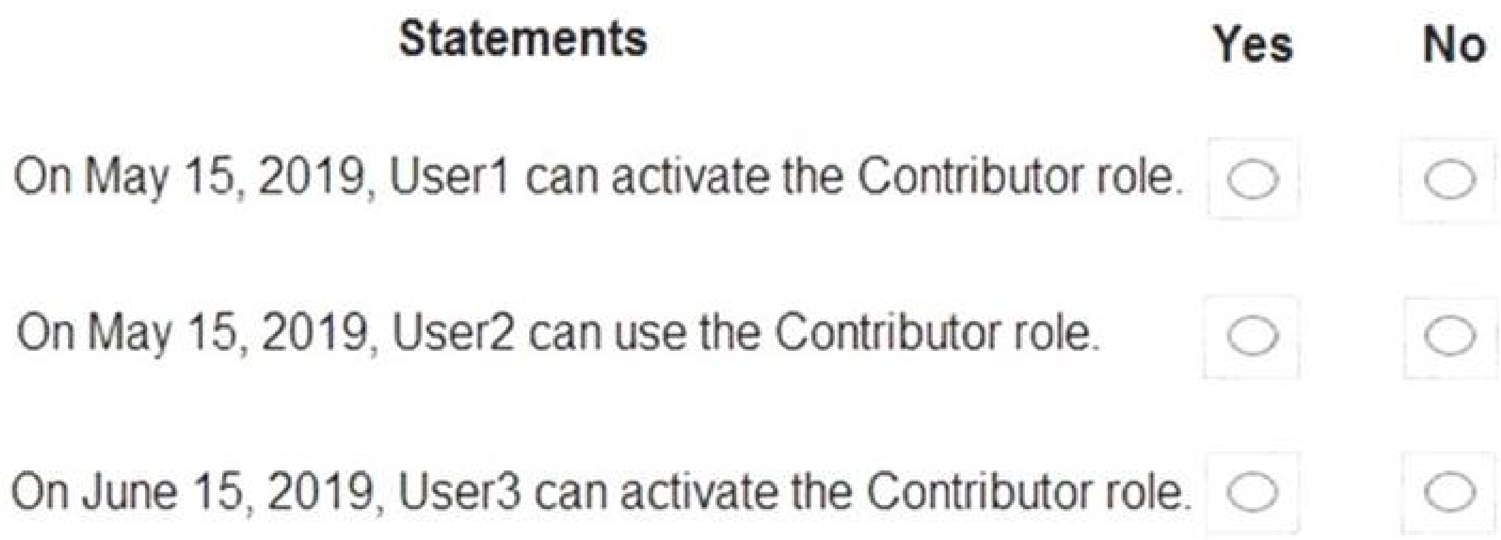
* Select Approver(s)
No member or group selected

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



Name	Assignment type
User1	Eligible
User2	Active
User3	Active

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



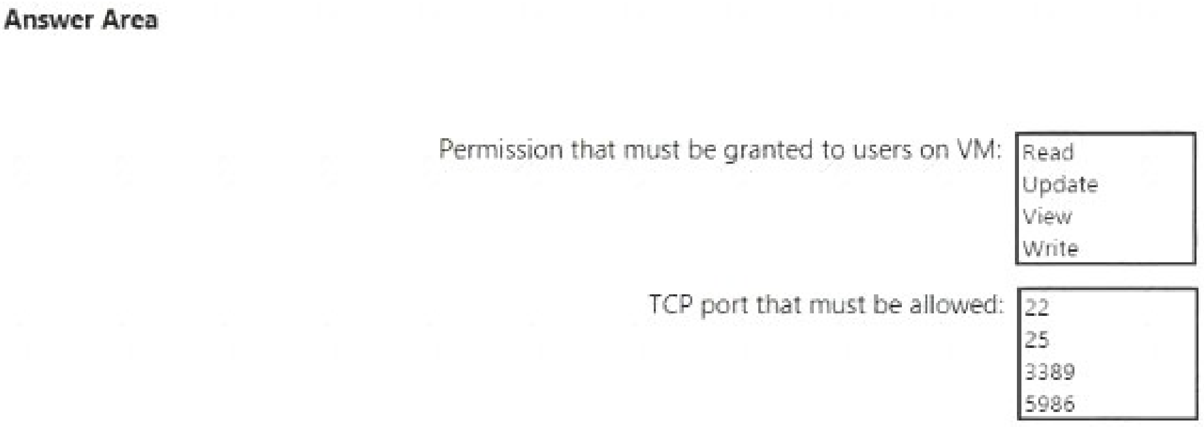
Statements	Yes	No
On May 15, 2019, User1 can activate the Contributor role.	○	○
On May 15, 2019, User2 can use the Contributor role.	○	○
On June 15, 2019, User3 can activate the Contributor role.	○	○

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 88
- (Exam Topic 4)
You are configuring just in time (JIT) VM access to a set of Azure virtual machines.
You need to grant users PowerShell access to the virtual machine by using JIT VM access. What should you configure? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

Permission that must be granted to users on VM:
Read
Update
View
Write

TCP port that must be allowed:
22
25
3389
5986

A. Mastered
B. Not Mastered

Answer: A

Explanation:
* 1. Read permission
* 2. 5986
https://docs.microsoft.com/en-us/azure/security-center/just-in-time-explained#what-permissions-are-needed-to-c

NEW QUESTION 90
- (Exam Topic 4)
You have an Azure subscription.
You plan to create a workflow automation in Azure Security Center that will automatically remediate a security vulnerability.
What should you create first?

A. a managed identity
B. an automation account
C. an Azure function app
D. an alert rule
E. an Azure logic app

Answer: E

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

NEW QUESTION 93
- (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

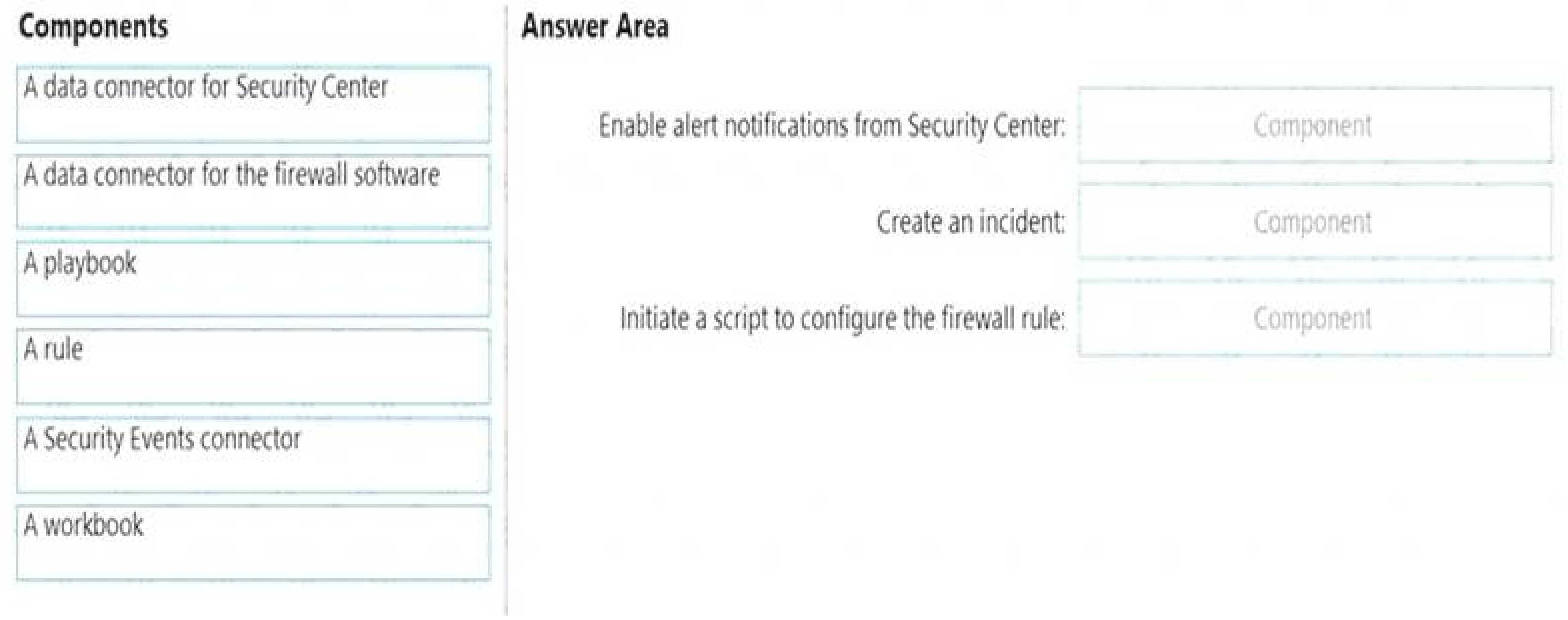
Answer: A

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 97
- (Exam Topic 4)
You have an Azure subscription that contains the following resources:

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

You need to ensure that when a high-priority alert is generated in Security Center for a virtual machine, an incident is created in Azure Sentinel and then a script is initiated to configure a firewall rule for the NVA.
How should you configure Azure Sentinel to meet the requirements? To answer, drag the appropriate components to the correct requirements. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Components

A data connector for Security Center
A data connector for the firewall software
A playbook
A rule
A Security Events connector
A workbook

Answer Area

Enable alert notifications from Security Center: Component
Create an incident: Component
Initiate a script to configure the firewall rule: Component

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 98
- (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 7
You need to collect all the audit failure data from the security log of a virtual machine named VM1 to an Azure Storage account. To complete this task, sign in to the Azure portal.

A. Mastered
B. Not Mastered

Answer: A

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

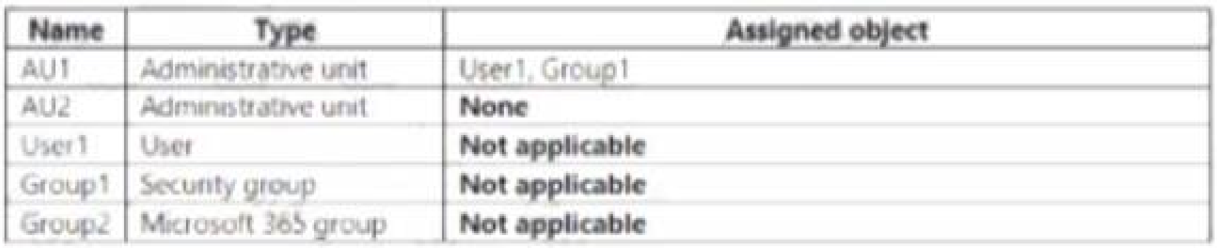
- In the Azure portal, search for and select the virtual machine named VM1.
- In the left pane, select Diagnostic settings.
- Select Add diagnostic setting.
- In the Add diagnostic setting pane, enter the following information:
- Name: Enter a name for the diagnostic setting.
- Destination: Select Storage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

NEW QUESTION 99
- (Exam Topic 4)
You have an Azure subscription that contains a Microsoft Defender External Attack Surface Management (Defender EASM) resource named EASM1. You review the Attack Surface Summary dashboard. You need to identify the following insights:
• Deprecated technologies that are no longer supported
• Infrastructure that will soon expire
Which section of the dashboard should you review?

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

Answer: C

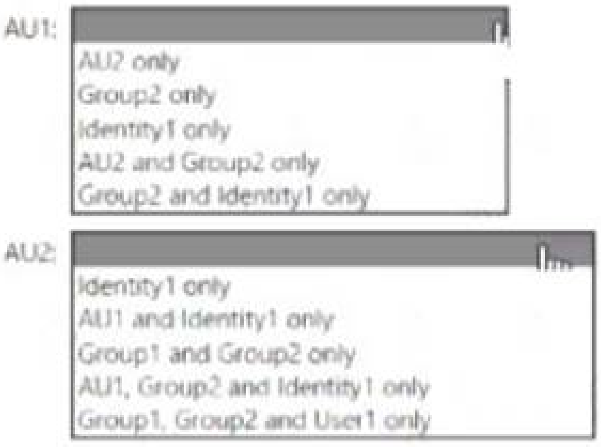
NEW QUESTION 100
- (Exam Topic 4)
You have an Azure subscription that has a managed identity named identity and is linked to an Azure Active Directory (Azure AD) tenant. The tenant contains the resources shown in the following table.
Which resources can be added to AUI and AU2? To answer, select the appropriate options in the answer area.



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

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

Answer Area



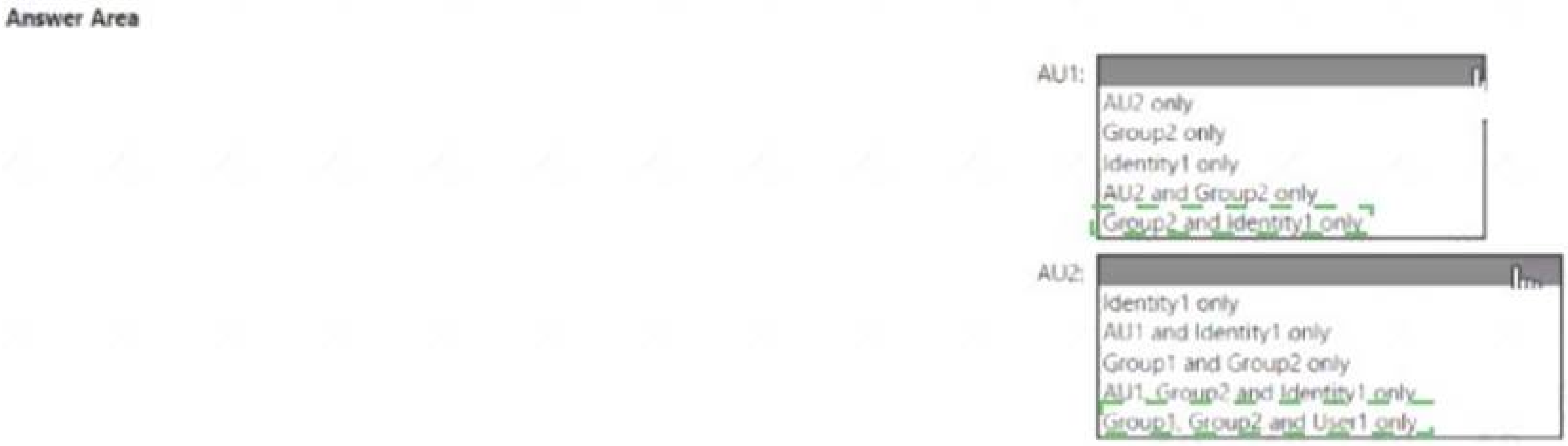
AU1:
- AU2 only
- Group2 only
- Identity1 only
- AU2 and Group2 only
- Group2 and Identity1 only

AU2:
- Identity1 only
- AU1 and Identity1 only
- Group1 and Group2 only
- AU1, Group2 and Identity1 only
- Group1, Group2 and User1 only

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

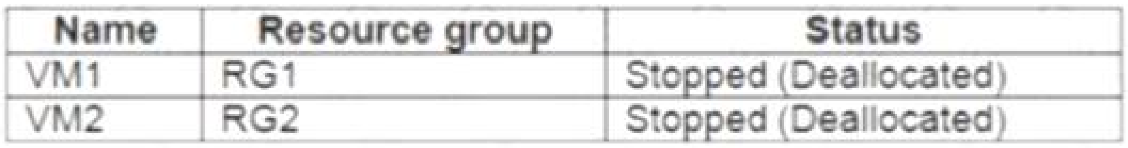
AU1:
- AU2 only
- Group2 only
- Identity1 only
- AU2 and Group2 only
- Group2 and Identity1 only

AU2:
- Identity1 only
- AU1 and Identity1 only
- Group1 and Group2 only
- AU1, Group2 and Identity1 only
- Group1, Group2 and User1 only

NEW QUESTION 103

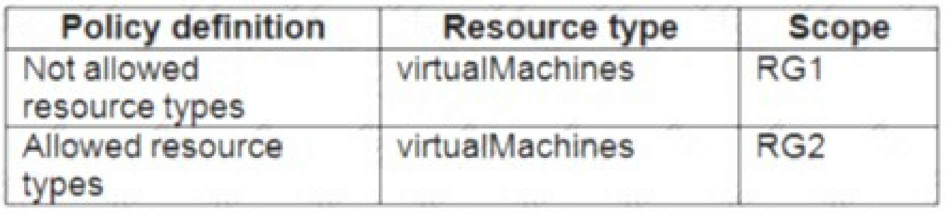
- (Exam Topic 4)

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



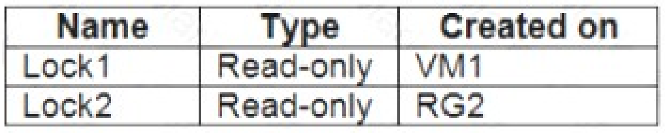
Name	Resource group	Status
VM1	RG1	Stopped (Deallocated)
VM2	RG2	Stopped (Deallocated)

You create the Azure policies shown in the following table.



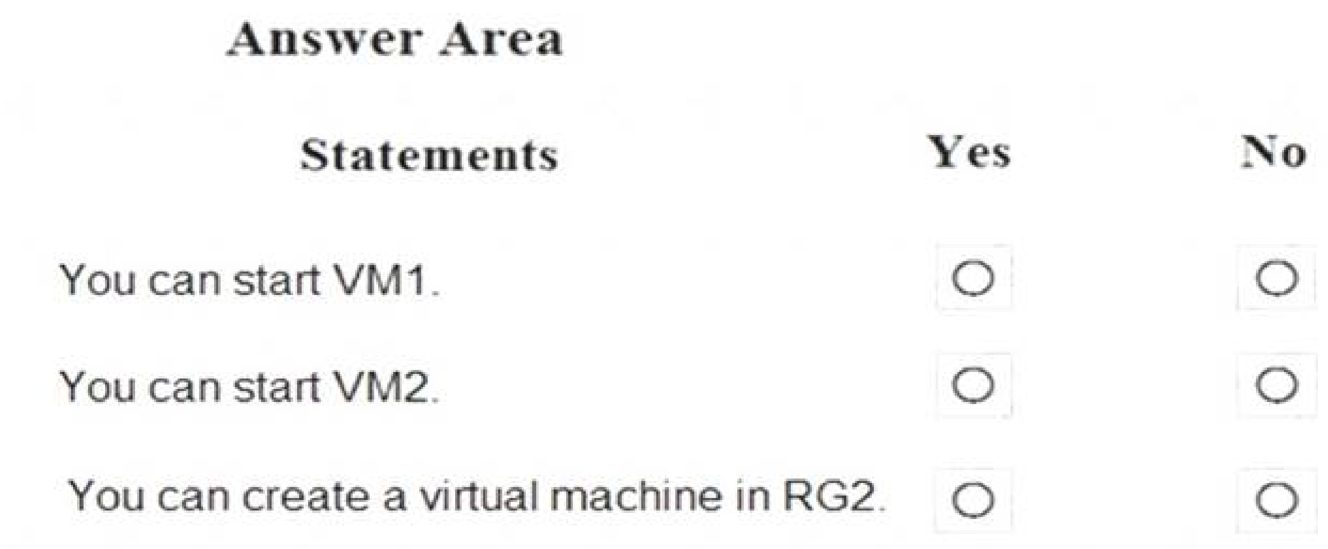
Policy definition	Resource type	Scope
Not allowed resource types	virtualMachines	RG1
Allowed resource types	virtualMachines	RG2

You create the resource locks shown in the following table.



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

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



Answer Area

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

A. Mastered
B. Not Mastered

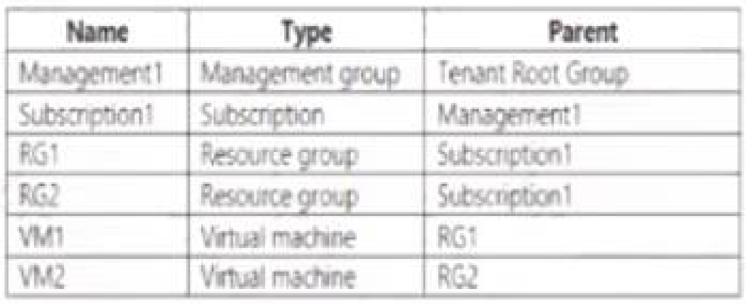
Answer: A

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

NEW QUESTION 106

- (Exam Topic 4)

You have the Azure resource shown in the following table.



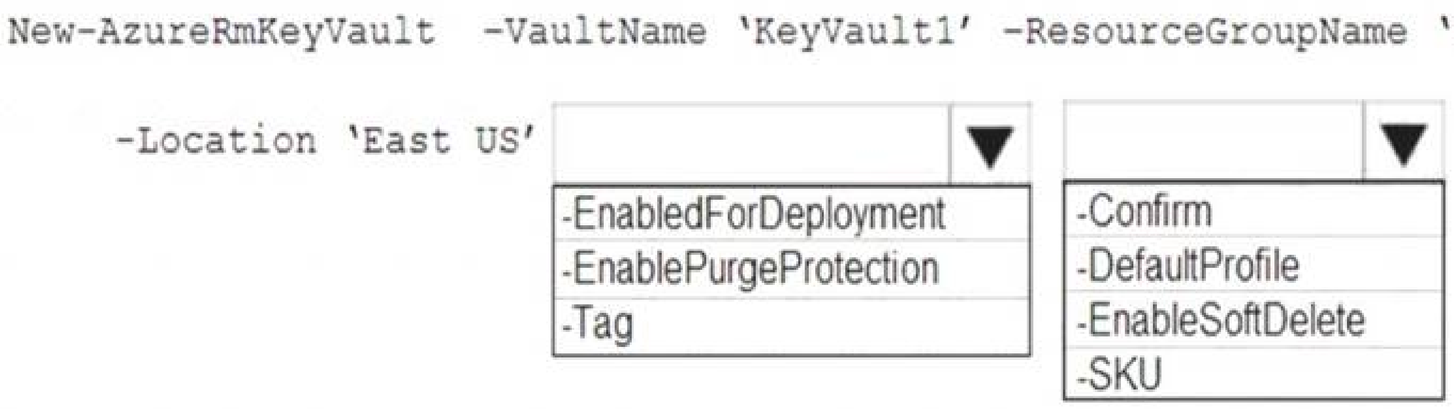
Name	Type	Parent
Management1	Management group	Tenant Root Group
Subscription1	Subscription	Management1
RG1	Resource group	Subscription1
RG2	Resource group	Subscription1
VM1	Virtual machine	RG1
VM2	Virtual machine	RG2

You need to meet the following requirements:
* Internet-facing virtual machines must be protected by using network security groups (NSGs).
* All the virtual machines must have disk encryption enabled.
What is the minimum number of security that you should create in Azure Security Center?

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

Answer: D

NEW QUESTION 108
- (Exam Topic 4)
You need to create an Azure key vault. The solution must ensure that any object deleted from the key vault be retained for 90 days.
How should you complete the command? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



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

     -Location 'East US'
```

- -EnabledForDeployment
- -EnablePurgeProtection
- -Tag

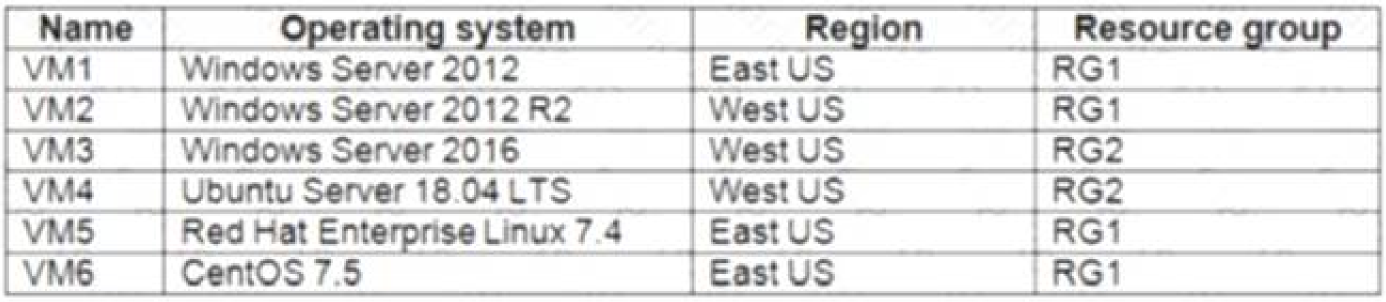
- -Confirm
- -DefaultProfile
- -EnableSoftDelete
- -SKU

A. Mastered
B. Not Mastered

Answer: A

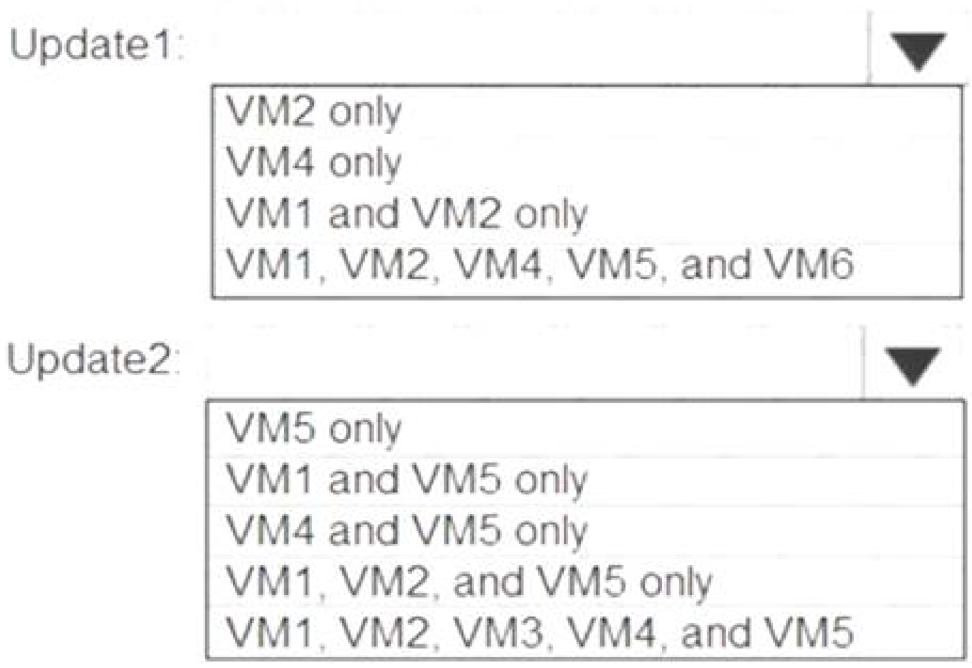
Explanation:
Box 1: -EnablePurgeProtection
If specified, protection against immediate deletion is enabled for this vault; requires soft delete to be enabled as well.
Box 2: -EnableSoftDelete
Specifies that the soft-delete functionality is enabled for this key vault. When soft-delete is enabled, for a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

NEW QUESTION 110
- (Exam Topic 4)
You have Azure virtual machines that have Update Management enabled. The virtual machines are configured as shown in the following table.



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

You schedule two update deployments named Update1 and Update2. Update1 updates VM3. Update2 updates VM6.
Which additional virtual machines can be updated by using Update1 and Update2? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Update1:
- VM2 only
- VM4 only
- VM1 and VM2 only
- VM1, VM2, VM4, VM5, and VM6

Update2:
- VM5 only
- VM1 and VM5 only
- VM4 and VM5 only
- VM1, VM2, and VM5 only
- VM1, VM2, VM3, VM4, and VM5

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Update1: VM1 and VM2 only
VM3: Windows Server 2016 West US RG2 Update2: VM4 and VM5 only
VM6: CentOS 7.5 East US RG1
For Linux, the machine must have access to an update repository. The update repository can be private or public.
References:
https://docs.microsoft.com/en-us/azure/automation/automation-update-management

NEW QUESTION 114
- (Exam Topic 4)
You have an Azure subscription that uses Microsoft Defender for Cloud. You have accounts for the following cloud services:
• Alibaba Cloud
• Amazon Web Services (AWS)
• Google Cloud Platform (GCP)
What can you add to Defender for Cloud?

A. AWS only
B. Alibaba Cloud and AWS only
C. Alibaba Good and GCP only
D. AWS and GCP only
E. Alibaba Cloud, AW
F. and GCP

Answer: A

NEW QUESTION 115
- (Exam Topic 4)
Your on-premises network contains a Hyper-V virtual machine named VM1. You need to use Azure Arc to onboard VM1 to Microsoft Defender for Cloud. What should you install first?

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

Answer: B

NEW QUESTION 117
- (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 119
- (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 123
- (Exam Topic 4)
You have an Azure subscription that contains 100 virtual machines and has Azure Security Cent,-. Standard tier enabled.
You plan to perform a vulnerability scan of each virtual machine.
You need to deploy the vulnerability scanner extension to the virtual machines by using an Azure Resource Manager template.
Which two values should you specify in the code to automate the deployment of the extension to the virtual machines? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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

Answer: AC

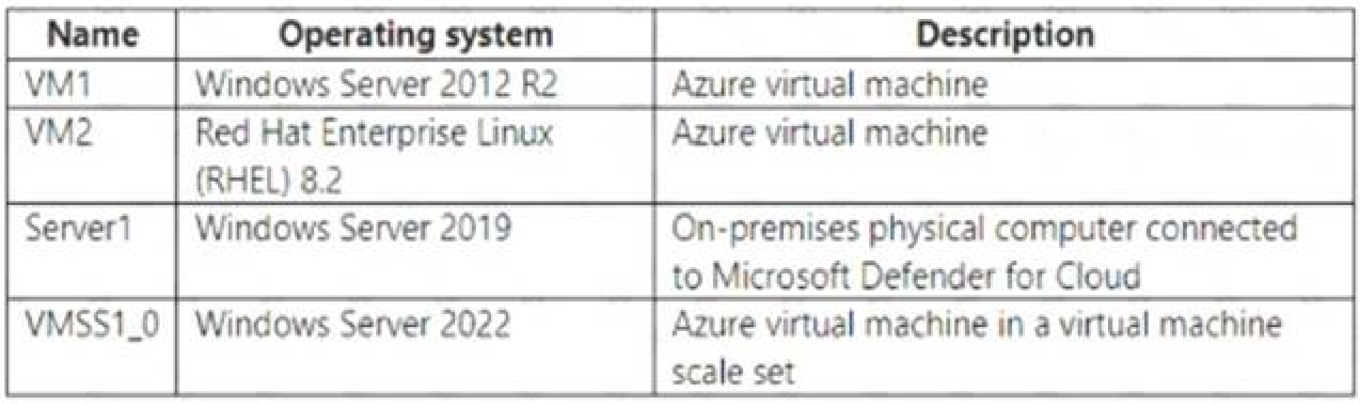
Explanation:
https://docs.microsoft.com/en-us/azure/azure-arc/servers/onboard-service-principal

NEW QUESTION 128
- (Exam Topic 4)
You have an Azure subscription.
You plan to map an online infrastructure and perform vulnerability scanning for the following:
• ASNs
• Hostnames
• IP addresses
• SSL certificates What should you use?

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

Answer: A

NEW QUESTION 129
- (Exam Topic 4)
You have an Azure subscription and the computers shown in the following table.



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

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

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

Answer: A

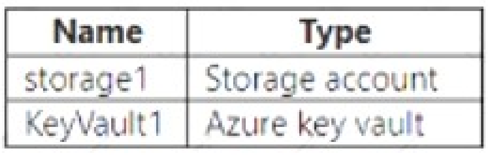
NEW QUESTION 130
- (Exam Topic 4)
You have an Azure web app named webapp1.
You need to configure continuous deployment for webapp1 by using an Azure Repo. What should you create first?

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 131
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.



Name	Type
storage1	Storage account
KeyVault1	Azure key vault

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

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

Answer: D

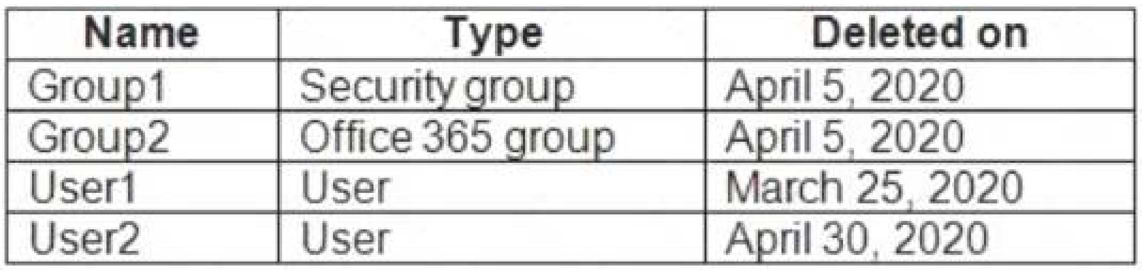
NEW QUESTION 135
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com. The User administrator role is assigned to a user named Admin1.
An external partner has a Microsoft account that uses the user1@outlook.com sign in.
Admin1 attempts to invite the external 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 139
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant. You have the deleted objects shown in the following table.



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

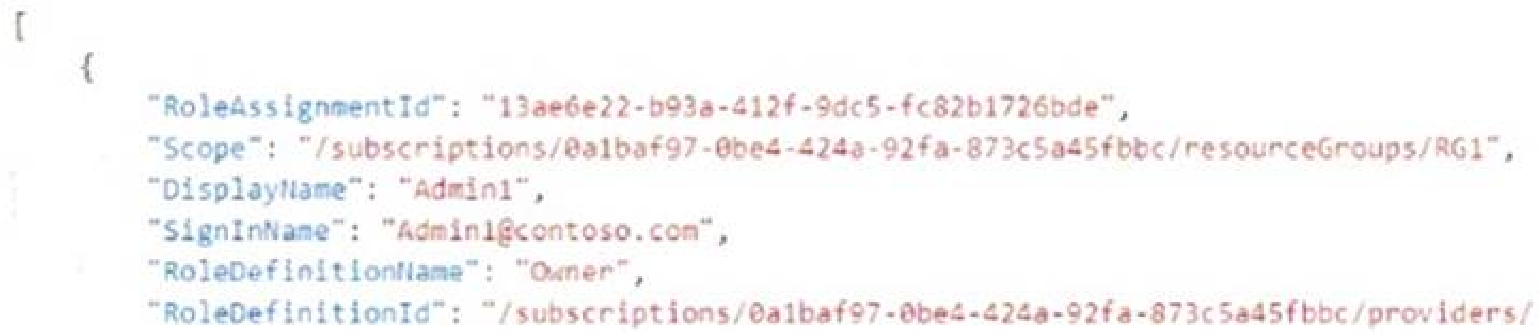
On May 4, 2020, you attempt to restore the deleted objects by using the Azure Active Directory admin center. Which two objects can you restore? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

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

Answer: BC

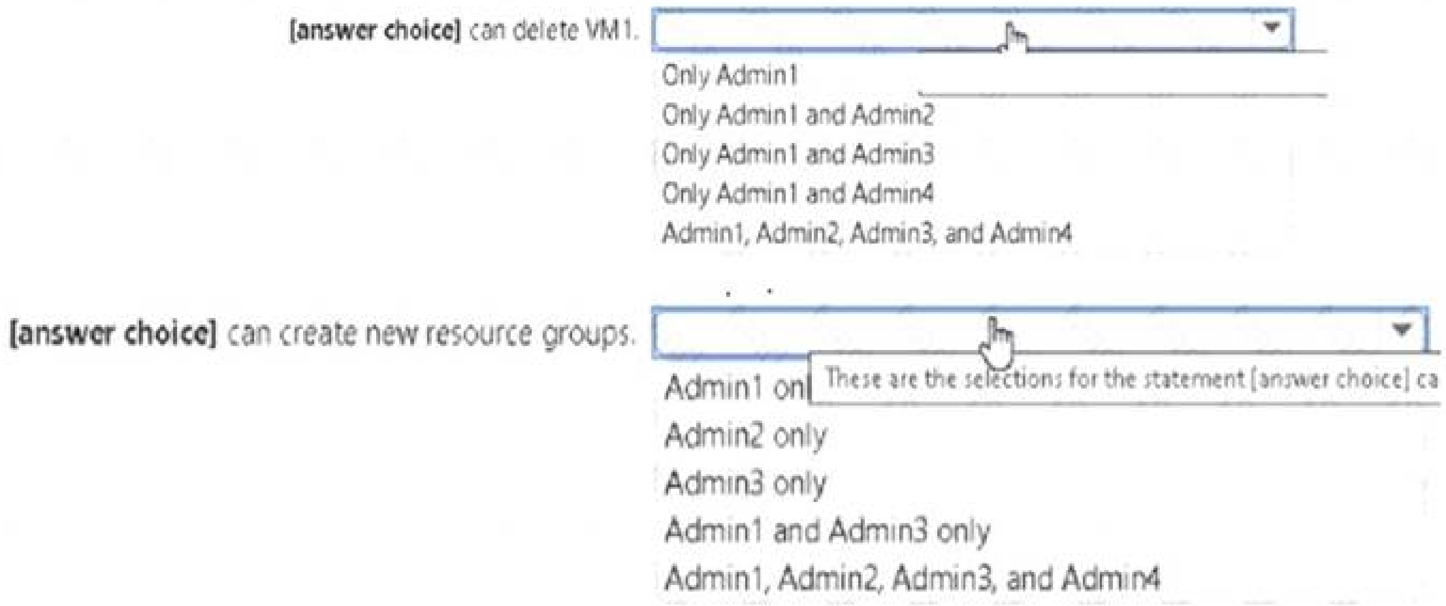
Explanation:
Deleted users and deleted Office 365 groups are available for restore for 30 days. You cannot restore a deleted security group.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-restore-deleted

NEW QUESTION 144
- (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.

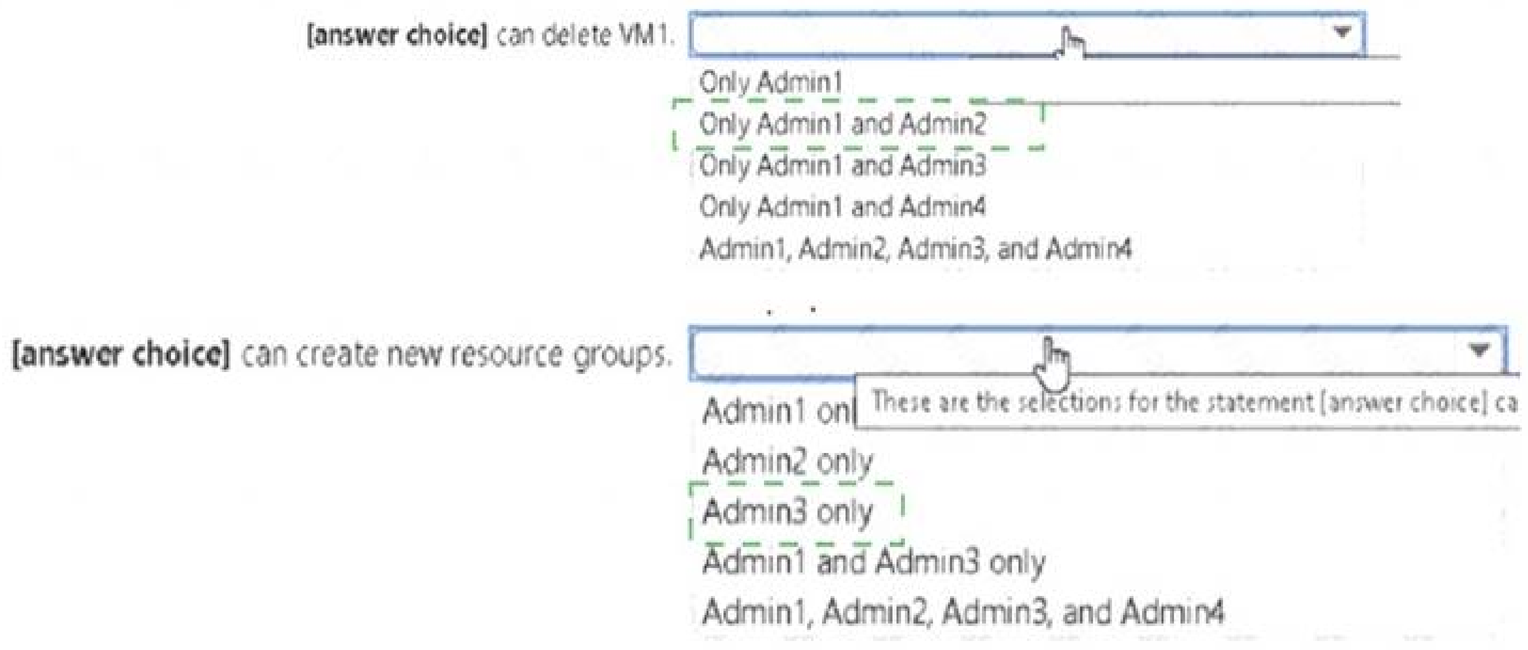
- Admin1 onl
- Admin2 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, Admin3, and Admin4

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



[answer choice] can delete VM1.

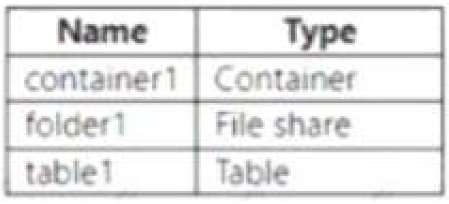
- Only Admin1
- [✓ Only Admin1 and Admin2]
- Only Admin1 and Admin3
- Only Admin1 and Admin4
- Admin1, Admin2, Admin3, and Admin4

[answer choice] can create new resource groups.

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

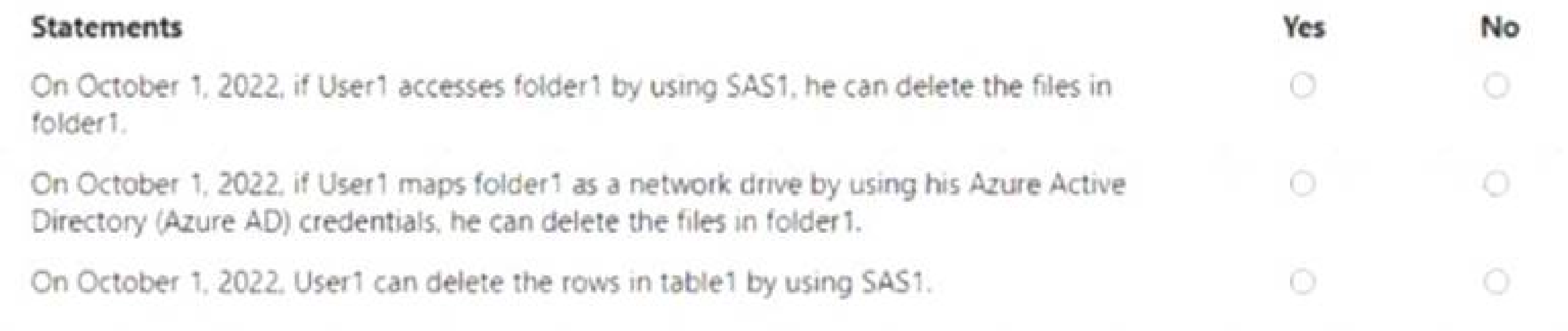
- Admin1 onl
- Admin2 only
- [✓ Admin3 only]
- Admin1 and Admin3 only
- Admin1, Admin2, Admin3, and Admin4

NEW QUESTION 149
- (Exam Topic 4)
You have an Azure subscription that contains a user named User1 and a storage account named storage 1. The storage1 account contains the resources shown in the following table:



Name	Type
container1	Container
folder1	File share
table1	Table

User1 is assigned the following roles for storage1:
• Storage Blob Data Reader
• Storage Table Data Contributor
• Storage File Data SMB Share Reader



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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
No, Yes, No

NEW QUESTION 153
- (Exam Topic 4)
You have an Azure subscription that contains an Azure SQL server named SQL1. SQL1 contains. You need to use Microsoft Defender for Cloud to complete a vulnerability assessment for DB1. What should you do first?

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

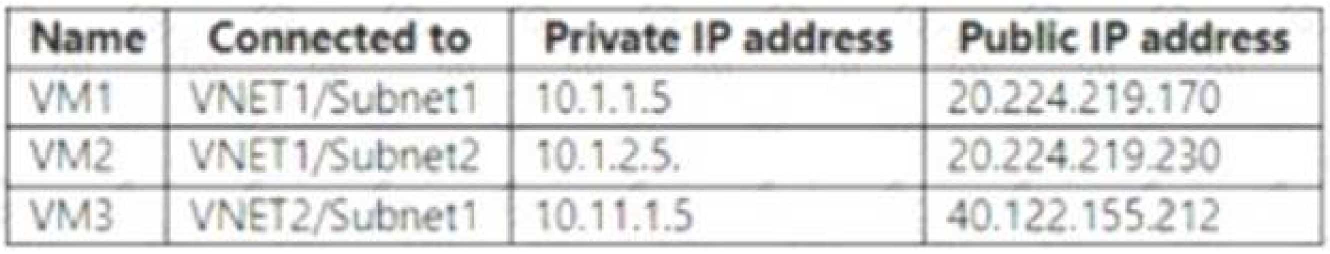
Answer: A

NEW QUESTION 156
- (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

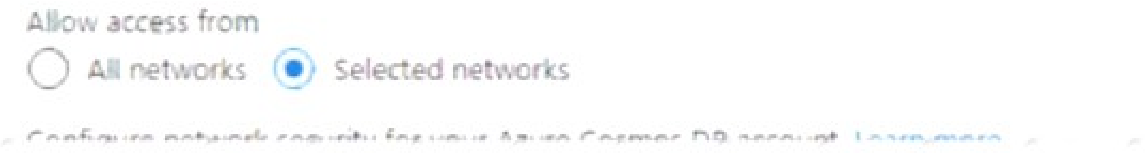
Answer: A

NEW QUESTION 161
- (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

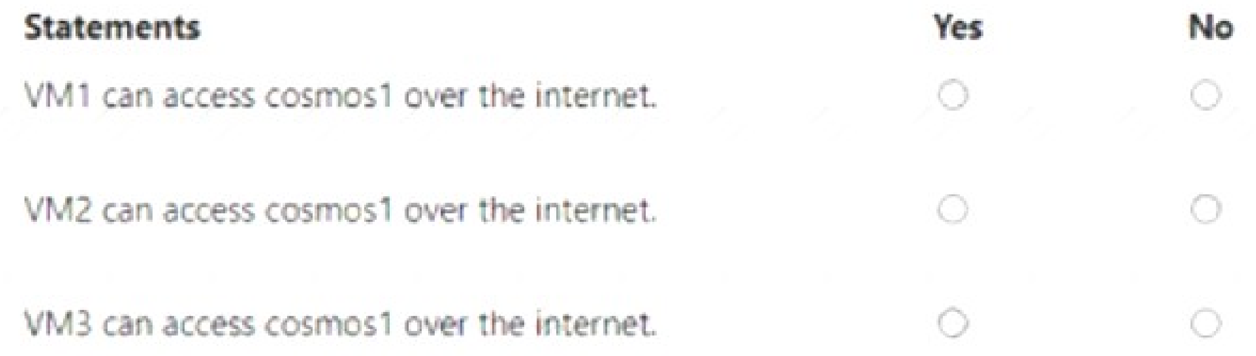
You have an Azure Cosmos DB account named cosmos1 configured as shown in the following exhibit.



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 164
- (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 165
- (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 167

- (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 9
You need to ensure that the rg1lod28681041n1 Azure Storage account is encrypted by using a key stored in the KeyVault28681041 Azure key vault.

A. Mastered
B. Not Mastered

Answer: A

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

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

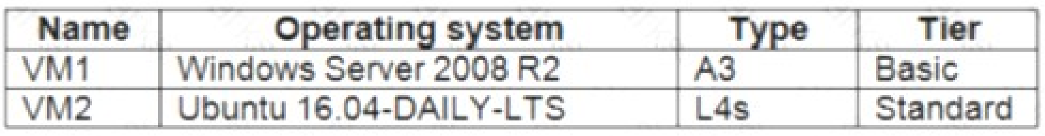
NEW QUESTION 171
- (Exam Topic 4)
Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
Your company has an Active Directory forest with a single domain, named 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 pass-through authentication and seamless SSO with password hash synchronization.
Does the solution meet the goal?

A. Yes
B. No

Answer: A

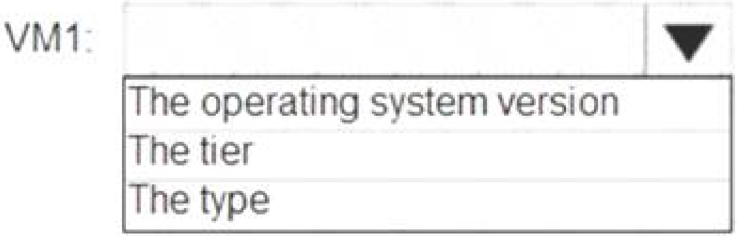
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

NEW QUESTION 175
- (Exam Topic 4)
You have two Azure virtual machines in the East US2 region as shown in the following table.

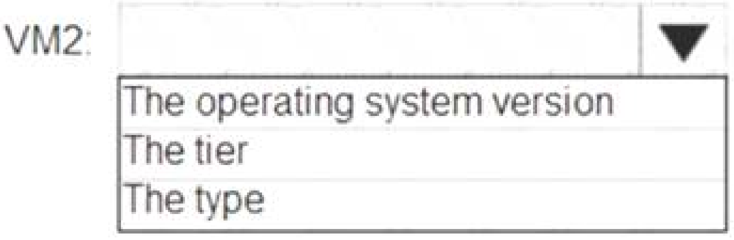


Name	Operating system	Type	Tier
VM1	Windows Server 2008 R2	A3	Basic
VM2	Ubuntu 16.04-DAILY-LTS	L4s	Standard

You deploy and configure an Azure Key vault.
You need to ensure that you can enable Azure Disk Encryption on VM1 and VM2.
What should you modify on each virtual machine? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



VM1:
The operating system version
The tier
The type



VM2:
The operating system version
The tier
The type

A. Mastered

B. Not Mastered

Answer: A

Explanation:
VM1: The Tier
The Tier needs to be upgraded to standard.
Disk Encryption for Windows and Linux IaaS VMs is in General Availability in all Azure public regions and Azure Government regions for Standard VMs and VMs with Azure Premium Storage.
VM2: the operating system
References:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/generation-2#generation-1-vs-generation-2-ca

NEW QUESTION 180
- (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 185
- (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 1
You need to configure Azure to allow RDP connections from the Internet to a virtual machine named VM1. The solution must minimize the attack surface of VM1.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
To configure Azure to allow RDP connections from the Internet to a virtual machine named VM1, you can follow the steps below:
- Create a new inbound security rule in the network security group (NSG) that is associated with the virtual network subnet that contains VM1. The rule should allow RDP traffic from the Internet to the virtual network subnet. You can use the Azure portal, Azure PowerShell, or Azure CLI to create the rule.
- Configure the network security group (NSG) to associate it with the virtual network subnet that contains VM1.
- Configure the virtual machine to allow RDP traffic. You can use the Azure portal, Azure PowerShell, or Azure CLI to configure the virtual machine.

To minimize the attack surface of VM1, you can use the following best practices:
- Use a strong password for the local administrator account on the virtual machine.
- Use Network Security Groups (NSGs) to restrict traffic to only the necessary ports and protocols.
- Use Azure Security Center to monitor and protect your virtual machines.

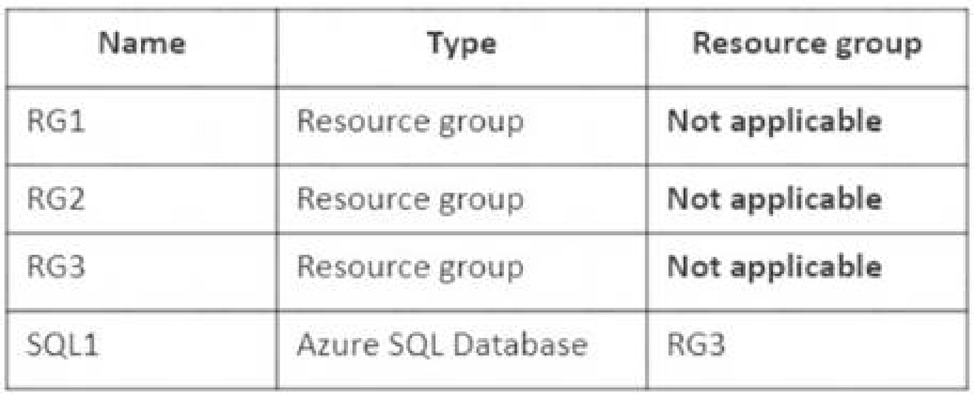
NEW QUESTION 189
- (Exam Topic 4)
You have an Azure subscription that contains a user named Adminl1 and a virtual machine named VM1. VM1 runs Windows Server 2019 and was deployed by using an Azure Resource Manager template. VM1 is the member of a backend pool of a public Azure Basic Load Balancer.
Admin1 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

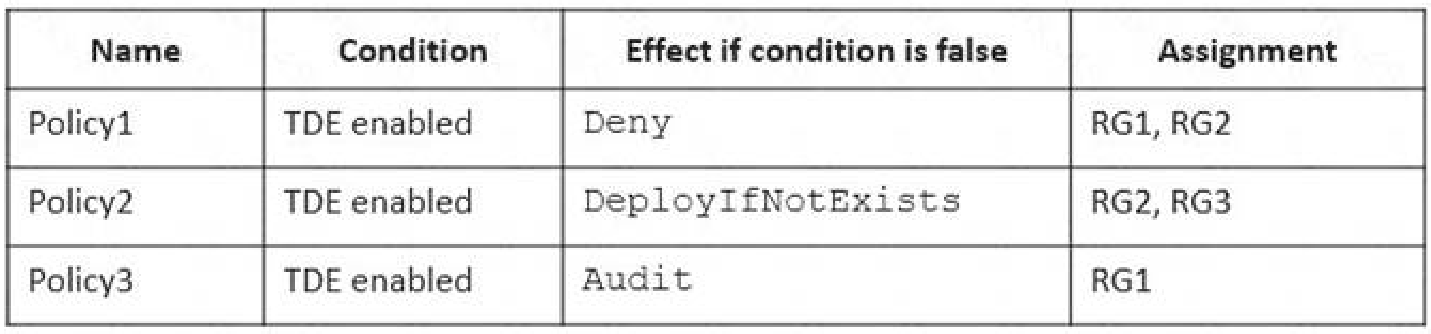
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time?tabs=jit-config-asc%2Cjit-re

NEW QUESTION 190
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.



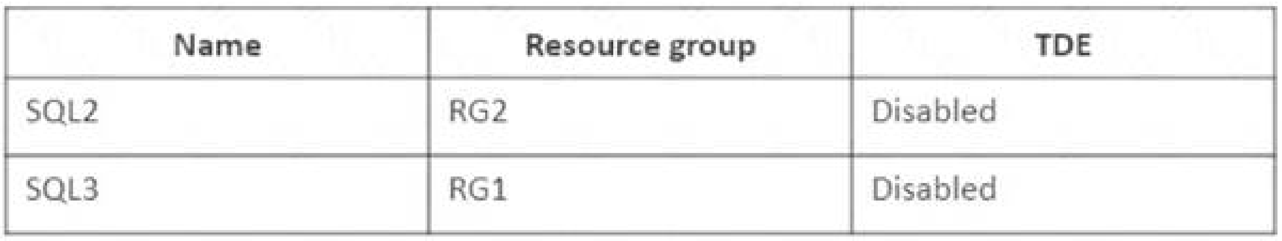
Name	Type	Resource group
RG1	Resource group	Not applicable
RG2	Resource group	Not applicable
RG3	Resource group	Not applicable
SQL1	Azure SQL Database	RG3

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



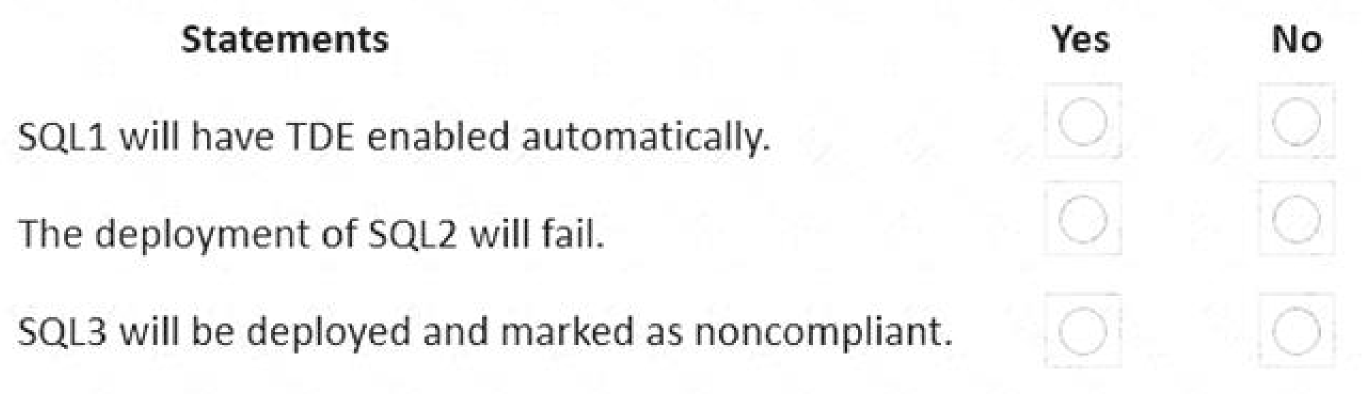
Name	Condition	Effect if condition is false	Assignment
Policy1	TDE enabled	Deny	RG1, RG2
Policy2	TDE enabled	DeployIfNotExists	RG2, RG3
Policy3	TDE enabled	Audit	RG1

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.



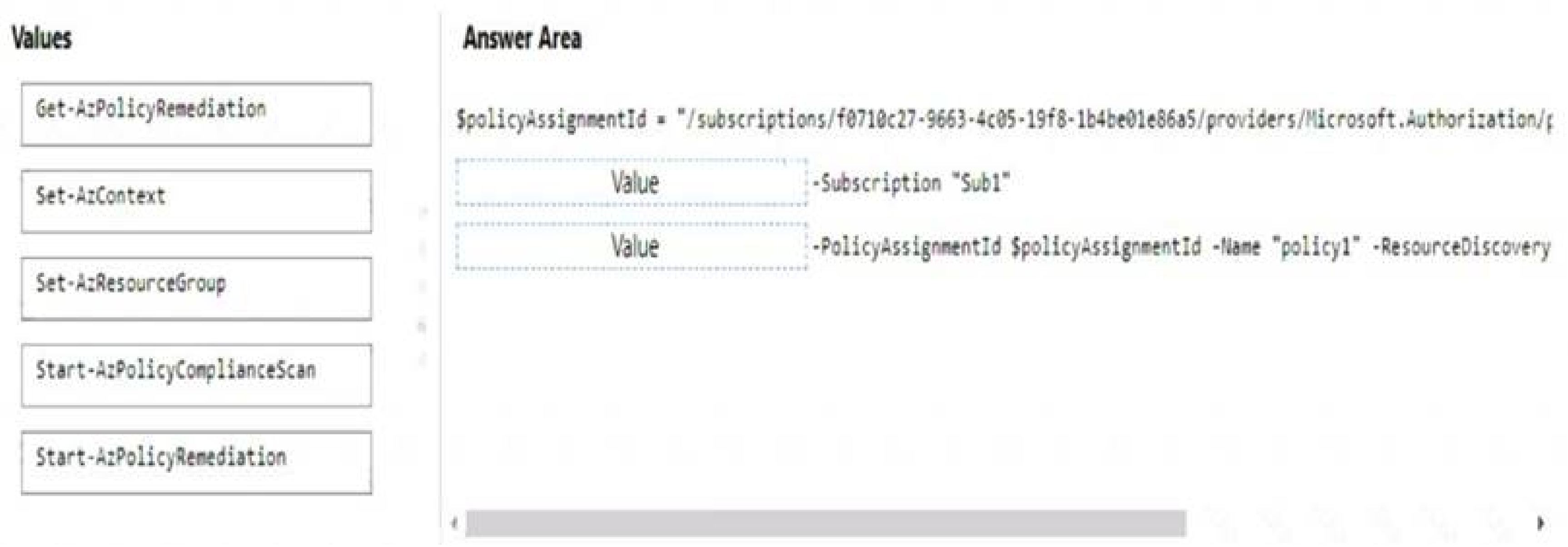
Statements	Yes	No
SQL1 will have TDE enabled automatically.	○	○
The deployment of SQL2 will fail.	○	○
SQL3 will be deployed and marked as noncompliant.	○	○

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 193
- (Exam Topic 4)
You have two Azure subscriptions named Sub1 and Sub2. Sub1 contains a resource group named RG1 and an Azure policy named Policy1.
You need to remediate the non-compliant resources in Sub1 based on Policy1.
How should you complete the PowerShell script? To answer, drag the appropriate values to the correct targets. Each value may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content. NOTE: Each correct selection is worth one point.



Values

- Get-AzPolicyRemediation
- Set-AzContext
- Set-AzResourceGroup
- Start-AzPolicyComplianceScan
- Start-AzPolicyRemediation

Answer Area

```
$policyAssignmentId = "/subscriptions/f0710c27-9663-4c05-19f8-1b4be01e86a5/providers/Microsoft.Authorization/p
Value -Subscription "Sub1"
Value -PolicyAssignmentId $policyAssignmentId -Name "policy1" -ResourceDiscovery
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:

For the first blank, use Set-AzContext
to set the current subscription context.

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

NEW QUESTION 195

- (Exam Topic 4)
Your company plans to create separate subscriptions for each department. Each subscription will be associated to the same Azure Active Directory (Azure AD) tenant.
You need to configure each subscription to have the same role assignments. What should you use?

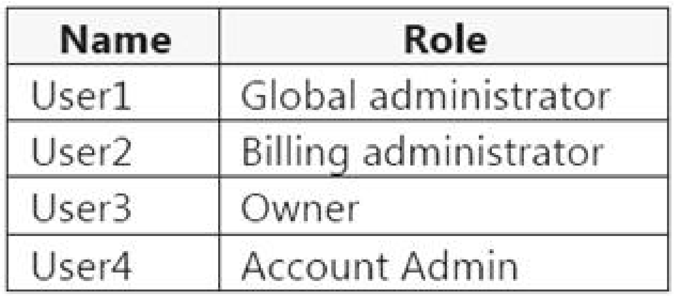
A. Azure Security Center
B. Azure Blueprints
C. Azure AD Privileged Identity Management (PIM)
D. Azure Policy

Answer: B

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

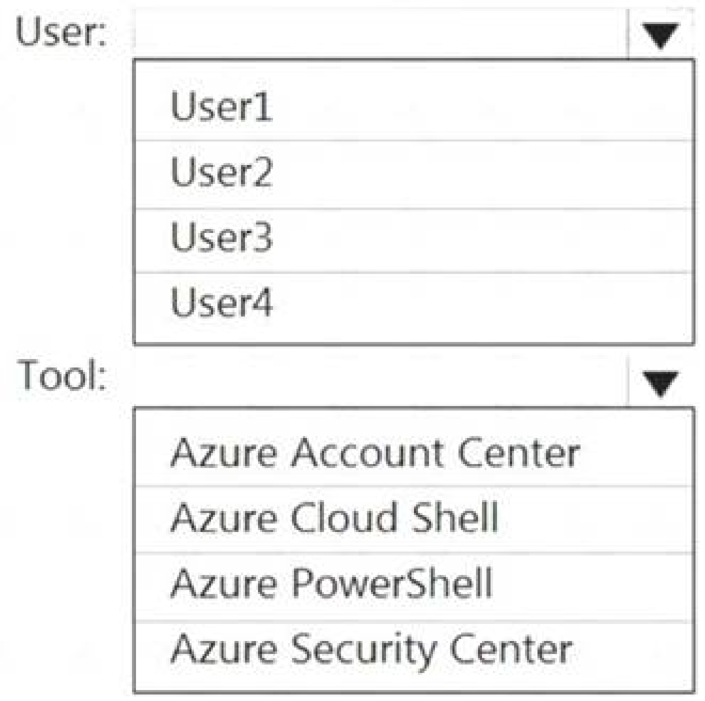
NEW QUESTION 197

- (Exam Topic 4)
Your company has an Azure subscription named Subscription1. Subscription1 is associated with the Azure Active Directory tenant that includes 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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Table Description automatically generated
Reference:
https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/billing-subscription-transfer

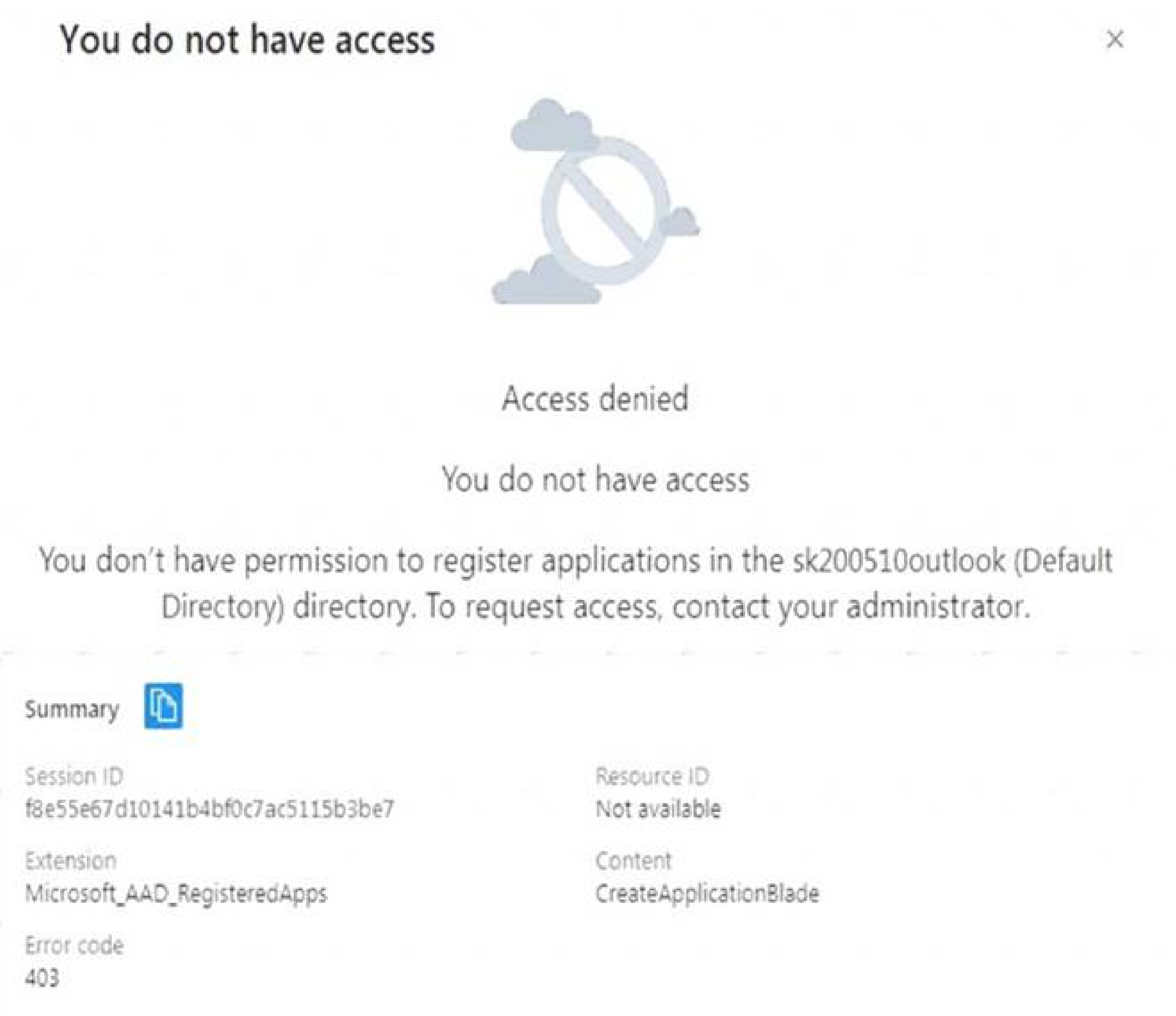
NEW QUESTION 199
- (Exam Topic 4)
You have an Azure subscription that contains a resource group named RG1 and a security group serverless RG1 contains 10 virtual machine, a virtual network VNET1, and a network security group (NSG) named NSG1. ServerAdmins can access the virtual machines by using RDP.
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 203
- (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 208
- (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 212
- (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 215
- (Exam Topic 4)
You have a Azure subscription.
You enable Azure Active Directory (Azure AD) Privileged identify (PIM).
Your company's security policy for administrator accounts has the following conditions:
* The accounts must use multi-factor authentication (MFA).
* The account must use 20-character complex passwords.
* The passwords must be changed every 180 days.
* The account must be managed by using PIM.
You receive alerts about administrator who have not changed their password during the last 90 days. You need to minimize the number of generated alerts.
Which PIM alert should you modify?

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

Answer: D

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

NEW QUESTION 217
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains a user named Admin1. Admin1 is assigned the Application developer role.
You purchase a cloud app named App1 and register App1 in Azure AD.
Admin1 reports that the option to enable token encryption for App1 is unavailable.
You need to ensure that Admin1 can enable token encryption for App1 in the Azure portal. What should you do?

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

Answer: C

Explanation:
This is a tricky one because uploading a certificate is also required. However, the question states that the Token Encryption option is unavailable. This is because the app is not added as an enterprise application. When the app is added as an enterprise application, the Token Encryption option will be available. Then you can upload the certificate.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/howto-saml-token-encryption

NEW QUESTION 218
- (Exam Topic 4)
You company has an Azure subscription named Sub1. Sub1 contains an Azure web app named WebApp1 that uses Azure Application Insights. WebApp1 requires users to authenticate by using OAuth 2.0 client secrets.
Developers at the company plan to create a multi-step web test app that preforms synthetic transactions emulating user traffic to Web App1.
You need to ensure that web tests can run unattended. What should you do first?

A. In Microsoft Visual Studio, modify the .webtest file.

B. Upload the .webtest file to Application Insights.
C. Register the web test app in Azure AD.
D. Add a plug-in to the web test app.

Answer: B

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

NEW QUESTION 219
- (Exam Topic 4)
You have an Azure subscription named Subcription1 that contains an Azure Active Directory (Azure AD) tenant named contosos.com and a resource group named RG1.
You create a custom role named Role1 for contoso.com.
You need to identify where you can use Role1 for permission delegation. What should you identify?

A. contoso.com only
B. contoso.com and RGT only
C. contoso.com and Subscription1 only
D. contoso.com, RG1, and Subcription1

Answer: A

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

NEW QUESTION 220
- (Exam Topic 4)
You have an Azure subscription that contains a virtual machine named VM1. You create an Azure key vault that has the following configurations:

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

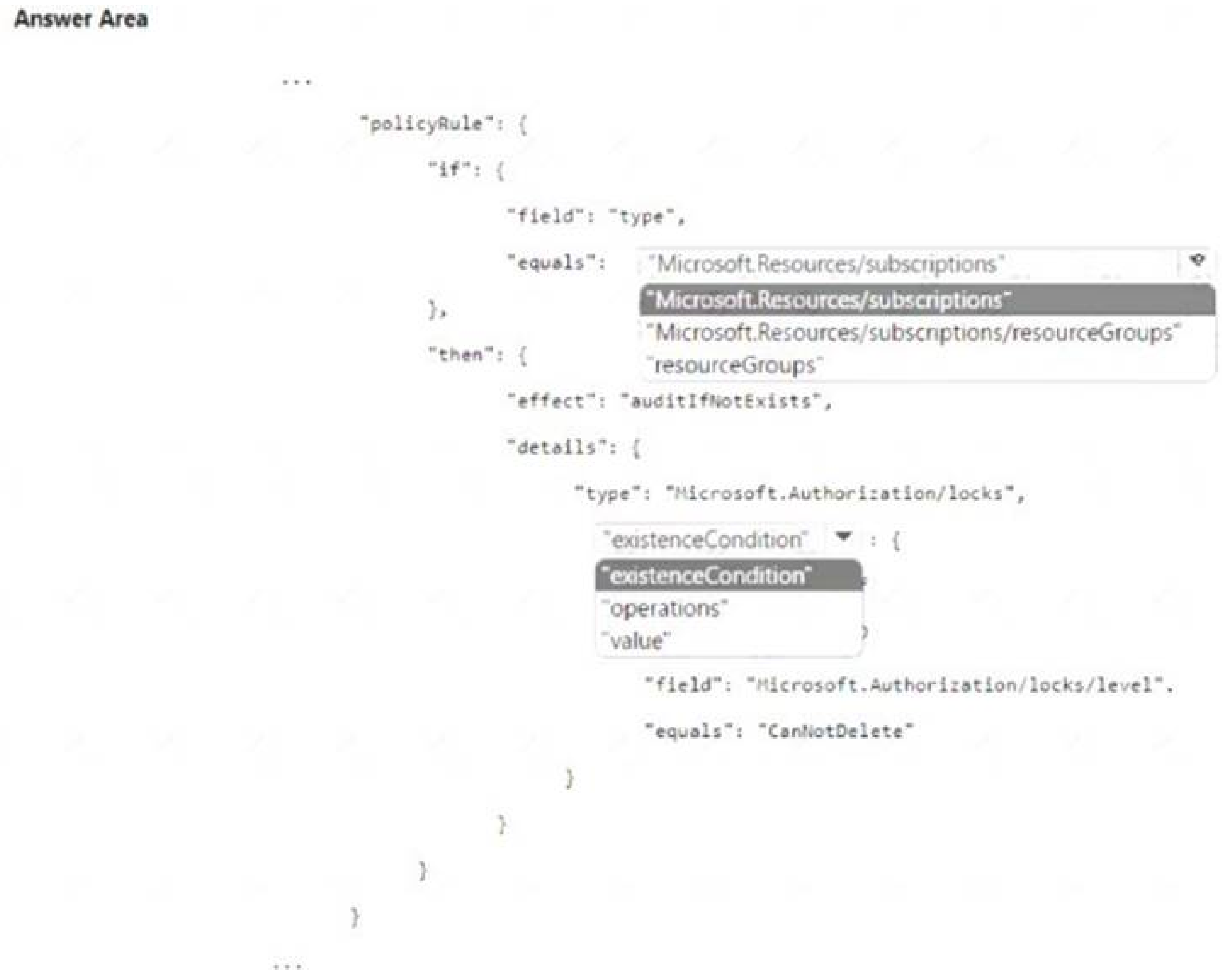
You need to use Vault5 to enable Azure Disk Encryption on VM1. The solution must support backing up VM1 by using Azure Backup.
Which key vault settings should you configure?

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

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

NEW QUESTION 222
- (Exam Topic 4)
You plan to deploy a custom policy initiative for Microsoft Defender for Cloud. You need to identify all the resource groups that have a Delete lock.
How should you complete the policy definition? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

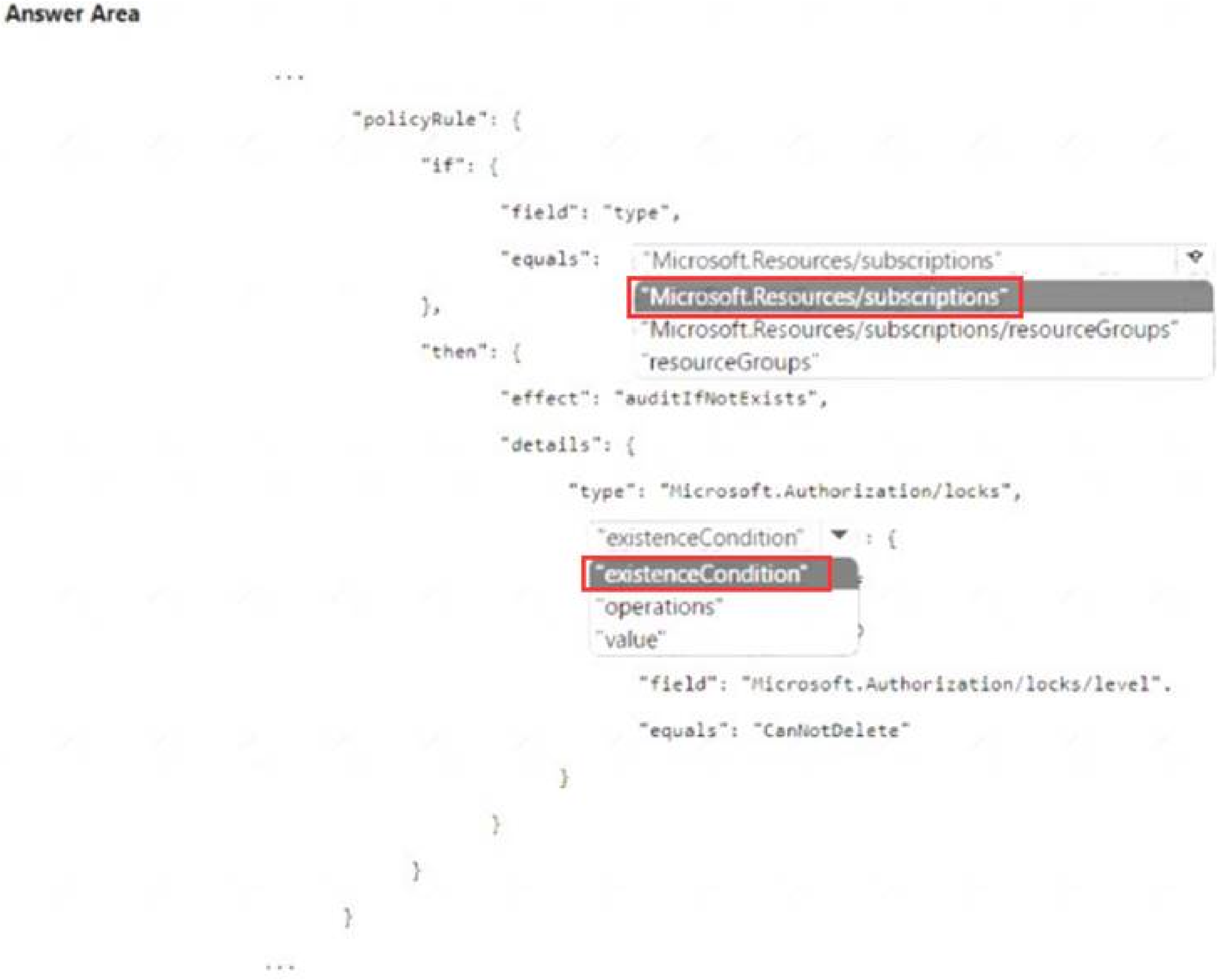
```
...
    "policyRule": {
        "if": {
            "field": "type",
            "equals": "Microsoft.Resources/subscriptions"
        },
        "then": {
            "effect": "auditIfNotExists",
            "details": {
                "type": "Microsoft.Authorization/locks",
                "existenceCondition"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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

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

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

NEW QUESTION 224

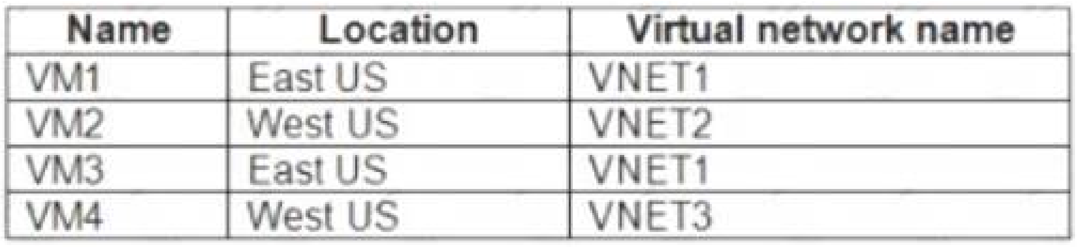
- (Exam Topic 4)
You have Azure Resource Manager templates that you use to deploy Azure virtual machines.
You need to disable unused Windows features automatically as instances of the virtual machines are provisioned.
What should you use?

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

Answer: B

Explanation:
You can use Azure Automation State Configuration to manage Azure VMs (both Classic and Resource Manager), on-premises VMs, Linux machines, AWS VMs, and on-premises physical machines.
Note: Azure Automation State Configuration provides a DSC pull server similar to the Windows Feature DSCService so that target nodes automatically receive configurations, conform to the desired state, and report back on their compliance. The built-in pull server in Azure Automation eliminates the need to set up and maintain your own pull server. Azure Automation can target virtual or physical Windows or Linux machines, in the cloud or on-premises.
References:
https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started

NEW QUESTION 228
- (Exam Topic 4)
You have an Azure subscription that contains the virtual machines shown in the following table.



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

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

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

Answer: A

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

NEW QUESTION 230
- (Exam Topic 4)
You have an Azure subscription named Sub1.
In Azure Security Center, you have a workflow automation named WF1. WF1 is configured to send an email message to a user named User1.
You need to modify WF1 to send email messages to a distribution group named Alerts. What should you use to modify WF1?

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

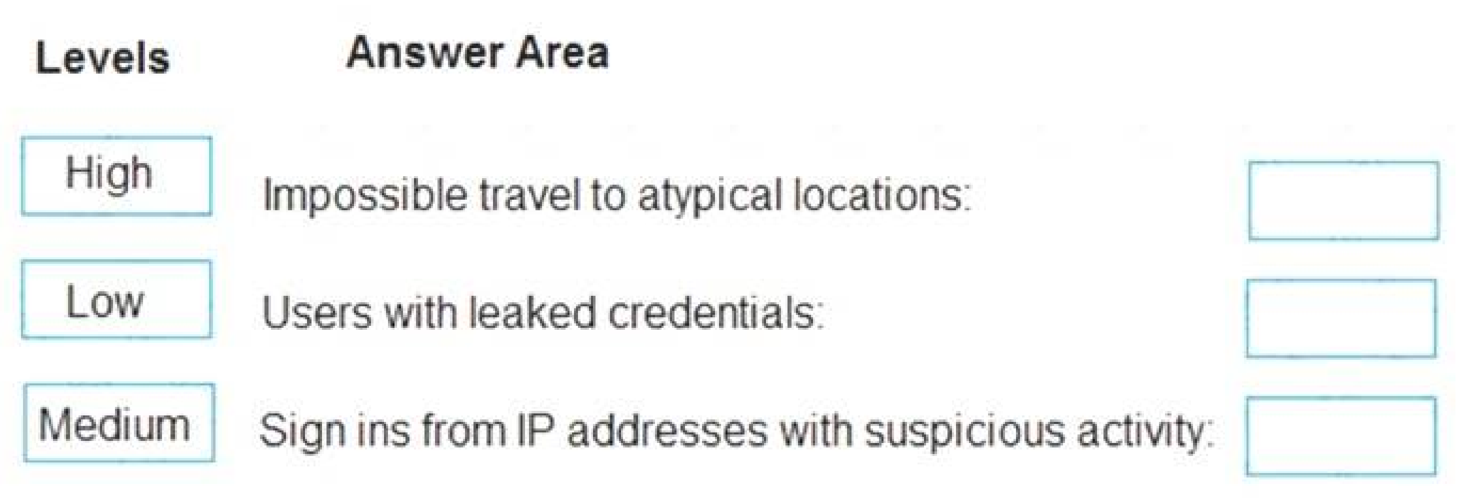
Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation
https://docs.microsoft.com/en-us/learn/modules/resolve-threats-with-azure-security-center/6-exerciseconfigure-p

NEW QUESTION 231
- (Exam Topic 4)
You are implementing conditional access policies.
You must evaluate the existing Azure Active Directory (Azure AD) risk events and risk levels to configure and implement the policies.
You need to identify the risk level of the following risk events:

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

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



Levels

High

Low

Medium

Answer Area

Impossible travel to atypical locations:

Users with leaked credentials:

Sign ins from IP addresses with suspicious activity:

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Medium High Medium Refer
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risk-events#sign-ins-from-ip

NEW QUESTION 235
- (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 239
- (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 4
You need to ensure that a user named user2-28681041 can manage the properties of the virtual machines in the RG1lod28681041 resource group. The solution must use the principle of least privilege.

A. Mastered
B. Not Mastered

Answer: A

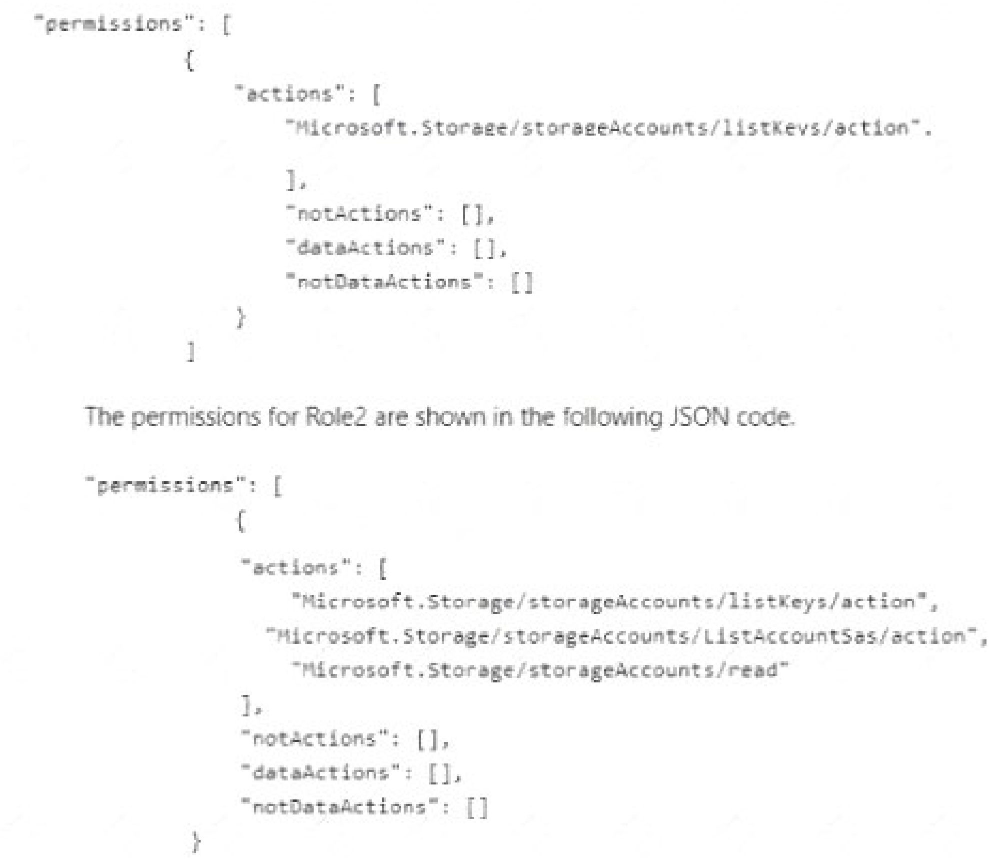
Explanation:
To ensure that a user named user2-28681041 can manage the properties of the virtual machines in the RG1lod28681041 resource group using the principle of least privilege, you can follow these steps:

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

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

NEW QUESTION 242
- (Exam Topic 4)

You have an Azure subscription mat contains a resource group named RG1. RG1 contains a storage account named storage1.
You have two custom Azure rotes named Role1 and Role2 that are scoped to RG1. The permissions for Role1 are shown in the following JSON code.

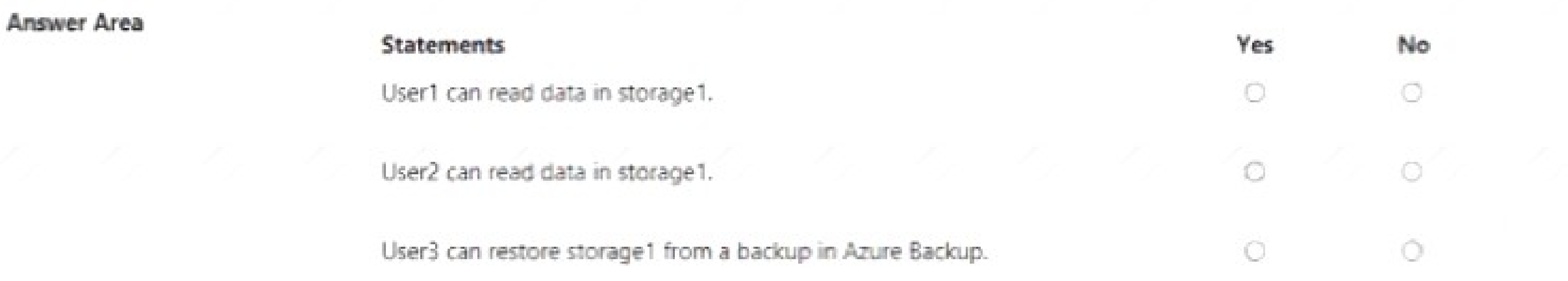


```
"permissions": [
            {
                "actions": [
                    "Microsoft.Storage/storageAccounts/listKeys/action".

                    ],
                    "notActions": [],
                    "dataActions": [],
                    "notDataActions": []
                }
            ]
```

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

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



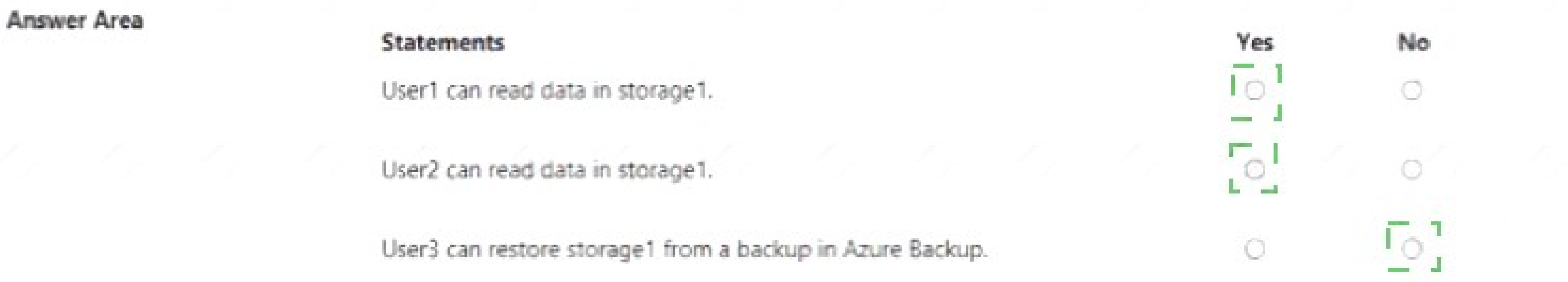
Answer Area

Statements	Yes	No
User1 can read data in storage1.	○	○
User2 can read data in storage1.	○	○
User3 can restore storage1 from a backup in Azure Backup.	○	○

A. Mastered
B. Not Mastered

Answer: A

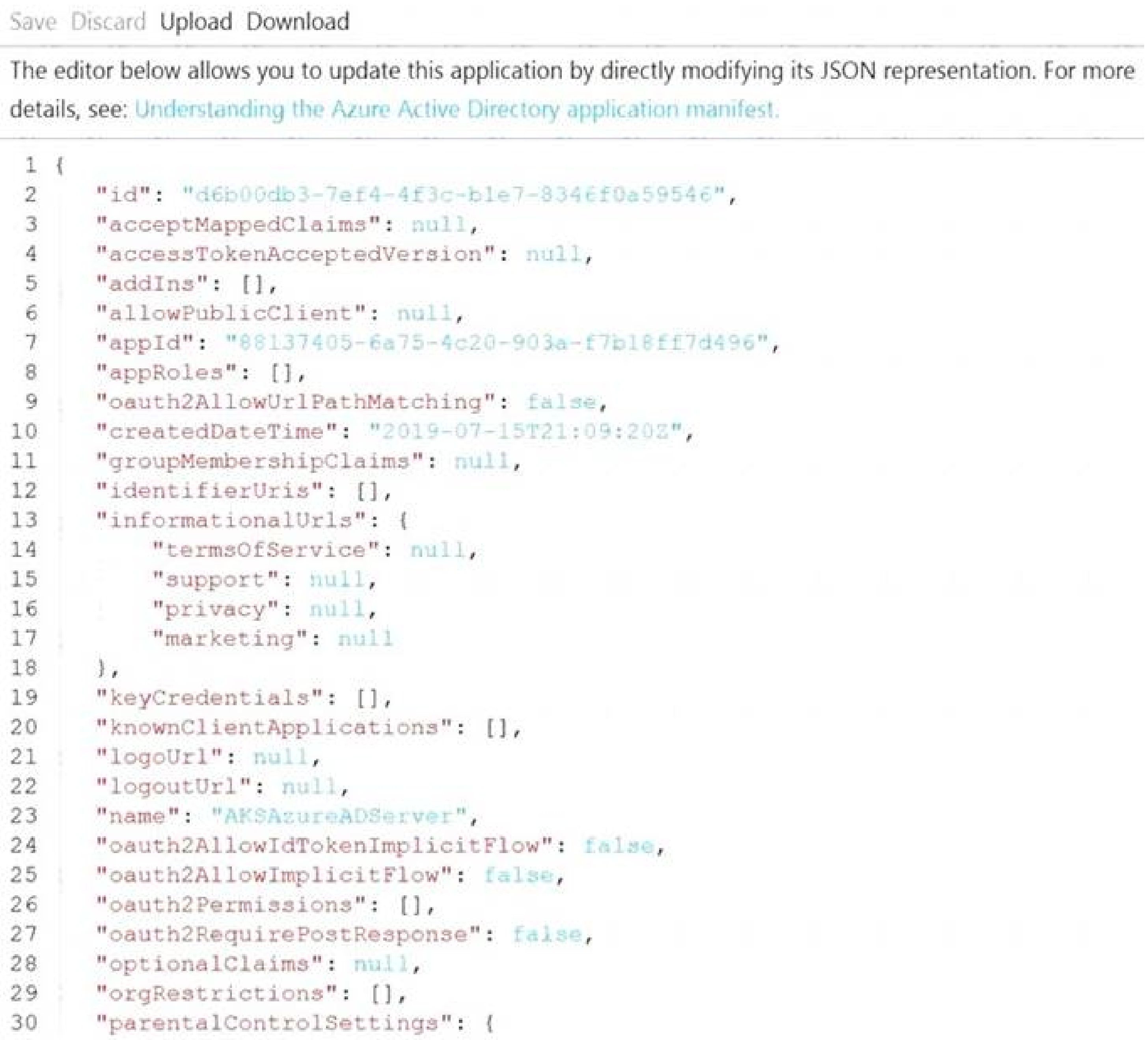
Explanation:



Answer Area

Statements	Yes	No
User1 can read data in storage1.	[✓ ○]	○
User2 can read data in storage1.	[✓ ○]	○
User3 can restore storage1 from a backup in Azure Backup.	○	[✓ ○]

NEW QUESTION 245
- (Exam Topic 4)
You plan to create an Azure Kubernetes Service (AKS) cluster in an Azure subscription. The manifest of the registered server application is shown in the following exhibit.



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

```
{
    "id": "d6b00db3-7ef4-4f3c-b1e7-8346f0a59546",
    "acceptMappedClaims": null,
    "accessTokenAcceptedVersion": null,
    "addIns": [],
    "allowPublicClient": null,
    "appId": "88137405-6a75-4c20-903a-f7b18ff7d496",
    "appRoles": [],
    "oauth2AllowUrlPathMatching": false,
    "createdDateTime": "2019-07-15T21:09:20Z",
    "groupMembershipClaims": null,
    "identifierUris": [],
    "informationalUrls": {
        "termsOfService": null,
        "support": null,
        "privacy": null,
        "marketing": null
    },
    "keyCredentials": [],
    "knownClientApplications": [],
    "logoUrl": null,
    "logoutUrl": null,
    "name": "AKSAzureADServer",
    "oauth2AllowIdTokenImplicitFlow": false,
    "oauth2AllowImplicitFlow": false,
    "oauth2Permissions": [],
    "oauth2RequirePostResponse": false,
    "optionalClaims": null,
    "orgRestrictions": [],
    "parentalControlSettings": {
```

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

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

Answer: C

Explanation:

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

NEW QUESTION 249
- (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

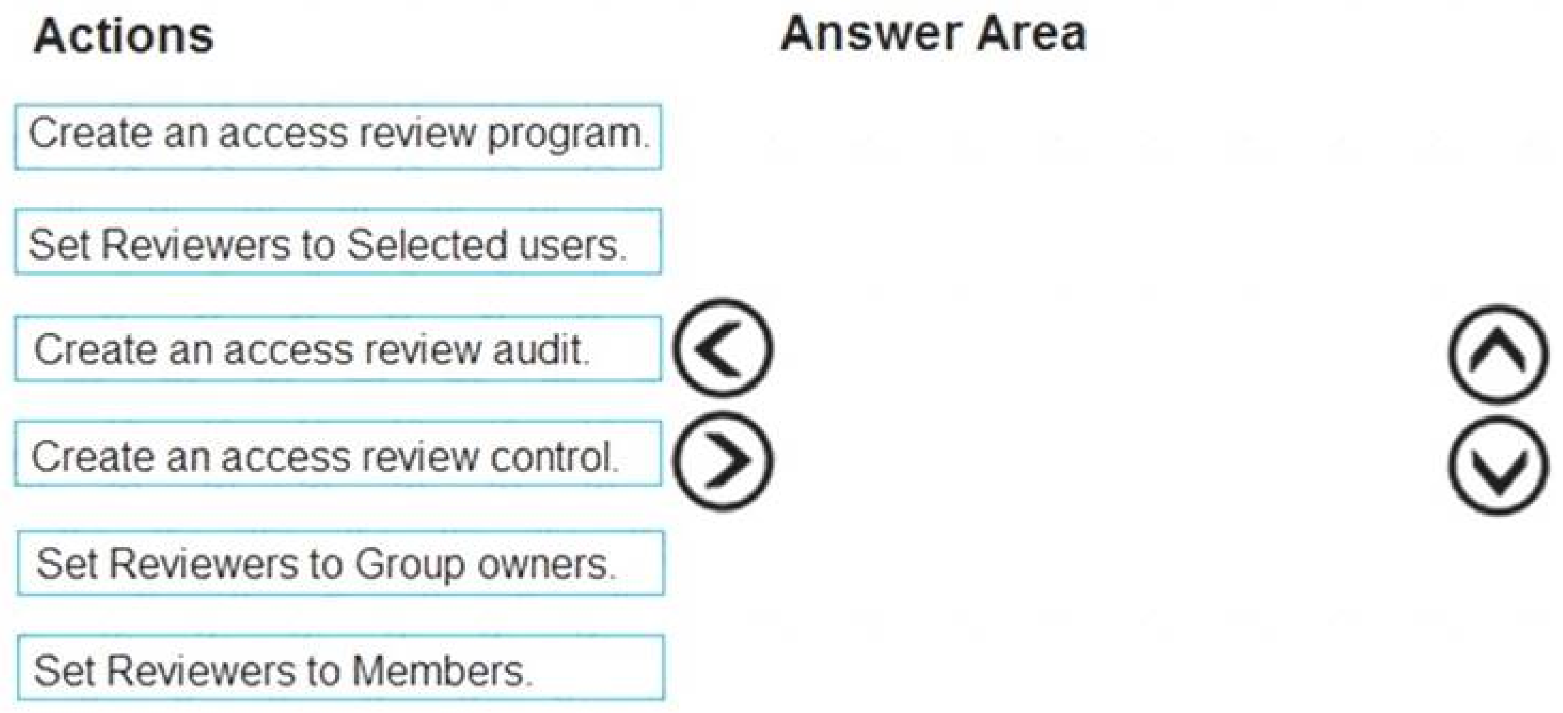
Explanation:
A network security group (NSG) enables you to filter inbound traffic to, and outbound traffic from, a virtual machine (VM). You can log network traffic that flows through an NSG with Network Watcher's NSG flow log
capability. Steps include:

- 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 253
- (Exam Topic 4)

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



Actions

Answer Area

Create an access review program.

Set Reviewers to Selected users.

Create an access review audit.

Create an access review control.

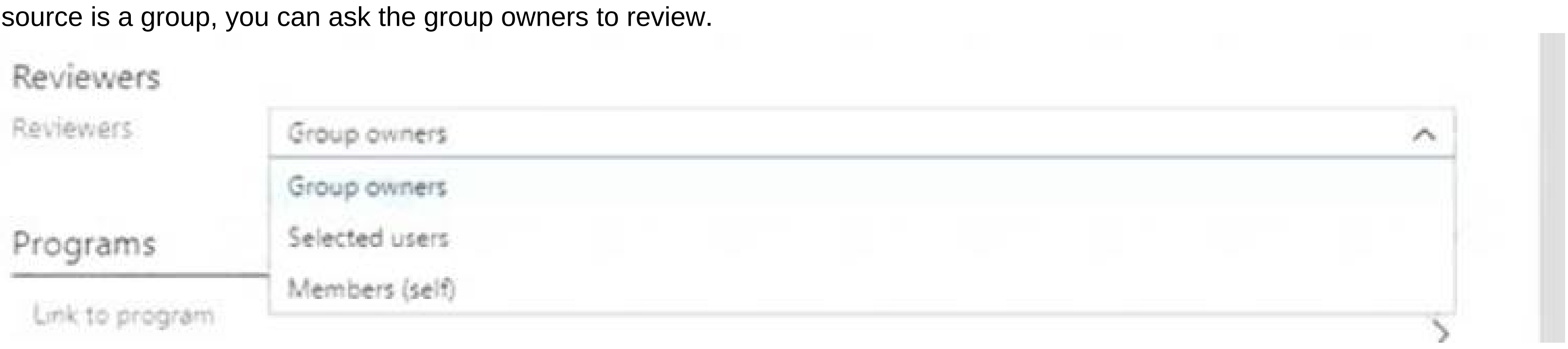
Set Reviewers to Group owners.

Set Reviewers to Members.

A. Mastered
B. Not Mastered

Answer: A

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

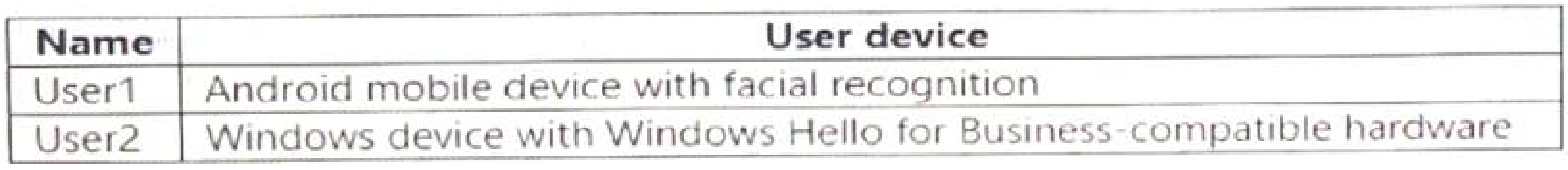


Reviewers

Reviewers: Group owners

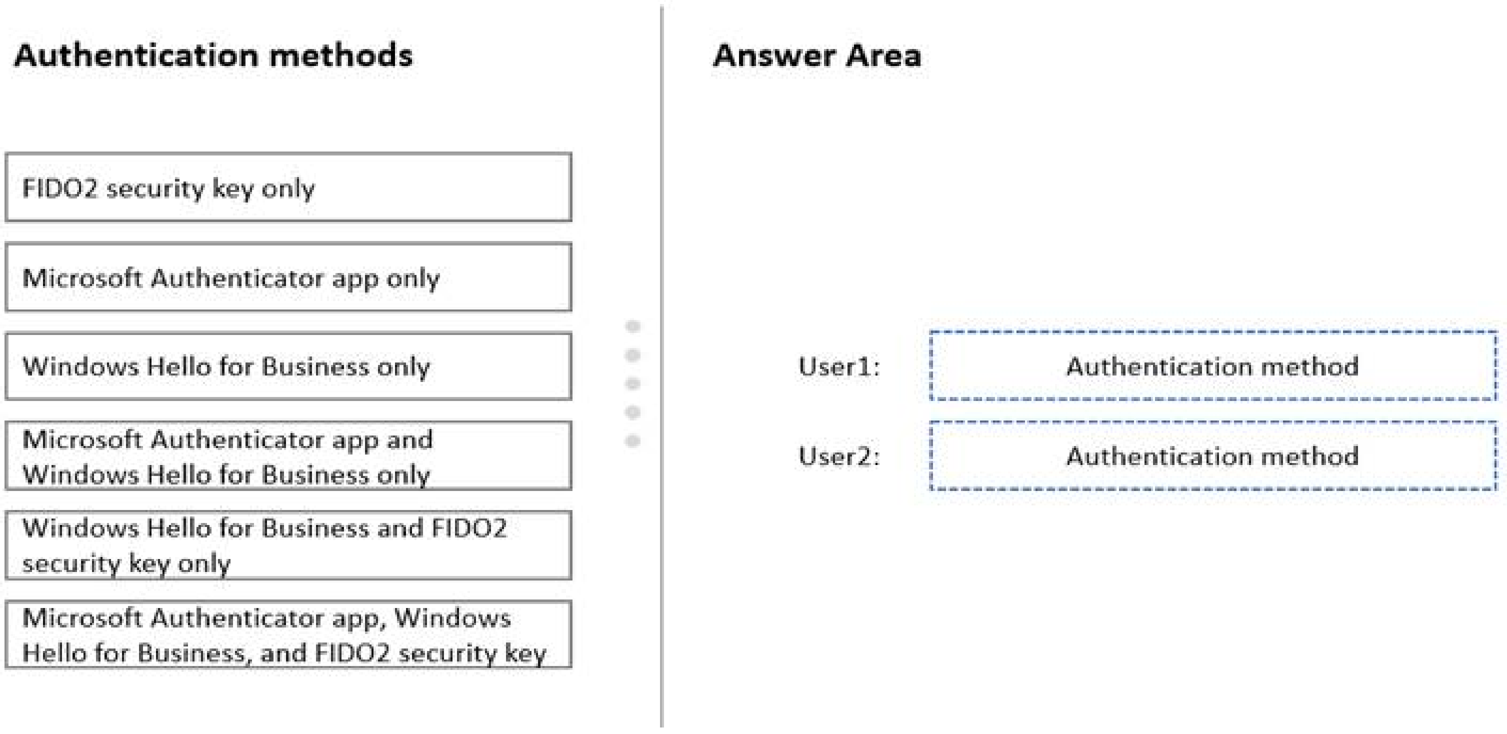
References:
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-programs-controls

NEW QUESTION 258
- (Exam Topic 4)
You have an Azure AD tenant that contains the users shown in the following table.



Name	User device
User1	Android mobile device with facial recognition
User2	Windows device with Windows Hello for Business-compatible hardware

You enable passwordless authentication for the tenant.
Which authentication method can each user use for passwordless authentication? To answer, drag the appropriate authentication methods to the correct users. Each authentication method 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.



Authentication methods

- FIDO2 security key only
- Microsoft Authenticator app only
- Windows Hello for Business only
- Microsoft Authenticator app and Windows Hello for Business only
- Windows Hello for Business and FIDO2 security key only
- Microsoft Authenticator app, Windows Hello for Business, and FIDO2 security key

Answer Area

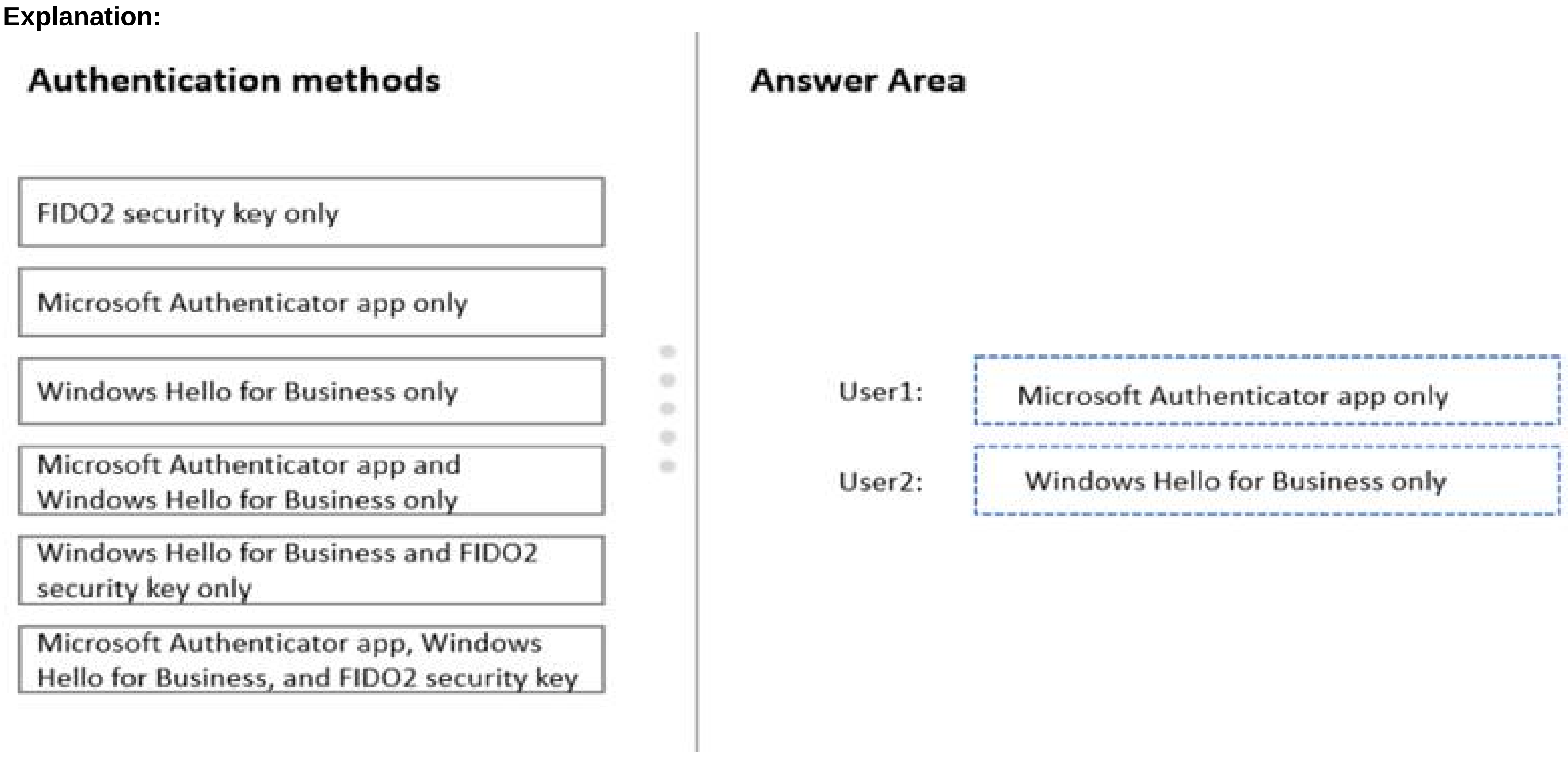
User1: Authentication method

User2: Authentication method

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Authentication methods

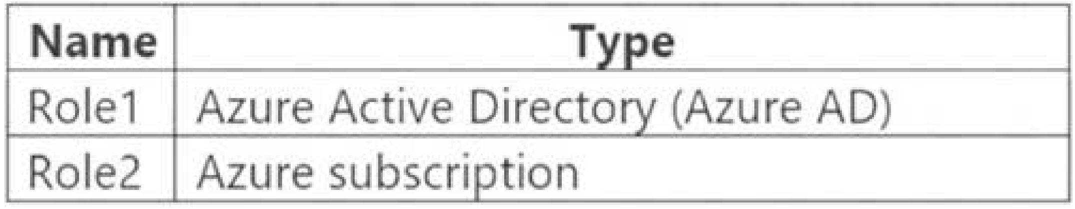
- FIDO2 security key only
- Microsoft Authenticator app only
- Windows Hello for Business only
- Microsoft Authenticator app and Windows Hello for Business only
- Windows Hello for Business and FIDO2 security key only
- Microsoft Authenticator app, Windows Hello for Business, and FIDO2 security key

Answer Area

User1: Microsoft Authenticator app only

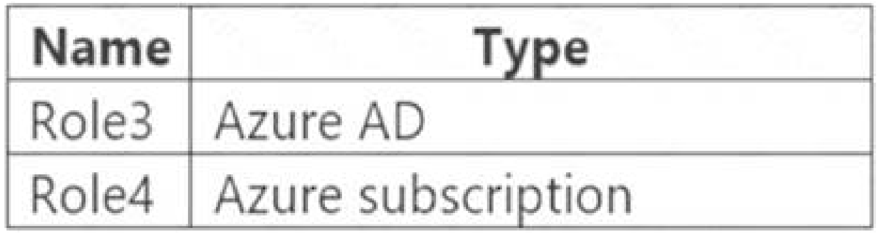
User2: Windows Hello for Business only

NEW QUESTION 259
- (Exam Topic 4)
You have an Azure subscription that contains the custom roles shown in the following table.



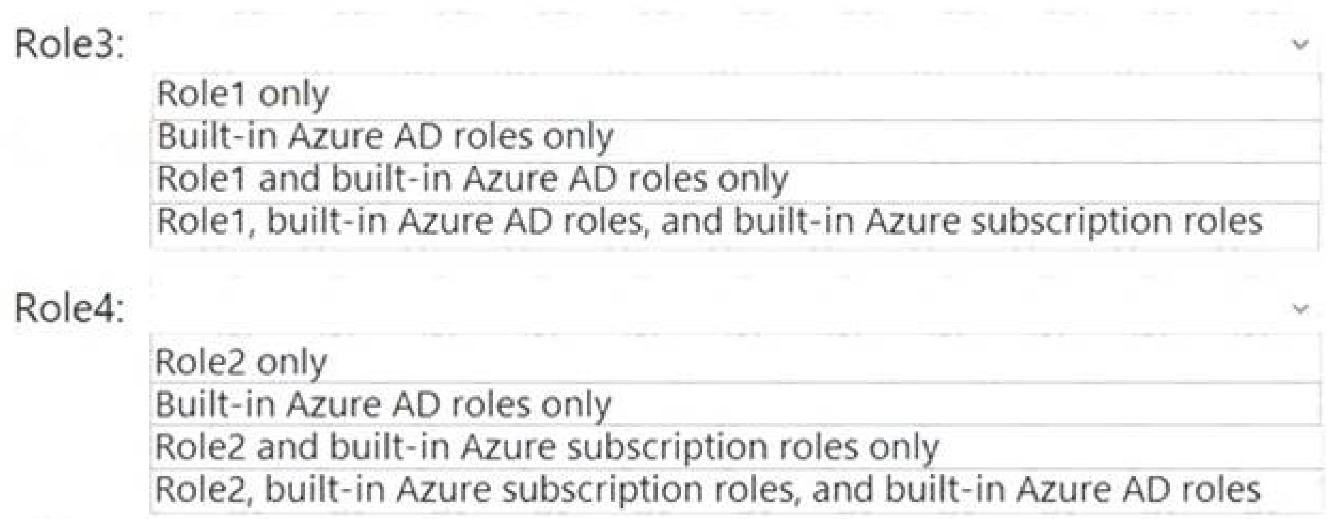
Name	Type
Role1	Azure Active Directory (Azure AD)
Role2	Azure subscription

In the Azure portal, you plan to create new custom roles by cloning existing roles. The new roles will be configured as shown in the following table.



Name	Type
Role3	Azure AD
Role4	Azure subscription

Which roles can you clone to create each new role? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Role3:
- Role1 only
- Built-in Azure AD roles only
- Role1 and built-in Azure AD roles only
- Role1, built-in Azure AD roles, and built-in Azure subscription roles

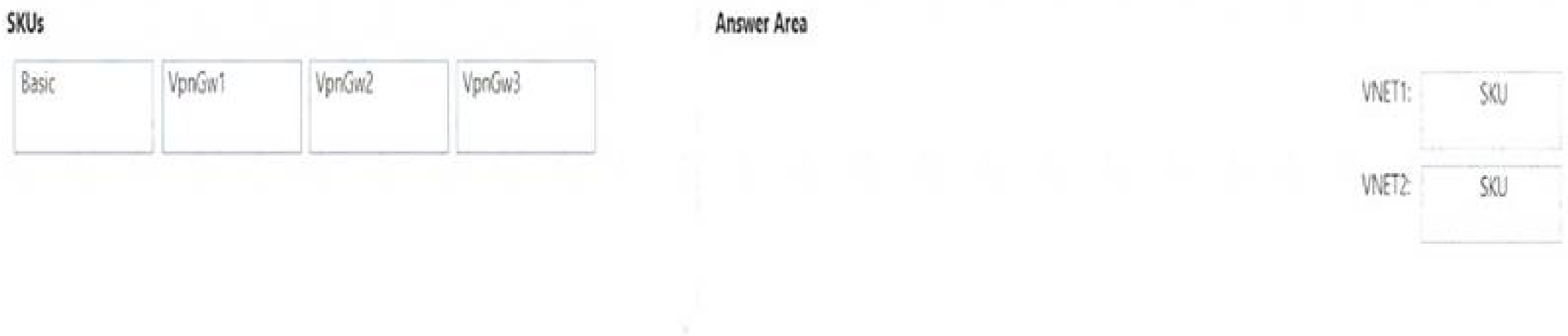
Role4:
- Role2 only
- Built-in Azure AD roles only
- Role2 and built-in Azure subscription roles only
- Role2, built-in Azure subscription roles, and built-in Azure AD roles

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/active-directory/roles/custom-create https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal

NEW QUESTION 263
- (Exam Topic 4)
You are configuring network connectivity for two Azure virtual networks named VNET1 and VNET2. You need to implement VPN gateways for the virtual networks to meet the following requirements:
* VNET1 must have six site-to-site connections that use BGP.
* VNET2 must have 12 site-to-site connections that use BGP.
* Costs must be minimized.
Which VPN gateway SKI) should you use for each virtual network? To answer, drag the appropriate SKUs to the correct networks. Each SKU may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point



SKUs

Basic | VpnGw1 | VpnGw2 | VpnGw3

Answer Area

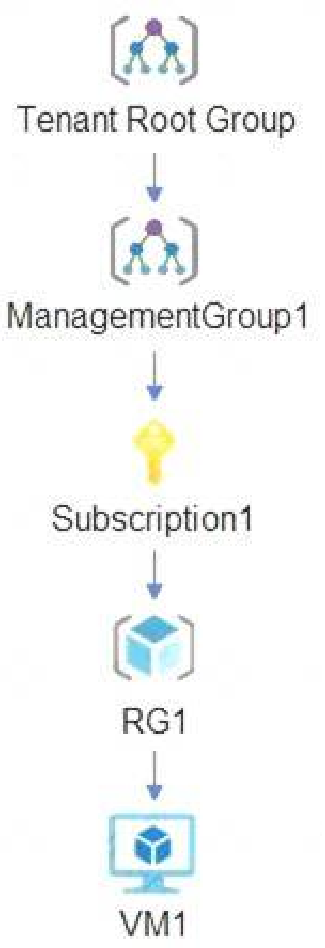
VNET1: SKU
VNET2: SKU

A. Mastered
B. Not Mastered

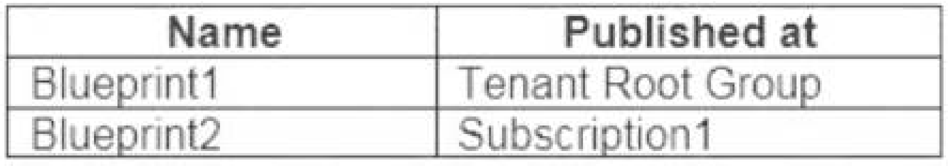
Answer: A

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

NEW QUESTION 268
- (Exam Topic 4)
You have the hierarchy of Azure resources shown in the following exhibit.

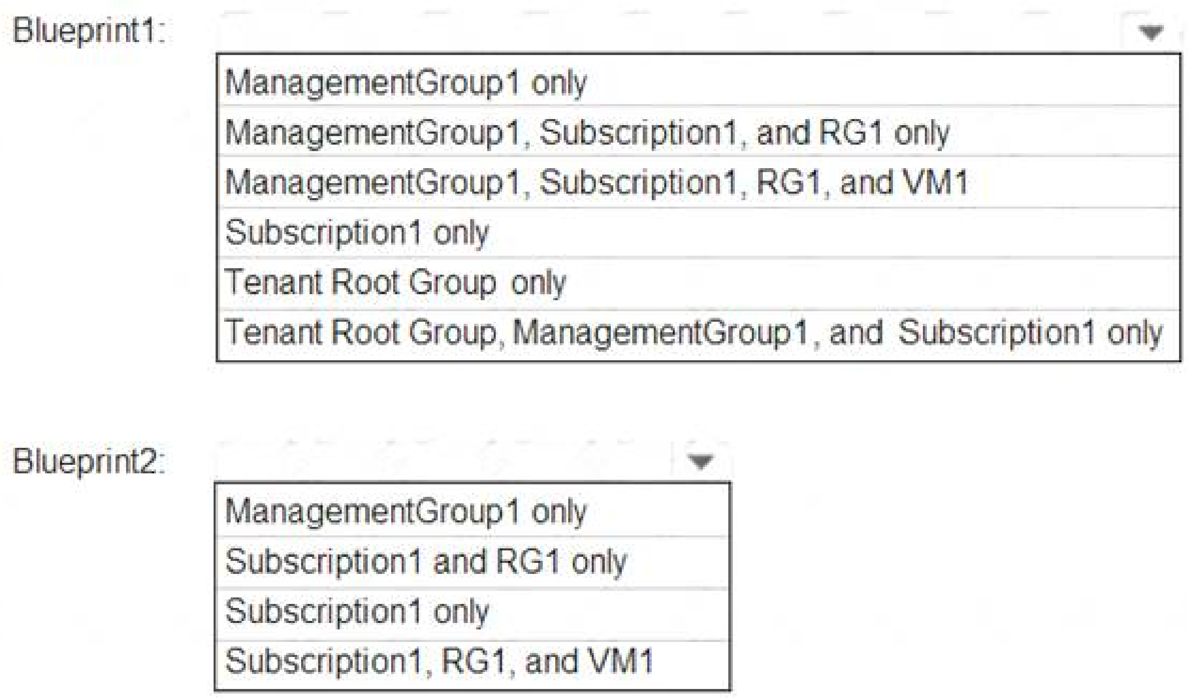


You create the Azure Blueprints definitions shown in the following table.



Name	Published at
Blueprint1	Tenant Root Group
Blueprint2	Subscription1

To which objects can you assign Blueprint1 and Blueprint2? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Blueprint1:
- ManagementGroup1 only
- ManagementGroup1, Subscription1, and RG1 only
- ManagementGroup1, Subscription1, RG1, and VM1
- Subscription1 only
- Tenant Root Group only
- Tenant Root Group, ManagementGroup1, and Subscription1 only

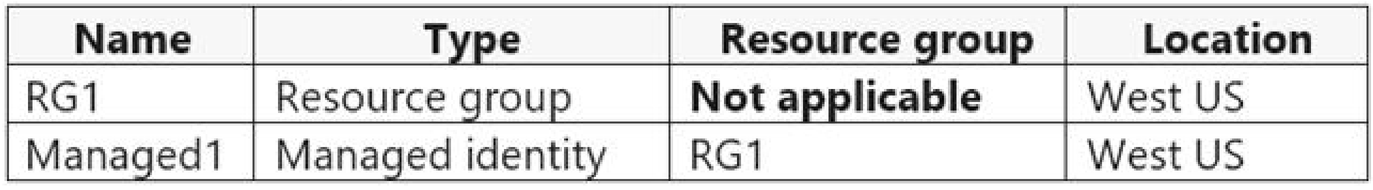
Blueprint2:
- ManagementGroup1 only
- Subscription1 and RG1 only
- Subscription1 only
- Subscription1, RG1, and VM1

A. Mastered
B. Not Mastered

Answer: A

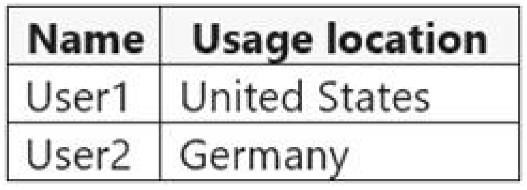
Explanation:
Blueprints can only be assigned to subscriptions.

NEW QUESTION 272
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.



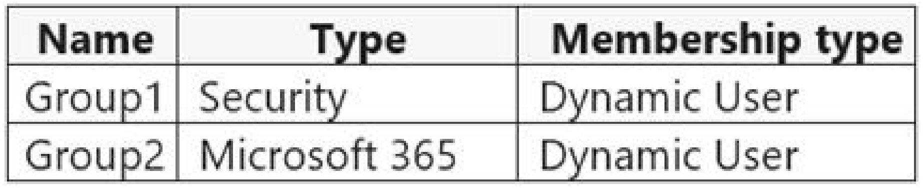
Name	Type	Resource group	Location
RG1	Resource group	**Not applicable**	West US
Managed1	Managed identity	RG1	West US

The subscription is linked to an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.



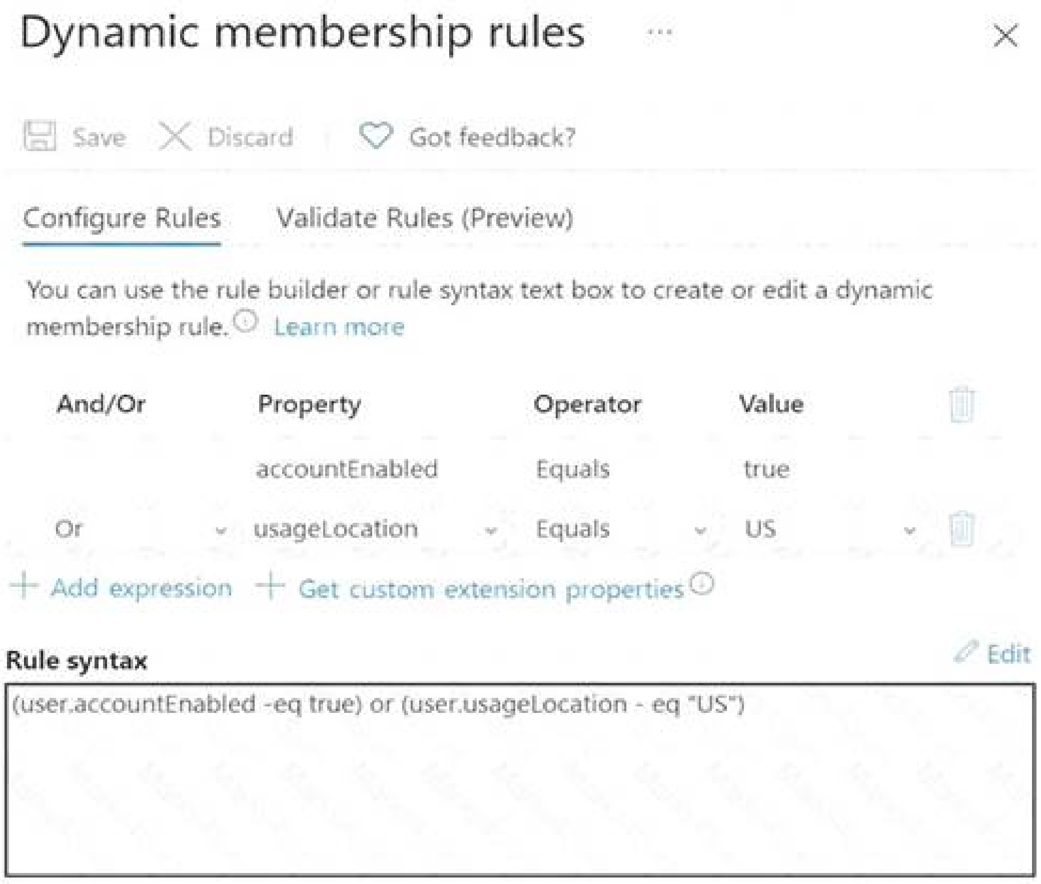
Name	Usage location
User1	United States
User2	Germany

You create the groups shown in the following table.



Name	Type	Membership type
Group1	Security	Dynamic User
Group2	Microsoft 365	Dynamic User

The membership rules for Group1 and Group2 are configured as shown in the following exhibit.



Dynamic membership rules ···

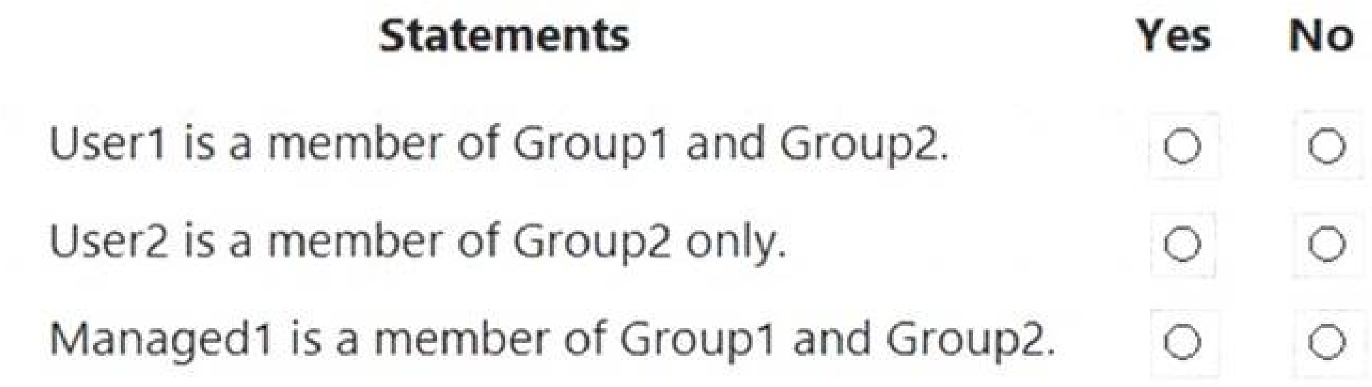
You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. Learn more

And/Or	Property	Operator	Value
	accountEnabled	Equals	true
Or	usageLocation	Equals	US

Rule syntax

```
(user.accountEnabled -eq true) or (user.usageLocation - eq "US")
```

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



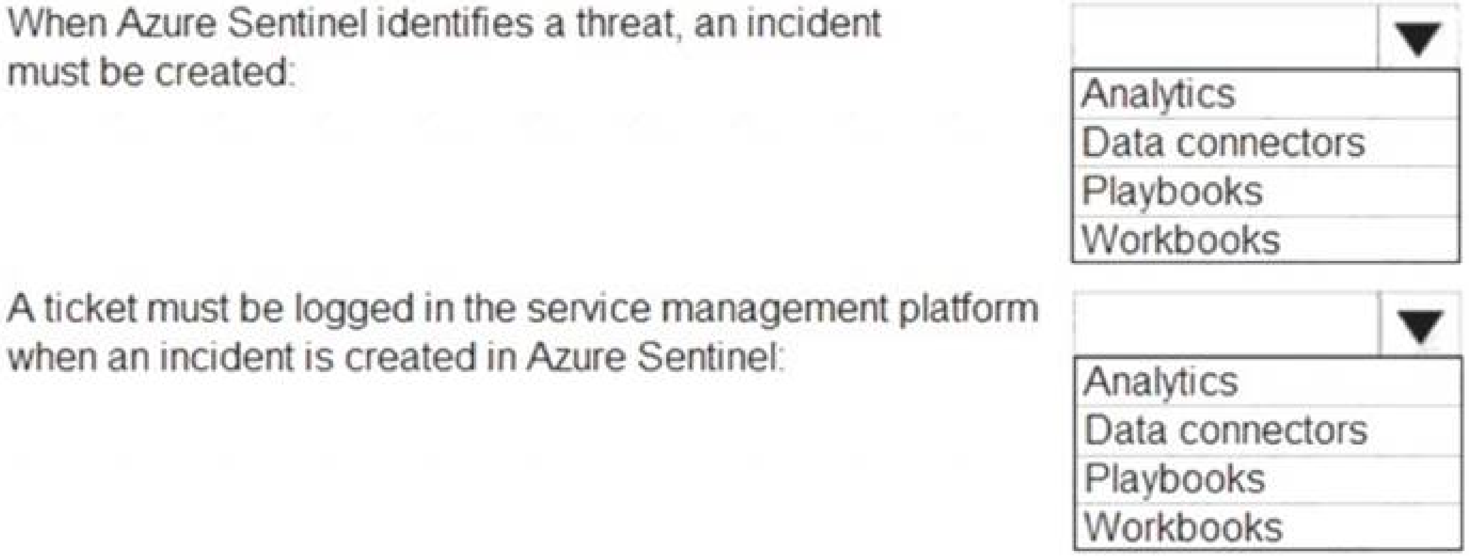
Statements	Yes	No
User1 is a member of Group1 and Group2.	○	○
User2 is a member of Group2 only.	○	○
Managed1 is a member of Group1 and Group2.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Text Description automatically generated
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership

NEW QUESTION 276
- (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

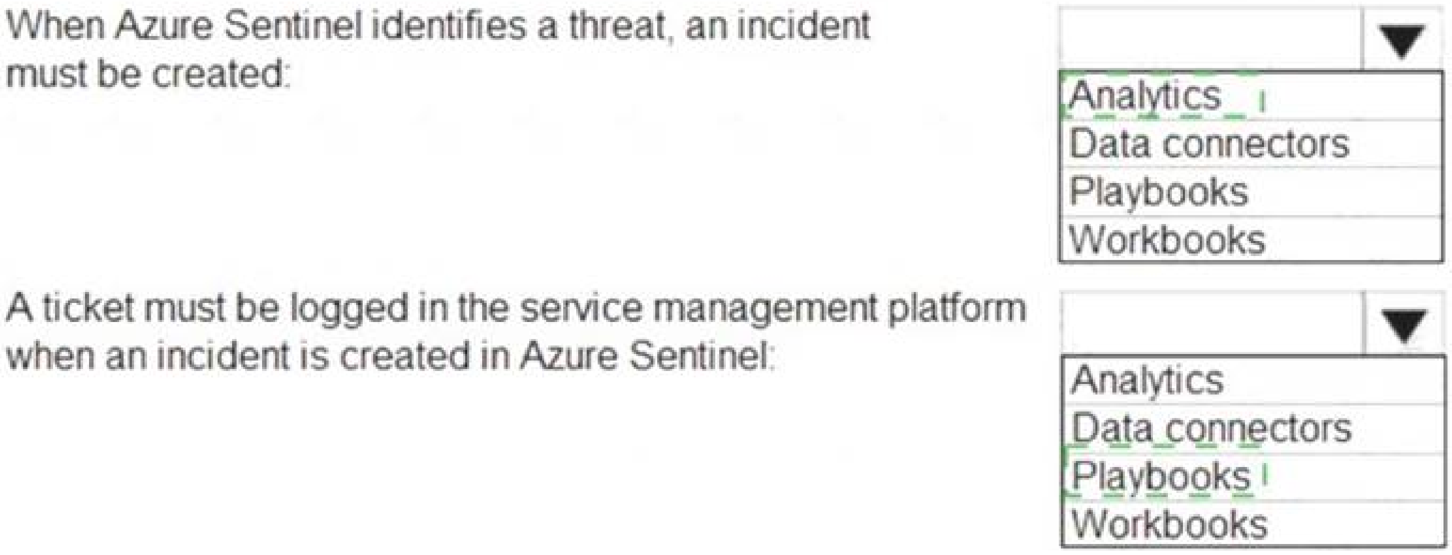
A ticket must be logged in the service management platform when an incident is created in Azure Sentinel:

- 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:

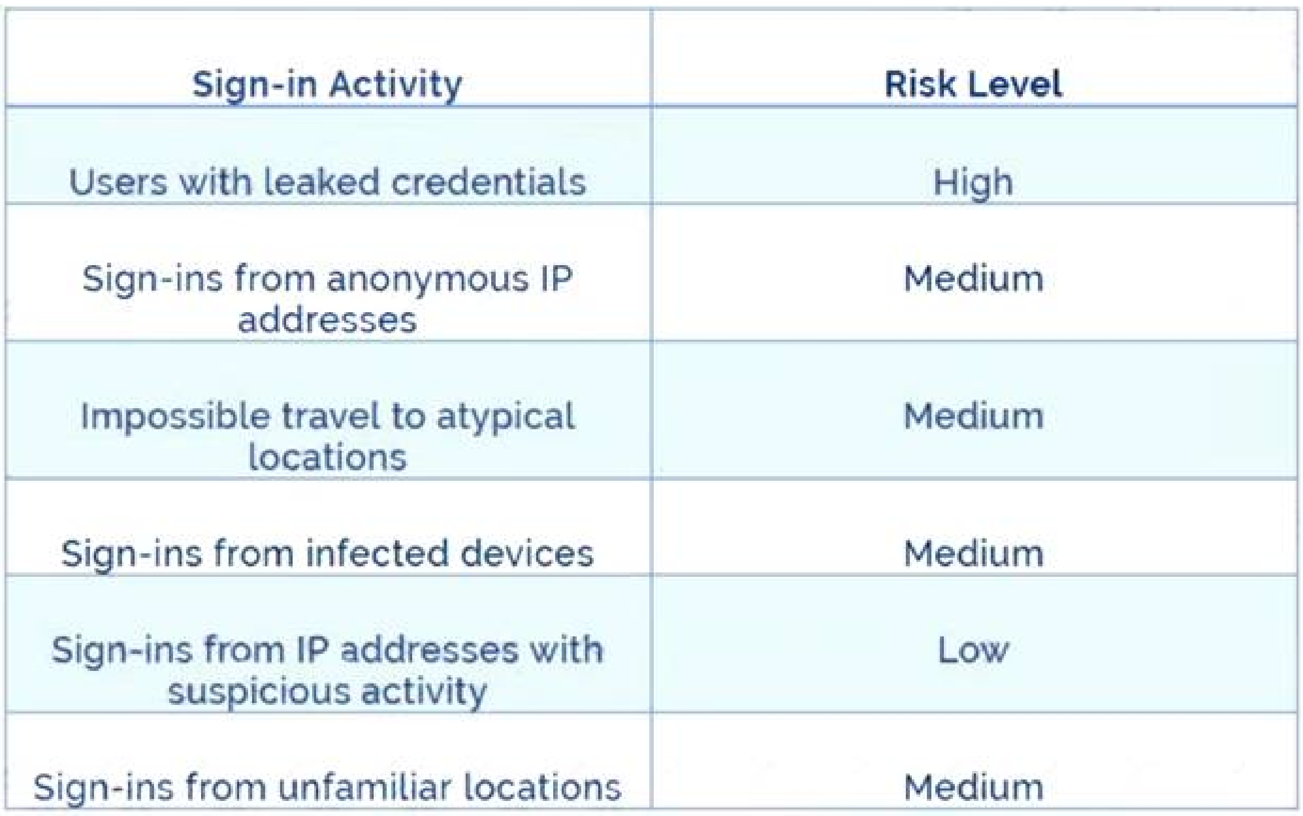
- Analytics
- Data connectors
- Playbooks
- Workbooks

NEW QUESTION 281
- (Exam Topic 4)
You have been tasked with applying conditional access policies for your company’s current Azure Active Directory (Azure AD).
The process involves assessing the risk events and risk levels.
Which of the following is the risk level that should be configured for users that have leaked credentials?

A. None
B. Low
C. Medium
D. High

Answer: D

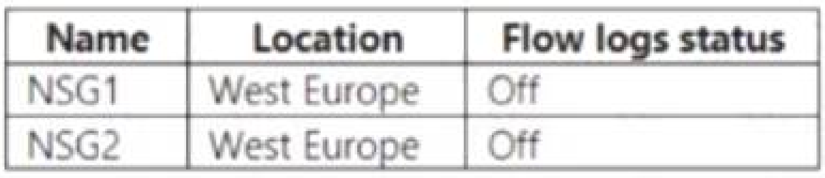
Explanation:
These six types of events are categorized in to 3 levels of risks – High, Medium & Low:
Table Description automatically generated



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

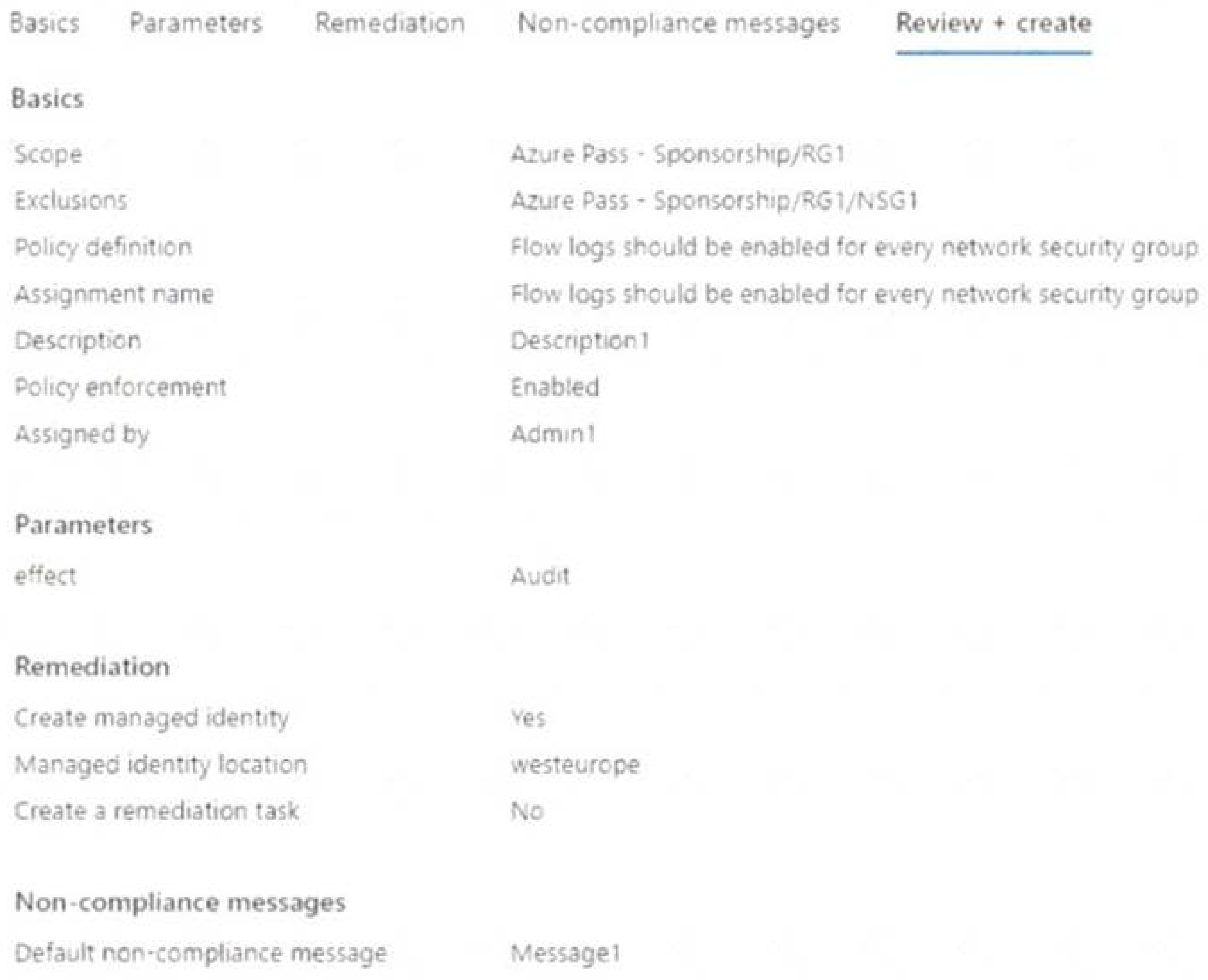
Reference:
http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/

NEW QUESTION 286
- (Exam Topic 4)
You have an Azure subscription that contains a resource group named RG1 and the network security groups (NSGs) shown in the following table.



Name	Location	Flow logs status
NSG1	West Europe	Off
NSG2	West Europe	Off

You create the Azure policy shown in the following exhibit.



Basics

Scope	Azure Pass - Sponsorship/RG1
Exclusions	Azure Pass - Sponsorship/RG1/NSG1
Policy definition	Flow logs should be enabled for every network security group
Assignment name	Flow logs should be enabled for every network security group
Description	Description1
Policy enforcement	Enabled
Assigned by	Admin1

Parameters

effect	Audit

Remediation

Create managed identity	Yes
Managed identity location	westeurope
Create a remediation task	No

Non-compliance messages

Default non-compliance message	Message1

You assign the policy to RG1.
What will occur if you assign the policy to NSG1 and NSG2?

A. Flow logs will be enabled for NSG1 and NSG2.
B. Flow logs will be enabled for NSG2 only.
C. Flow logs will be disabled for NSG1 and NSG2.
D. Flow logs will be enabled for NSG1 only.

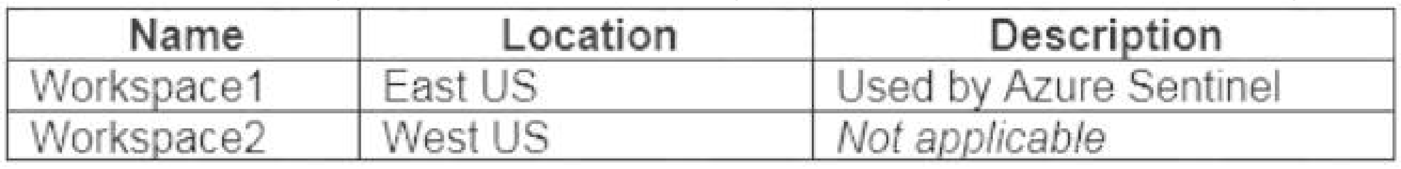
Answer: B

NEW QUESTION 291
- (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

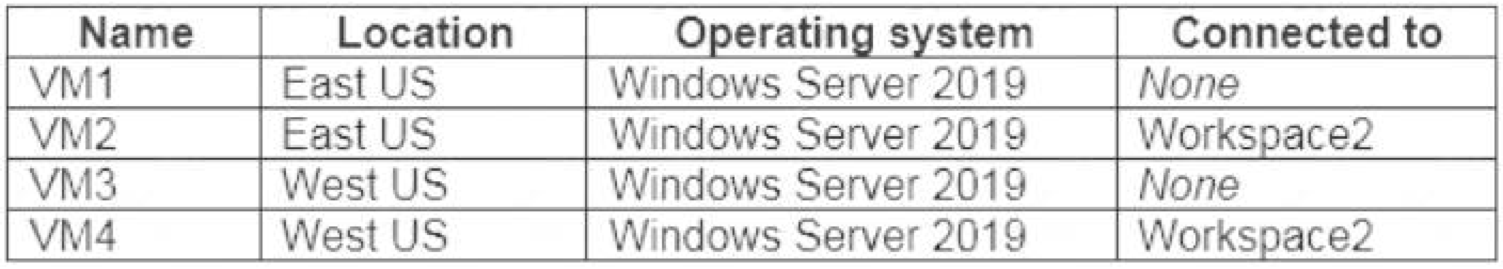
Answer: B

NEW QUESTION 296
- (Exam Topic 4)
You have an Azure subscription that contains the Azure Log Analytics workspaces shown in the following table.



Name	Location	Description
Workspace1	East US	Used by Azure Sentinel
Workspace2	West US	*Not applicable*

You create the virtual machines shown in the following table.



Name	Location	Operating system	Connected to
VM1	East US	Windows Server 2019	*None*
VM2	East US	Windows Server 2019	Workspace2
VM3	West US	Windows Server 2019	*None*
VM4	West US	Windows Server 2019	Workspace2

You plan to use Azure Sentinel to monitor Windows Defender Firewall on the virtual machines. Which virtual machines you can connect to Azure Sentinel?

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

Answer: D

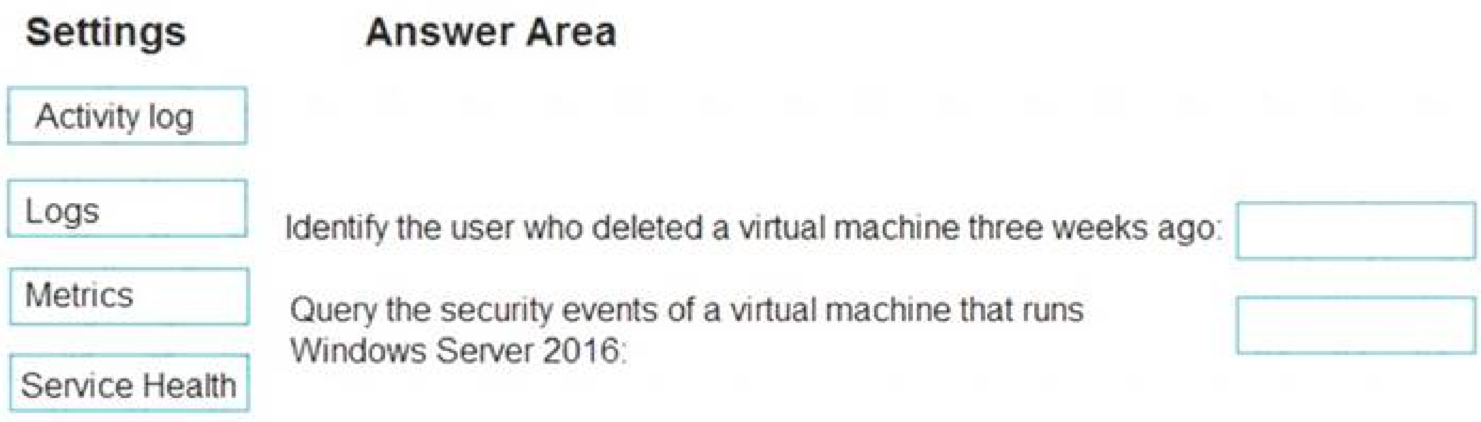
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-windows-firewall

NEW QUESTION 299
- (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 304
- (Exam Topic 4)
You have an Azure subscription.
You create a new virtual network named VNet1.
You plan to deploy an Azure web app named App1 that will use VNet1 and will be reachable by using private IP addresses. The solution must support inbound and outbound network traffic.
What should you do?

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

Answer: D

NEW QUESTION 306
- (Exam Topic 4)
Your company plans to create separate subscriptions for each department. Each subscription will be associated to the same Azure Active Directory (Azure AD) tenant.
You need to configure each subscription to have the same role assignments. What should you use?

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

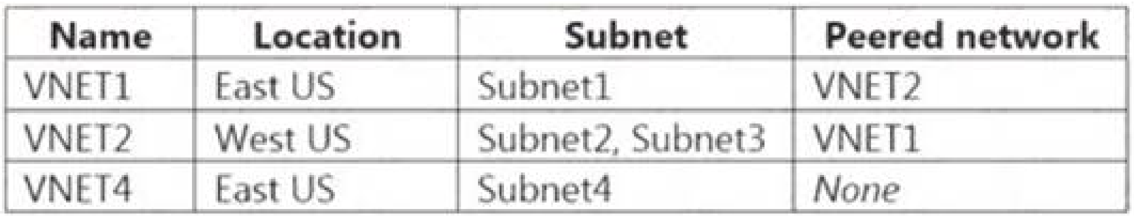
Answer: D

Explanation:
Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of
Azure resources that implements and adheres to an organization's standards, patterns, and requirements.
Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

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

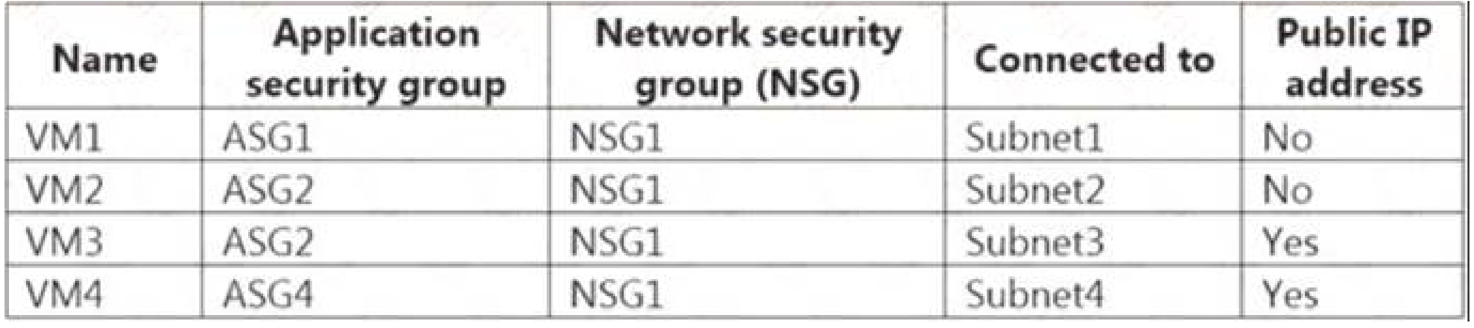
Reference:
https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

NEW QUESTION 309
- (Exam Topic 4)
You have the Azure virtual networks shown in the following table.



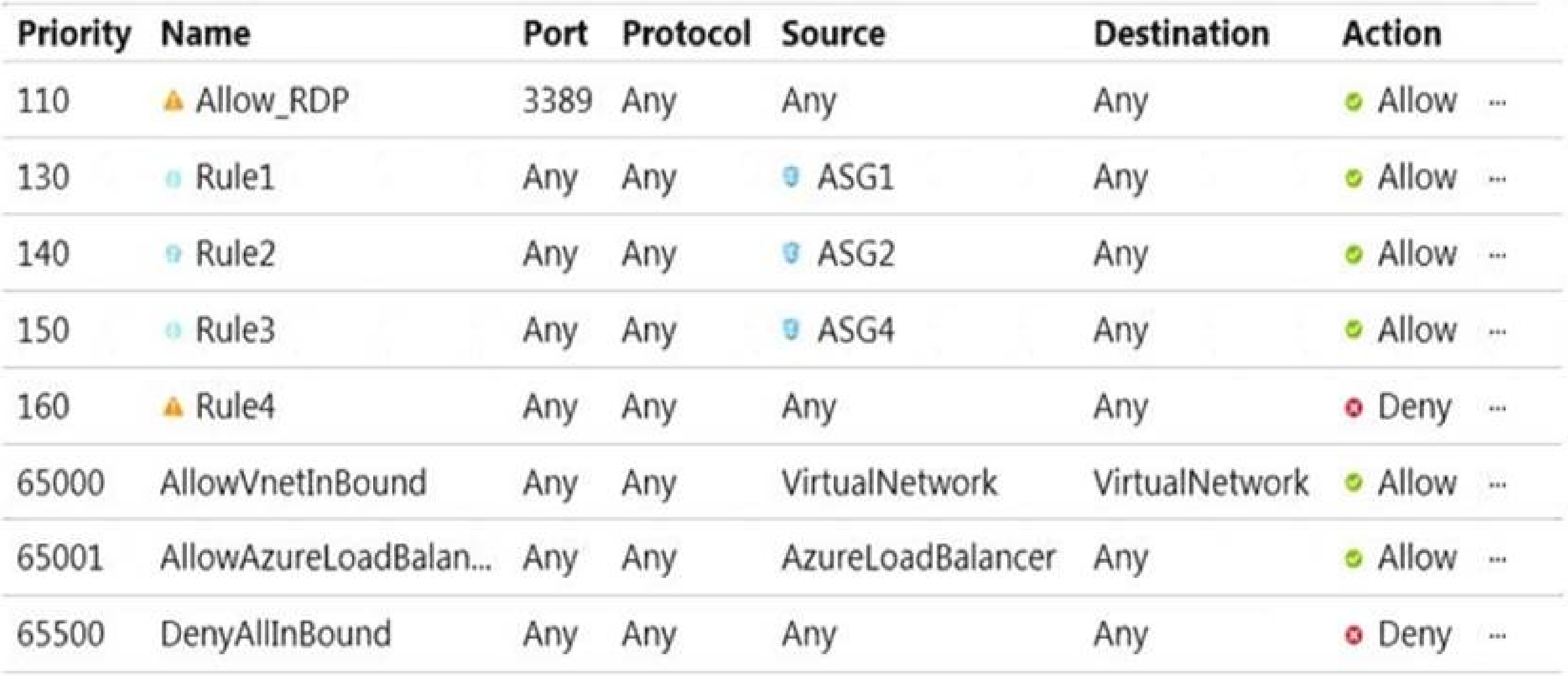
Name	Location	Subnet	Peered network
VNET1	East US	Subnet1	VNET2
VNET2	West US	Subnet2, Subnet3	VNET1
VNET4	East US	Subnet4	*None*

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



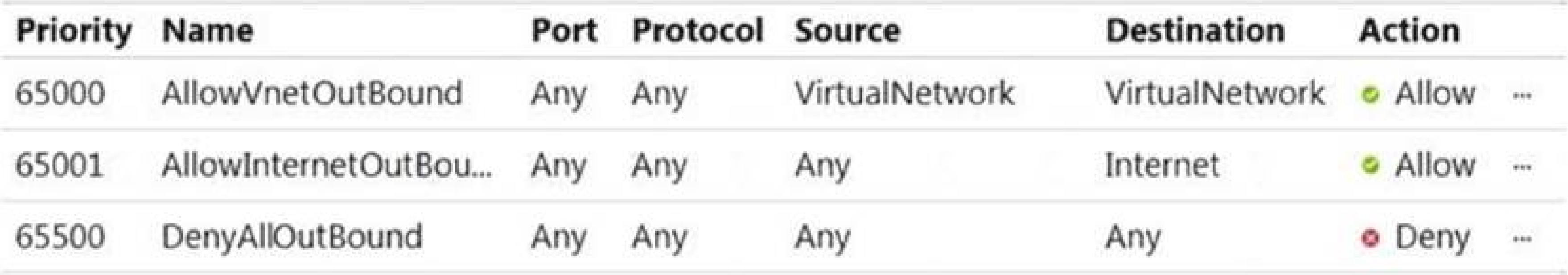
Name	Application security group	Network security group (NSG)	Connected to	Public IP address
VM1	ASG1	NSG1	Subnet1	No
VM2	ASG2	NSG1	Subnet2	No
VM3	ASG2	NSG1	Subnet3	Yes
VM4	ASG4	NSG1	Subnet4	Yes

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



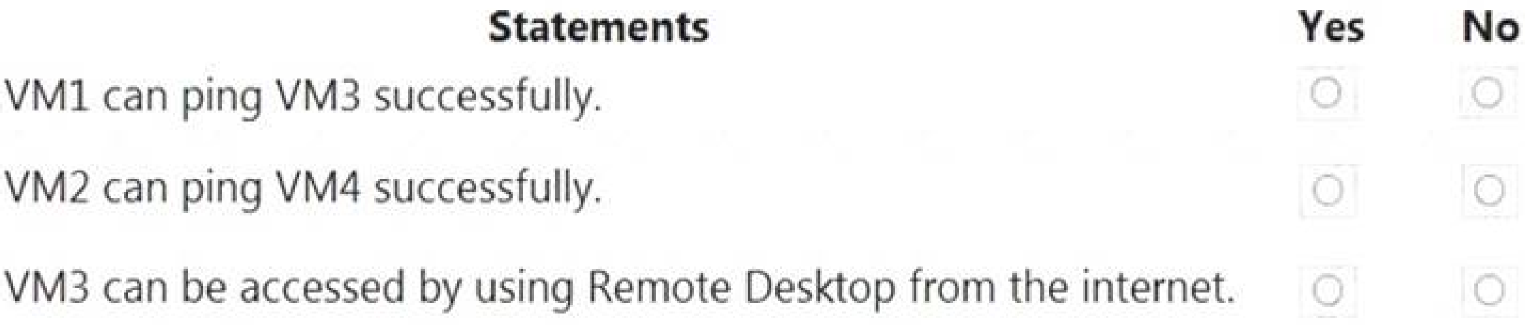
Priority	Name	Port	Protocol	Source	Destination	Action
110	Allow_RDP	3389	Any	Any	Any	Allow ...
130	Rule1	Any	Any	ASG1	Any	Allow ...
140	Rule2	Any	Any	ASG2	Any	Allow ...
150	Rule3	Any	Any	ASG4	Any	Allow ...
160	Rule4	Any	Any	Any	Any	Deny ...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork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

Outbound security rules



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

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



Statements	Yes	No
VM1 can ping VM3 successfully.	○	○
VM2 can ping VM4 successfully.	○	○
VM3 can be accessed by using Remote Desktop from the internet.	○	○

A. Mastered
B. Not Mastered

Answer: A

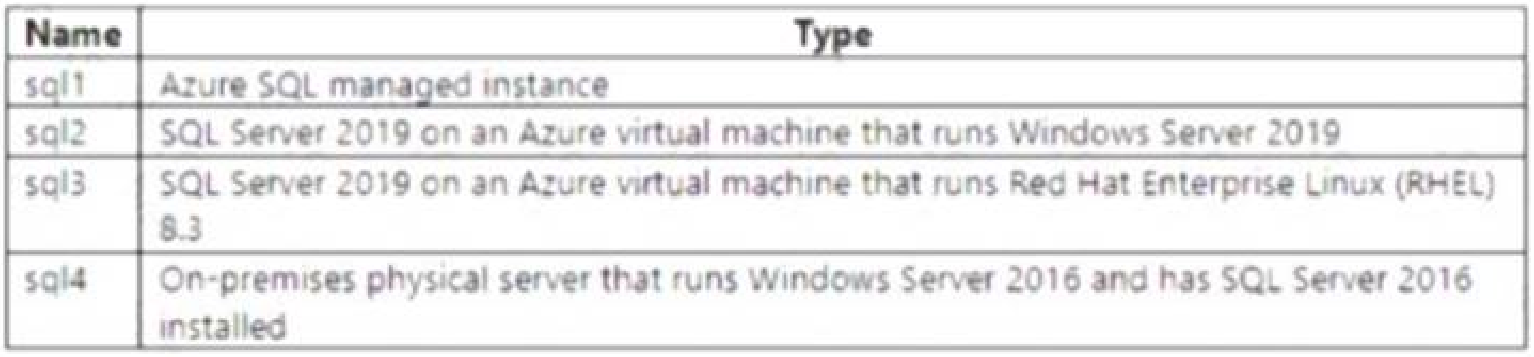
Explanation:
Box 1: Yes
VM1 and VM3 are on peered VNets. The firewall rules with a source of ASG1 and ASG2 allow ‘any’ traffic on ‘any’ protocol so pings are allowed between VM1 and VM3.
Box 2: No
VM2 and VM4 are on separate VNets and the VNets are not peered. Therefore, the pings would have to go over the Internet. VM4 does have a public IP and the firewall allows pings. However, for VM2 to be able to ping VM4, VM2 would also need a public IP address. In Azure, pings don’t go out through the default gateway as they would in a physical network. For an Azure VM to ping external IPs, the VM must have a public IP address assigned to it.
Box 3: Yes
VM3 has a public IP address and the firewall allows traffic on port 3389.

NEW QUESTION 314
- (Exam Topic 4)
You have an Azure subscription that contains an Azure Blob storage account bolb1. You need to configure attribute-based access control (ABAC) for blob1.
Which attributes can you use in access conditions?

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

Answer: A

NEW QUESTION 317
- (Exam Topic 4)
You have an on-premises network and an Azure subscription.
You have the Microsoft SQL Server instances shown in the following table.



Name	Type
sql1	Azure SQL managed instance
sql2	SQL Server 2019 on an Azure virtual machine that runs Windows Server 2019
sql3	SQL Server 2019 on an Azure virtual machine that runs Red Hat Enterprise Linux (RHEL) 8.3
sql4	On-premises physical server that runs Windows Server 2016 and has SQL Server 2016 installed

You plan to implement Microsoft Defender for SQL.
Which SQL Server instances will be protected by Microsoft Defender for SQL?

A. sql1 and sql2 only
B. sql1, sql2, andsql3 only
C. sql1 sql2 and so.14 only
D. sql1, sql2, sql3, and sql4

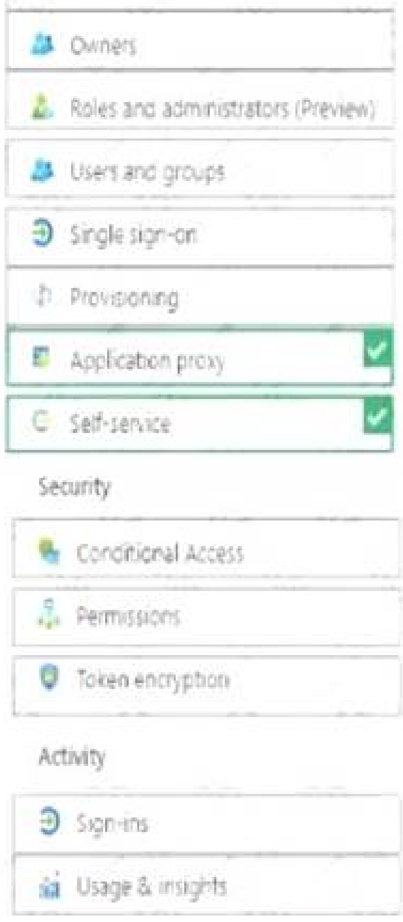
Answer: D

NEW QUESTION 322
- (Exam Topic 4)
You have an Azure subscription that uses Microsoft Sentinel.
You need to create a Microsoft Sentinel notebook that will use the Guided Investigation - Anomaly Lookup template.
What should you create first?

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

Answer: A

NEW QUESTION 326
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains two users named User1 and User2 and a registered app named App1.
You create an app-specific role named Role1.
You need to assign Role1 to User1 and enable User2 to request access to App1.
Which two settings should you modify? To answer select the appropriate settings in the answer area NOTE: Each correct selection is worth one pant.



Owners
Roles and administrators (Preview)
Users and groups
Single sign-on
Provisioning
Application proxy ☑
Self-service ☑
Security
Conditional Access
Permissions
Token encryption
Activity
Sign-ins
Usage & insights

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, application Description automatically generated

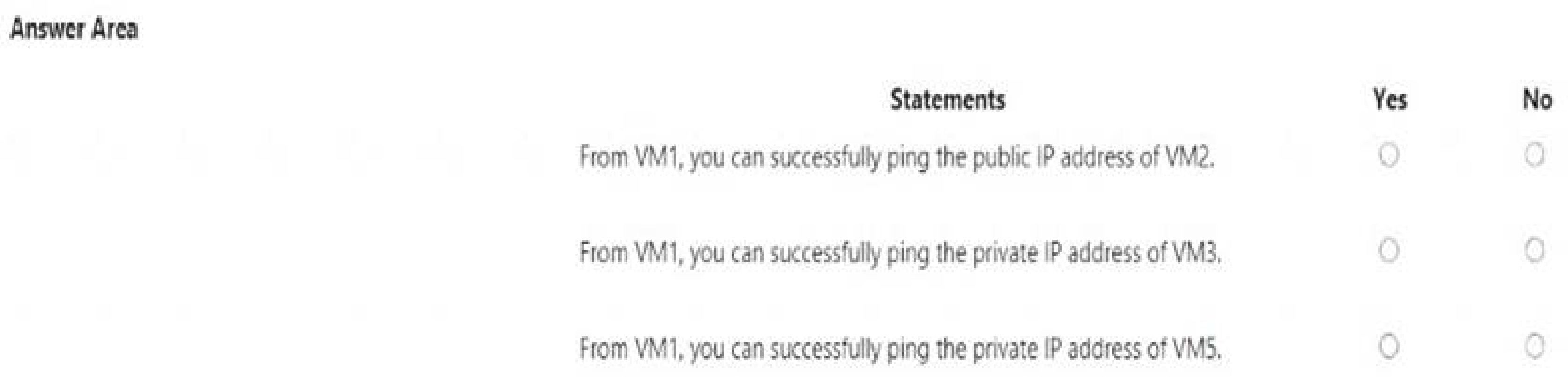
NEW QUESTION 331
- (Exam Topic 4)
You have an Azure AD tenant that contains 500 users and an administrative unit named AU1.

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

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

Answer: E

NEW QUESTION 336
- (Exam Topic 4)
You are evaluating the security of the network communication between the virtual machines in Sub2. For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
From VM1, you can successfully ping the public IP address of VM2.	○	○
From VM1, you can successfully ping the private IP address of VM3.	○	○
From VM1, you can successfully ping the private IP address of VM5.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Q1: No { and it should not be allowed as only TCP 80 is allowed from the "Internet" service tag
Q2: Yes {as it should be for VMs in the same local subnet pinging each other on private IP and no NSG configured}
Q3: Yes {VM5 is in subnet where 1st rule of NSG allows any traffic from any source to the destination}

NEW QUESTION 340
- (Exam Topic 3)
From Azure Security Center, you need to deploy SecPol1. What should you do first?

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

Answer: C

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

NEW QUESTION 341
......