Microsoft

Exam Questions az-500

Microsoft Azure Security Technologies

NEW QUESTION 1
- (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

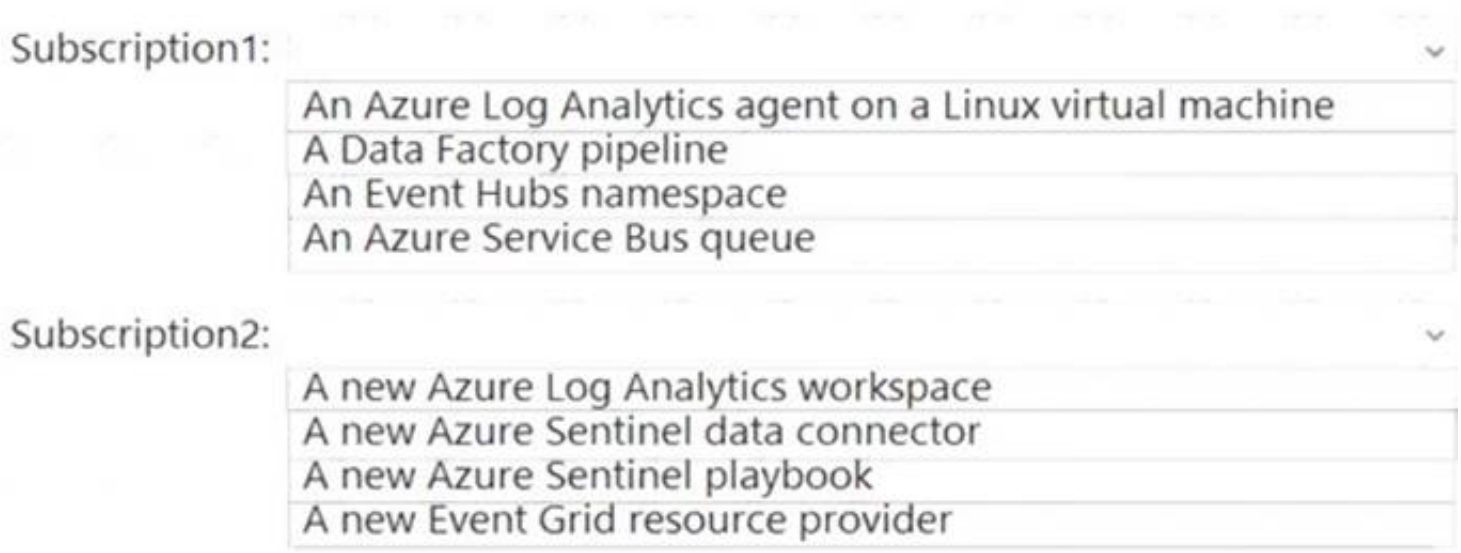
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-subscriptions-associ

NEW QUESTION 2
- (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.



A. Mastered
B. Not Mastered

Answer: A

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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Create and register an Azure AD application. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to specify a name, such as SQLServerCTP1, and select the supported account types, such as Accounts in this organization directory only.
Grant application permissions. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to assign the Directory.Read.All permission to the application and grant admin consent for your organization.
Create and assign a certificate. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to create a self-signed certificate and

upload it to the application. You also need to store the certificate in Azure Key Vault and grant access policies to the application and your SQL Server.
Configure Azure AD authentication for SQL Server through Azure portal. You can use the Azure portal to do
this. You need to select your SQL Server resource and enable Azure AD authentication. You also need to select your Azure AD application as the Azure AD admin for your SQL Server.
Create logins and users. You can use SSMS or Transact-SQL to do this. You need to connect to your SQL Server as the Azure AD admin and create a login for Danny-31330471. You also need to create a user for Danny-31330471 in each database that he needs access to.
Connect with a supported authentication method. You can use SSMS or SqlClient to do this. You need to specify the Authentication connection property in the connection string as Active Directory Password or Active Directory Integrated. You also need to provide the username and password of Danny-31330471.

NEW QUESTION 4
- (Exam Topic 4)
You have an Azure web app named WebApp1. You upload a certificate to WebApp1.
You need to make the certificate accessible to the app code of WebApp1. What should you do?

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

Answer: B

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

NEW QUESTION 5
- (Exam Topic 4)
You have an Azure subscription that contains the virtual machines shown in the following table.
Subnet1 and Subnet2 have a network security group {NSG). The NSG has an outbound rule that has the following configurations:
• Port; Any
• Source: Any
• Priority: 100
• Action: Deny
• Protocol: Any
• Destination: Storage
The subscription contains a storage account named storage1.
You create a private endpoint named Private1 that has the following settings:
• Resource type: Microsoft.Storage/storageAccounts
• Resource: storage1
• Target sub-resource: blob
• Virtual network: VNet1
• Subnet: Subnet1
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.
Answer Area

Statements	Yes	No
From VM2, you can create a container in storage1.	○	○
From VM1, you can upload data to the blob storage of storage1.	○	○
From VM2, you can upload data to the blob storage of storage1.	○	○

A. Mastered
B. Not Mastered

Answer: A

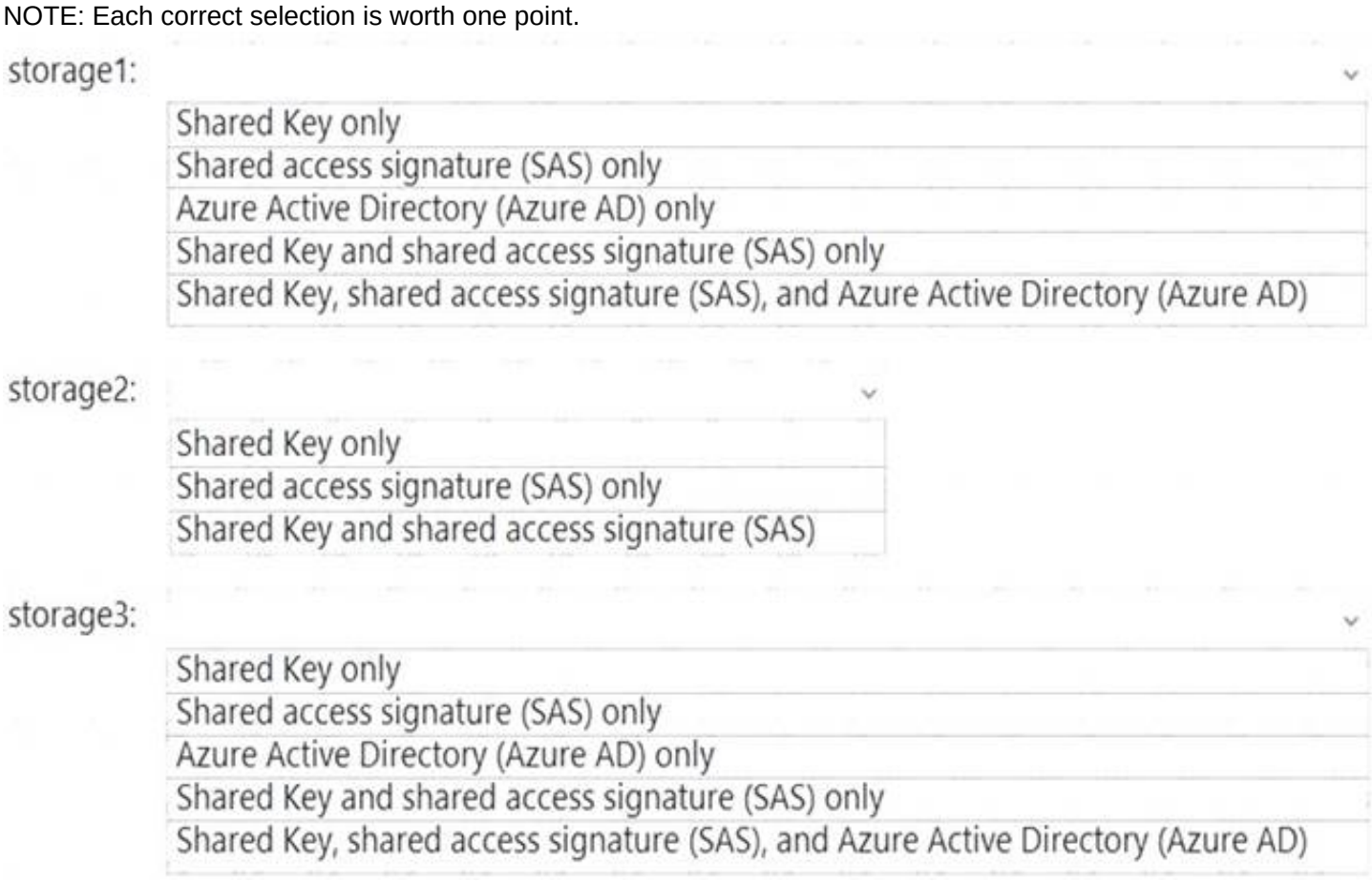
Explanation:
Answer Area

Statements	Yes	No
From VM2, you can create a container in storage1.	○	○
From VM1, you can upload data to the blob storage of storage1.	○	○
From VM2, you can upload data to the blob storage of storage1.	○	○

NEW QUESTION 6
- (Exam Topic 4)
You have an Azure subscription that contains the storage accounts shown in the following table.

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

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



A. Mastered
B. Not Mastered

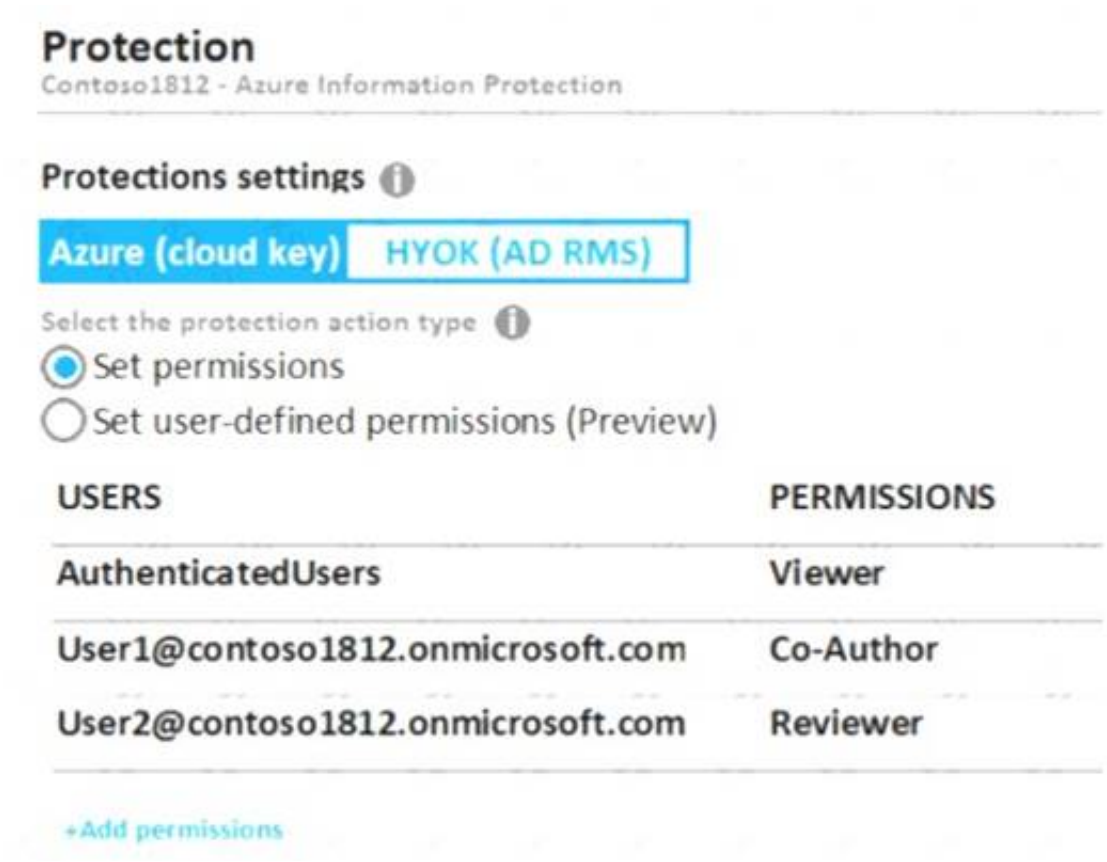
Answer: A

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

NEW QUESTION 7
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant named contoso1812.onmicrosoft.com that contains the users shown in the following table.

Name	Username	Type
User1	User1@contoso1812.onmicrosoft.com	Member
User2	User2@contoso1812.onmicrosoft.com	Member
User3	User3@contoso1812.onmicrosoft.com	Member
User4	User4@outlook.com	Guest

You create an Azure Information Protection label named Label1. The Protection settings for Label1 are configured as shown in the exhibit. (Click the Exhibit tab.)

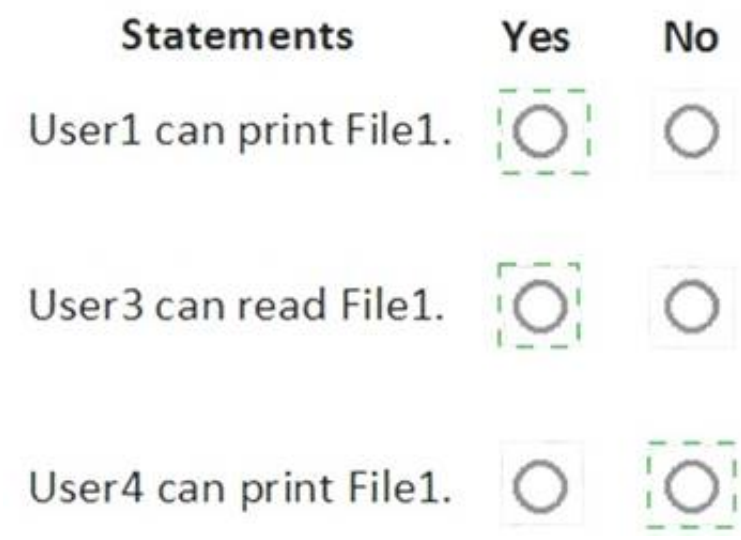


Label1 is applied to a file named File1.
For each of the following statements, select Yes if the statement is true, Otherwise, select No. NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

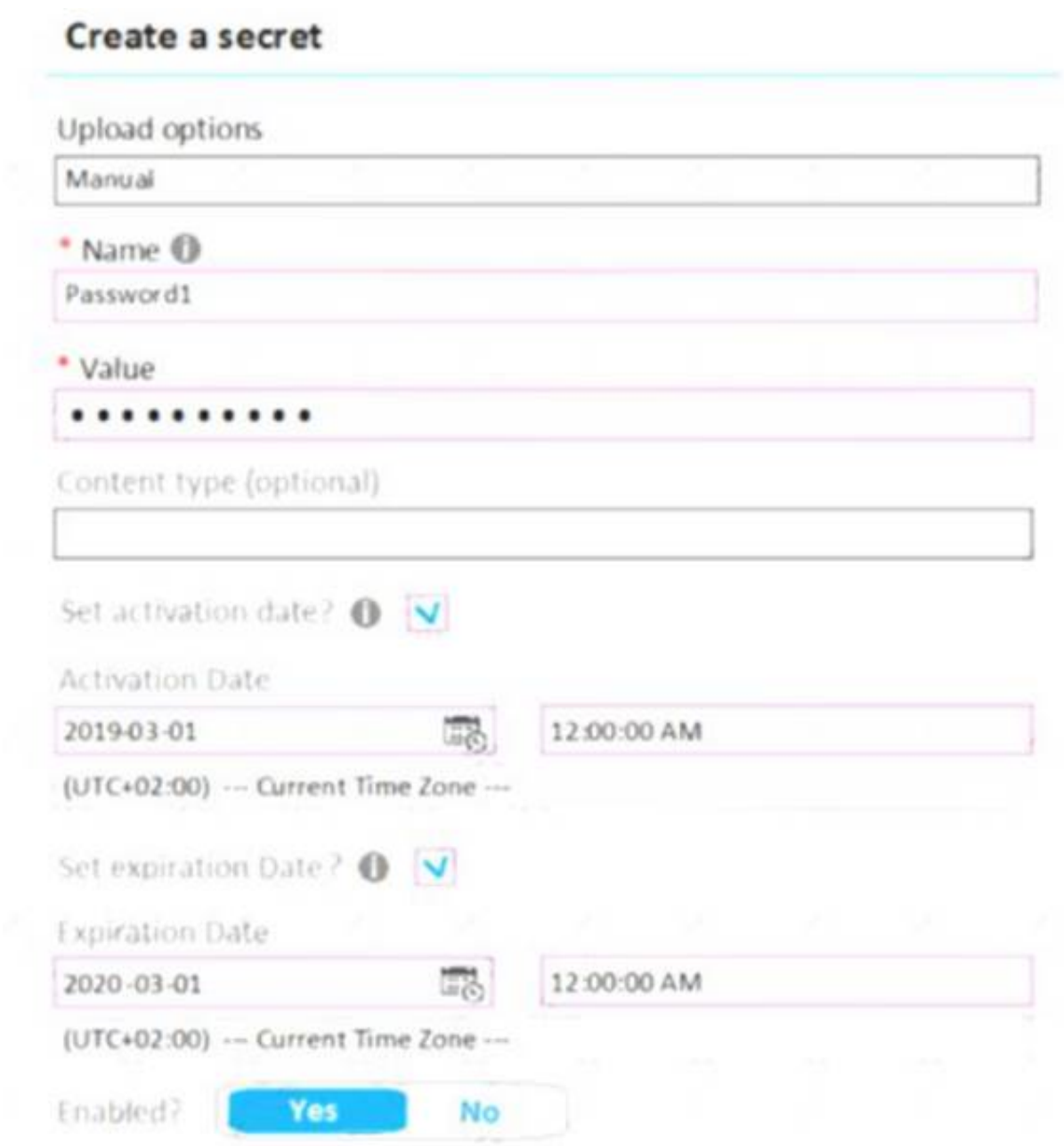
Explanation:



NEW QUESTION 8
- (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.)



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 9
- (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 10
- (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 subscription that contains four Azure SQL managed instances.
You need to evaluate the vulnerability of the managed instances to SQL injection attacks. What should you do first?

A. Create an Azure Sentinel workspace.

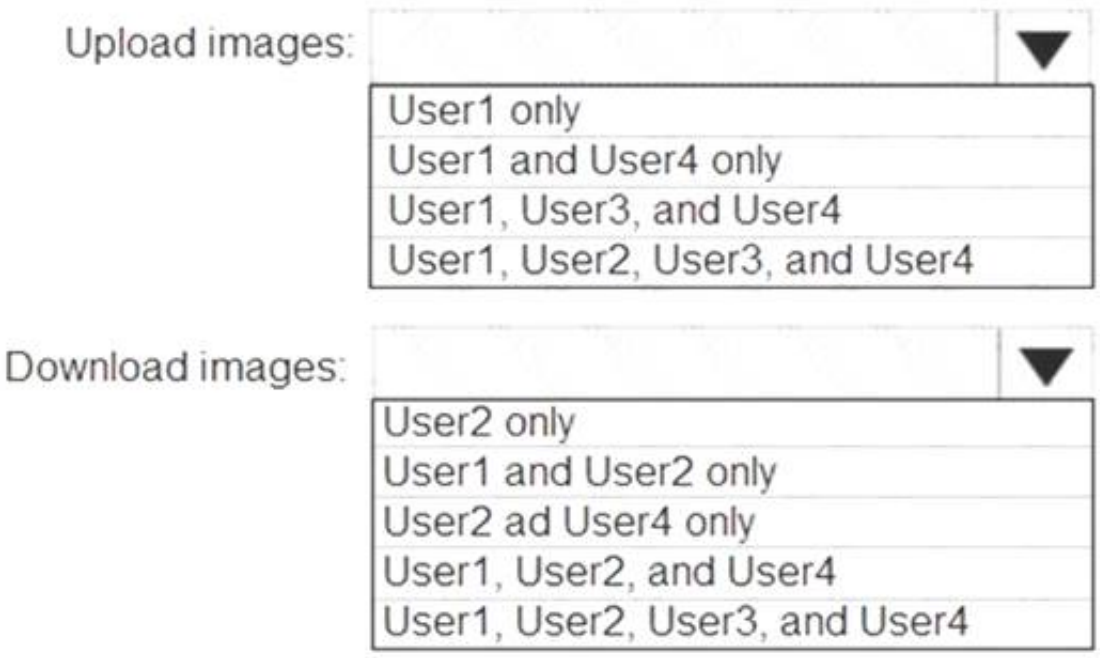
B. Enable Advanced Data Security.
C. Add the SQL Health Check solution to Azure Monitor.
D. Create an Azure Advanced Threat Protection (ATP) instance.

Answer: B

NEW QUESTION 13
- (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

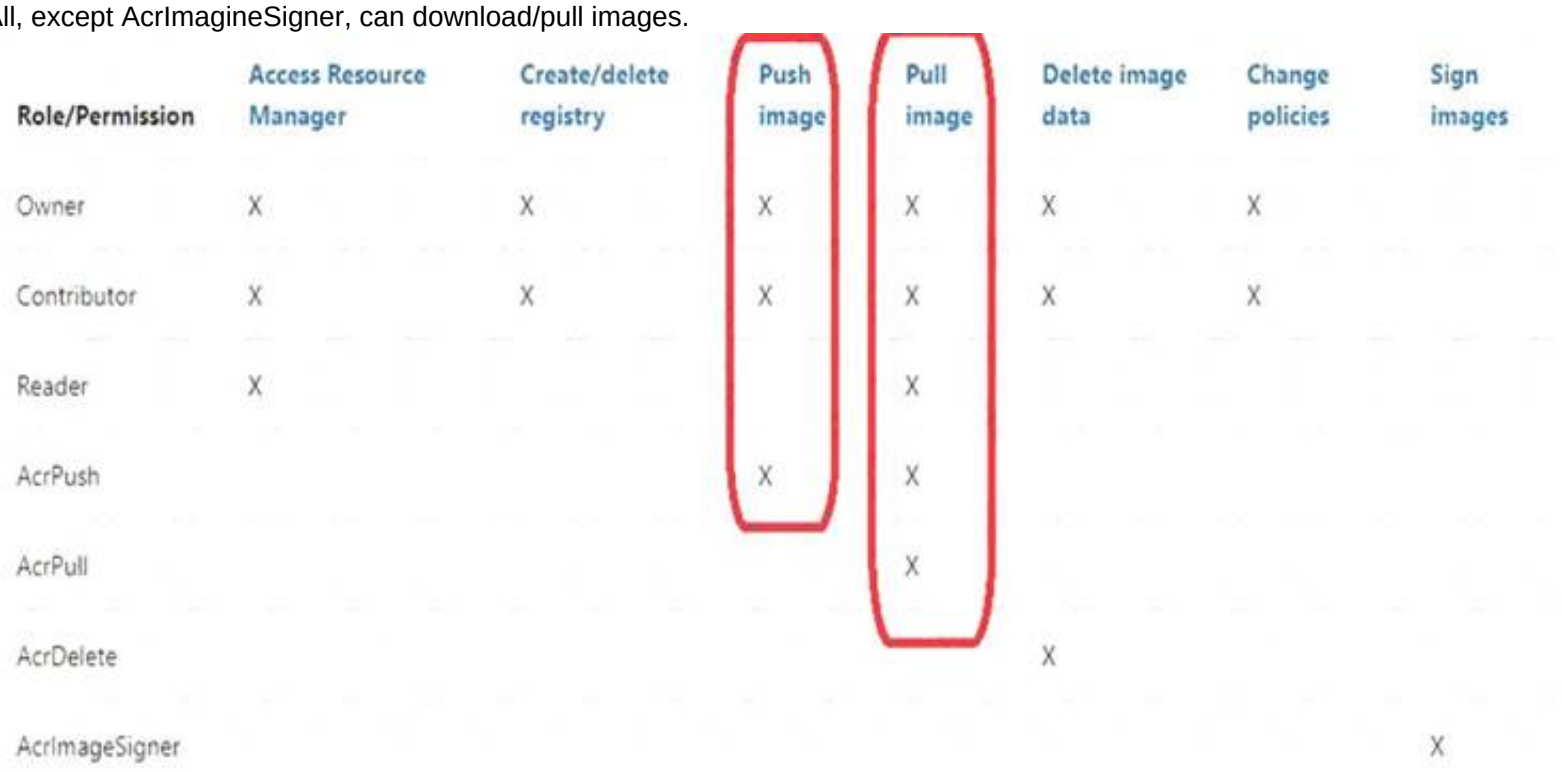
Which users can upload images to Registry1 and download images from Registry1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



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 18
- (Exam Topic 4)
You have an Azure Active Din-dory (Azure AD) tenant named contoso.com that contains a user named User1. You plan to publish several apps in the tenant.
You need to ensure that User1 can grant admin consent for the published apps.
Which two possible user roles can you assign to User! to achieve this goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

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

Answer: CE

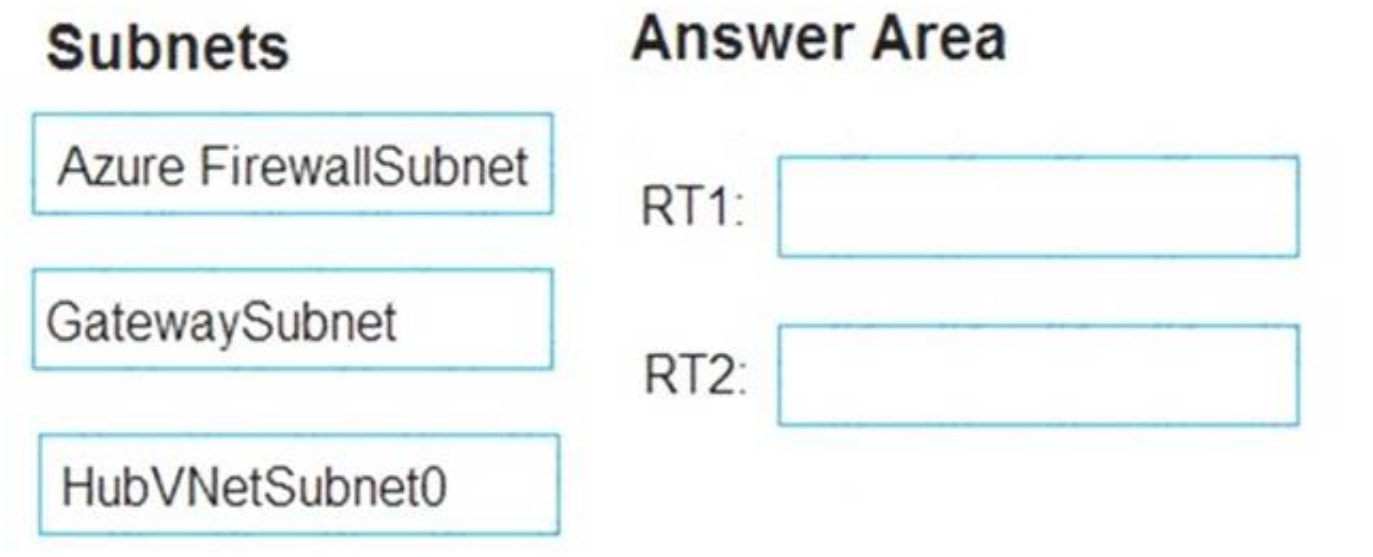
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent

NEW QUESTION 21
- (Exam Topic 4)
You have an Azure subscription that contains the virtual networks shown in the following table.

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

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

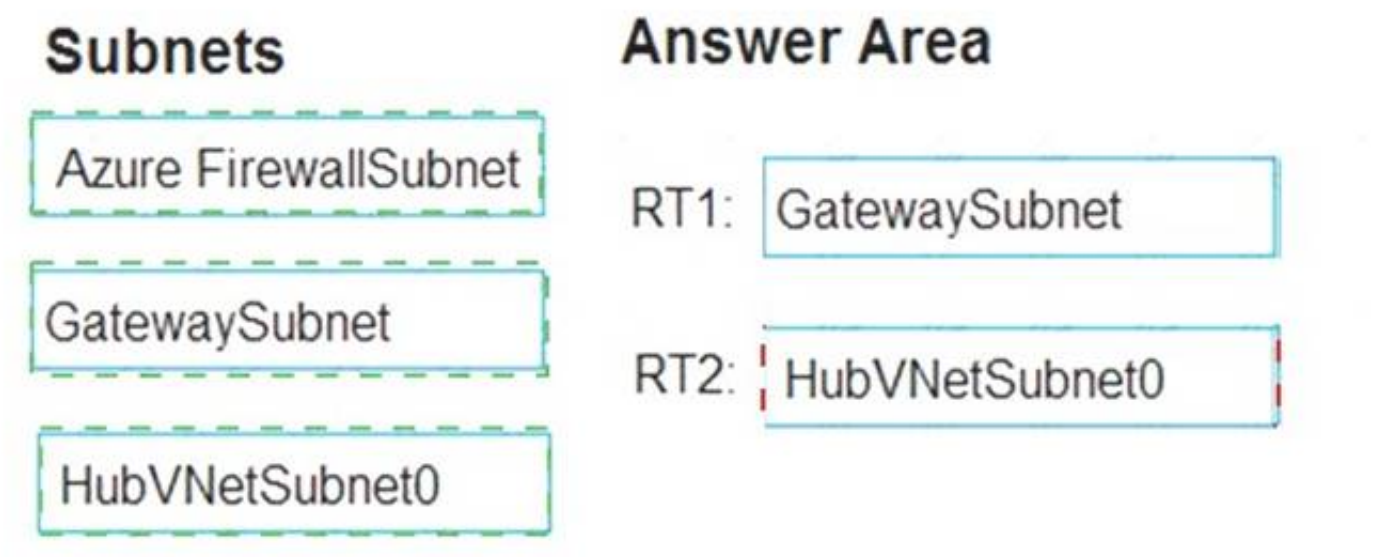
You need to ensure that traffic between SpokeVNetSubnet0 and the on-premises network flows through the Azure firewall.
To which subnet should you associate each route table? To answer, drag the appropriate subnets to the correct route tables. Each subnet may be used once, more than once, or not at all.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



A. Mastered
B. Not Mastered

Answer: A

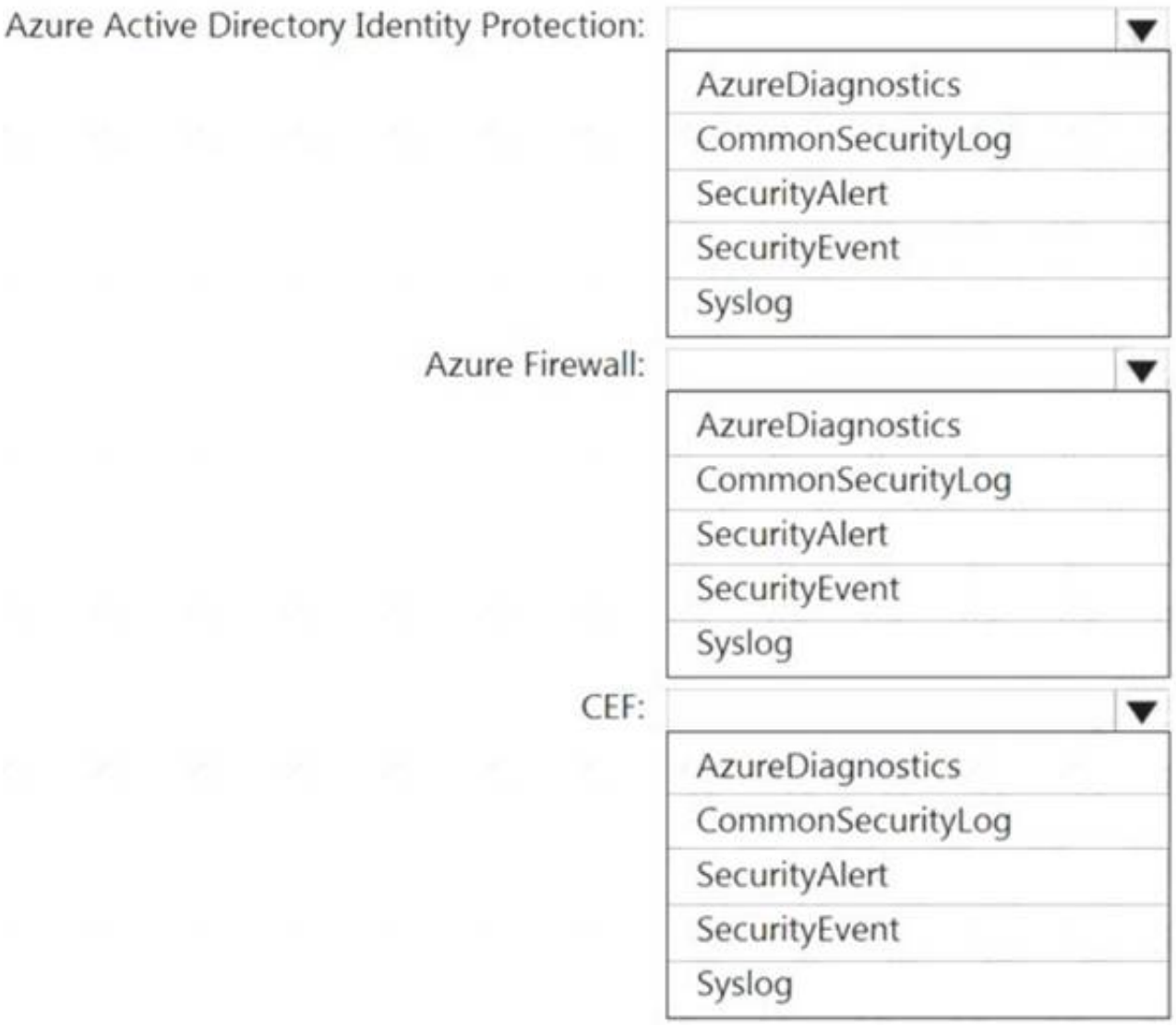
Explanation:



NEW QUESTION 26
- (Exam Topic 4)
You have an Azure Sentinel workspace that has the following data connectors:

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

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



A. Mastered
B. Not Mastered

Answer: A

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

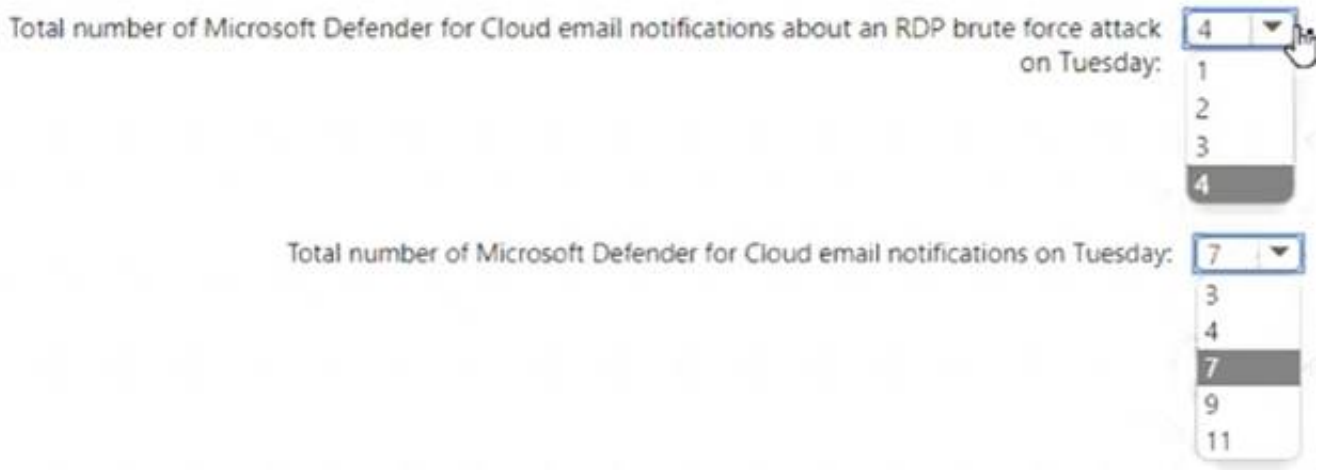
NEW QUESTION 27
- (Exam Topic 4)
On Monday, you configure an email notification in Microsoft Defender for Cloud to notify user1 @contoso.com about alerts that have a severity level of Low, Medium, or High. On Tuesday, Microsoft Defender for Cloud generates the security alerts shown in the following table.

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

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

selection is worth one point.

Answer Area

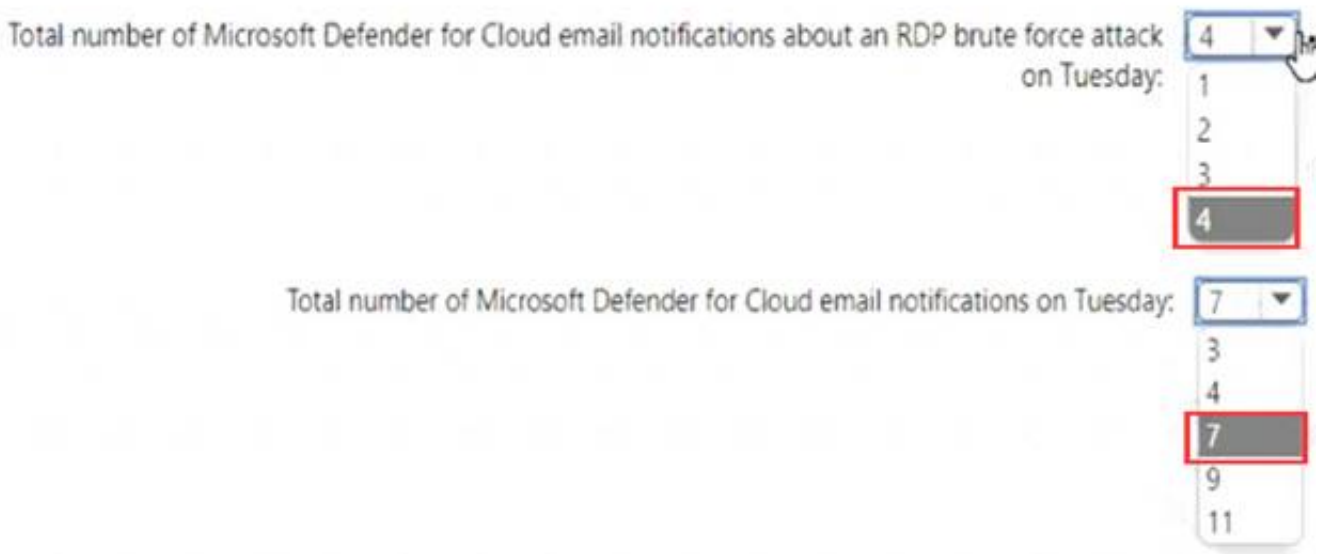


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 29
- (Exam Topic 4)
You have an Azure subscription.
You plan to create a custom role-based access control (RBAC) role that will provide permission to read the Azure Storage account.
Which property of the RBAC role definition should you configure?

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

Answer: D

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

NEW QUESTION 32
- (Exam Topic 4)
Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
Your company has an Active Directory forest with a single domain, named weylandindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.
You have been tasked with integrating Active Directory and the Azure AD tenant. You intend to deploy Azure AD Connect.
Your strategy for the integration must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.
Solution: You recommend the use of password hash synchronization and seamless SSO. Does the solution meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 33
- (Exam Topic 4)
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 35
- (Exam Topic 4)
You have an Azure subscription that contains an Azure key vault named Vault1. On January 1, 2019, Vault1 stores the following secrets.

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

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

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

Password1:
- Never
- Always
- Only after May 1, 2019

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

A. Mastered
B. Not Mastered

Answer: A

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

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

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

NEW QUESTION 38
- (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 42
- (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:

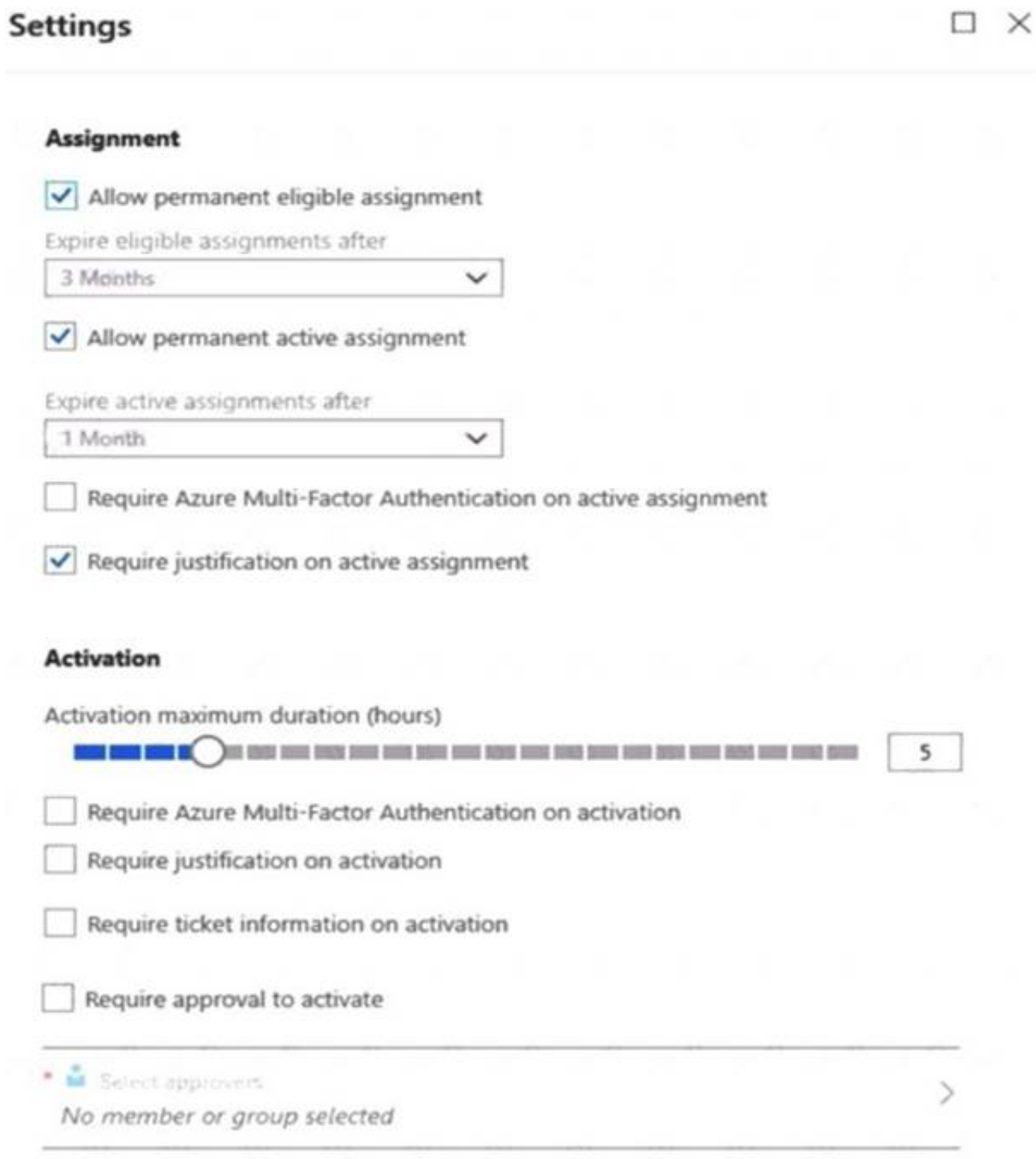
- Providing security recommendations for the virtual machines. Example recommendations include: app system updates, configure ACLs endpoints, enable antimalware, enable network security groups, and apply disk encryption.
- Monitoring the state of your virtual machines.

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

NEW QUESTION 45
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

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



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

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

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

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	○	○
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	○	○
User3 can activate the Security Administrator role.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Yes
Eligible Type: A role assignment that requires a user to perform one or more actions to use the role. If a user has been made eligible for a role, that means they can activate the role when they need to perform privileged tasks. There's no difference in the access given to someone with a permanent versus an eligible role assignment. The only difference is that some people don't need that access all the time.
You can choose from two assignment duration options for each assignment type (eligible and active) when you configure settings for a role. These options become the default maximum duration when a user is assigned to the role in Privileged Identity Management.
Use the Activation maximum duration slider to set the maximum time, in hours, that a role stays active before it expires. This value can be from one to 24 hours.
Box 2: Yes
Active Type: A role assignment that doesn't require a user to perform any action to use the role. Users assigned as active have the privileges assigned to the role
Box 3: Yes
User3 is member of Group2. Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure https://docs.microsoft.com/bs-cyrl-ba/azure/active-directory/privileged-identity-management/pim-resource-roles

NEW QUESTION 46
- (Exam Topic 4)
Lab Task
Task 6
You need to configure a Microsoft SQL server named Web3l 330471 only to accept connections from the Subnet0 subnet on the VNET01 virtual network.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Configure the firewall settings for the SQL server. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to add a firewall rule that allows inbound traffic from the IP address range of the Subnet0 subnet. You also need to disable the option to allow Azure services and resources to access this server.
Configure the network settings for the SQL server. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to enable service endpoints for SQL Server on the Subnet0 subnet. You also need to add a virtual network rule that links the SQL server to the Subnet0 subnet.
Configure the connection settings for the SQL server. You can use SQL Server Management Studio or Transact-SQL to do this. You need to enable remote server connections and specify a TCP port for listening. You also need to configure SQL Server Authentication or Azure Active Directory Authentication for connecting to the SQL server.

NEW QUESTION 49
- (Exam Topic 4)
You have an Azure subscription that contains the virtual machines shown in the following table.

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

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

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

On which virtual machines is the Log Analytics agent installed?

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

Answer: D

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

NEW QUESTION 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 57
- (Exam Topic 4)
You have three on-premises servers named Server1, Server2, and Server3 that run Windows Server1 and Server2 and located on the Internal network. Server3 is located on the premises network. All servers have access to Azure.
From Azure Sentinel, you install a Windows firewall data connector.
You need to collect Microsoft Defender Firewall data from the servers for Azure Sentinel. What should you do?

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

Answer: C

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

NEW QUESTION 59
- (Exam Topic 4)
Your network contains an Active Directory forest named contoso.com. The forest contains a single domain. You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD)
tenant named contoso.com.
You plan to deploy Azure AD Connect and to integrate Active Directory and the Azure AD tenant. You need to recommend an integration solution that meets the following requirements:
Ensures that password policies and user logon restrictions apply to user accounts that are synced to the Tenant Minimizes the number of servers required for the solution.
Which authentication method should you include in the recommendation?

A. federated identity with Active Directory Federation Services (AD FS)
B. password hash synchronization with seamless single sign-on (SSO)
C. pass-through authentication with seamless single sign-on (SSO)

Answer: C

Explanation:
* 1. Ensures that password policies and user logon restrictions apply to user accounts that are synced to the tenant
>> Pass-Through Authentication enforce on-premises user account states, password policies, and sign-in hours.
* 2. Minimizes the number of servers required for the solution.
>> Pass-through needs a lightweight agent to be installed one (or more) on-premises servers.
>> PW Hash also require installing Azure AD Connect on your existing DC.

NEW QUESTION 60
- (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 62
- (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 66
- (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 67
- (Exam Topic 4)
You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
An administrator named Admin1 has access to the following identities:

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

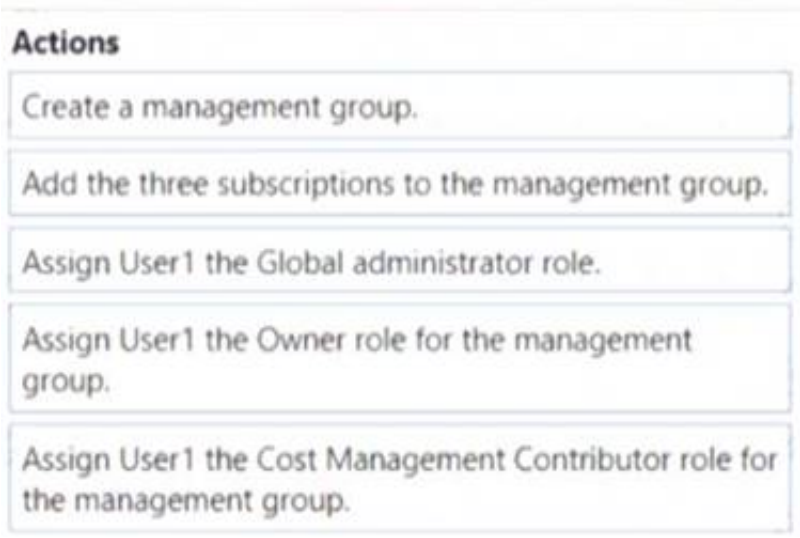
You plan to use Azure Account Center to transfer the ownership of Sub1 to Admin1. To which accounts can you transfer the ownership of Sub1?

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

Answer: C

Explanation:
When you transfer billing ownership of your subscription to an account in another Azure AD tenant, you can move the subscription to the new account's tenant. If you do so, all users, groups, or service principals who had role based access (RBAC) to manage subscriptions and its resources lose their access. Only the user in the new account who accepts your transfer request will have access to manage the resources.
Reference:
https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer
https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transferring-subscription-to-anaccou

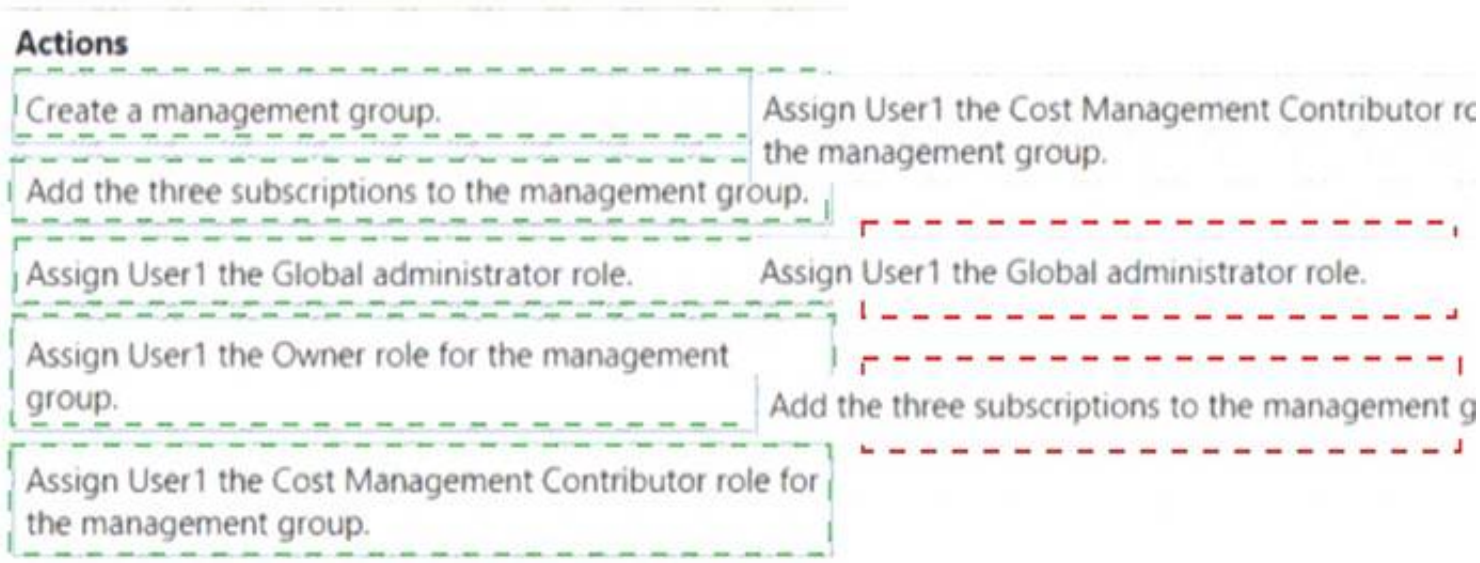
NEW QUESTION 71
- (Exam Topic 4)
You have three Azure subscriptions and a user named User1.
You need to provide User1 with the ability to manage and view costs for the resources across all three subscriptions. The solution must use the principle of least privilege.
Which three actions should you perform 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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 74
- (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.

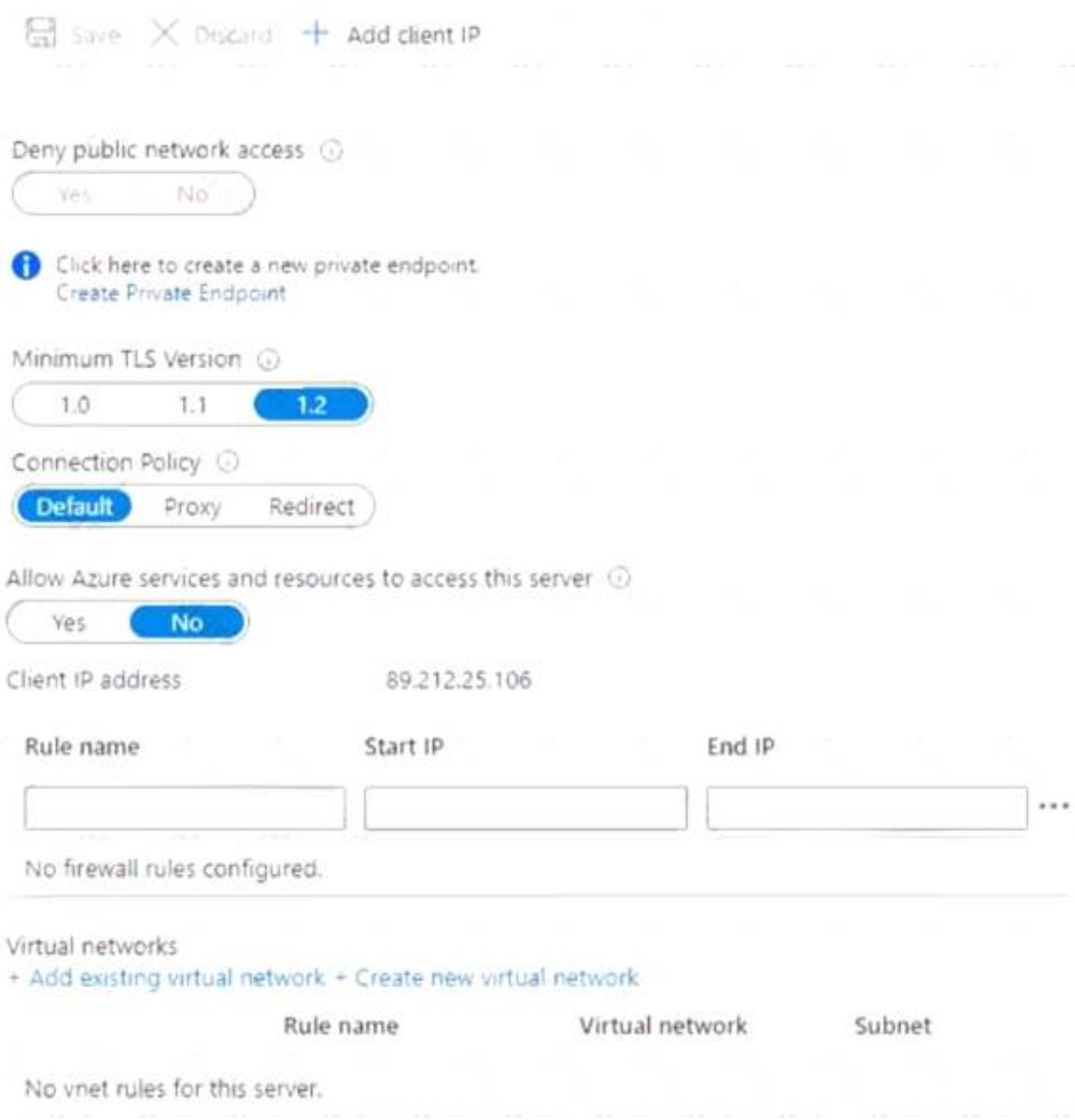
Statements	Yes	No
Admin1 can recover key1 on June 5.	○	○
Admin2 can purge secret1 on June 12.	○	○
Admin3 can recover key1 on June 17.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Yes
Yes No

NEW QUESTION 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.



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 83
- (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 87
- (Exam Topic 4)
You have an Azure subscription that contains virtual machines. You enable just in time (JIT) VM access to all the virtual machines.
You need to connect to a virtual machine by using Remote Desktop. What should you do first?

A. From Azure Directory (Azure AD) Privileged Identity Management (PIM), activate the Security administrator user role.
B. From Azure Active Directory (Azure AD) Privileged Identity Management (PIM), activate the Owner role for the virtual machine.
C. From the Azure portal, select the virtual machine, select Connect, and then select Request access.
D. From the Azure portal, select the virtual machine and add the Network Watcher Agent virtual machine extension.

Answer: C

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

NEW QUESTION 92
- (Exam Topic 4)
You have a network security group (NSG) bound to an Azure subnet.
You run Get-AzureRmNetworkSecurityRuleConfig and receive the output shown in the following exhibit.

```
Name                                  : DenyStorageAccess
Description                           :
Protocol                              : *
SourcePortRange                       : {*}
DestinationPortRange                  : {*}
SourceAddressPrefix                   : {*}
DestinationAddressPrefix              : {Storage}
SourceApplicationSecurityGroups       : []
DestinationApplicationSecurityGroups  : []
Access                                : Deny
Priority                              : 105
Direction                             : Outbound

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

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

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

- able to connect to East US
- able to connect to East US 2
- able to connect to West Europe
- prevented from connecting to all regions

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

- allowed
- dropped
- forwarded

A. Mastered
B. Not Mastered

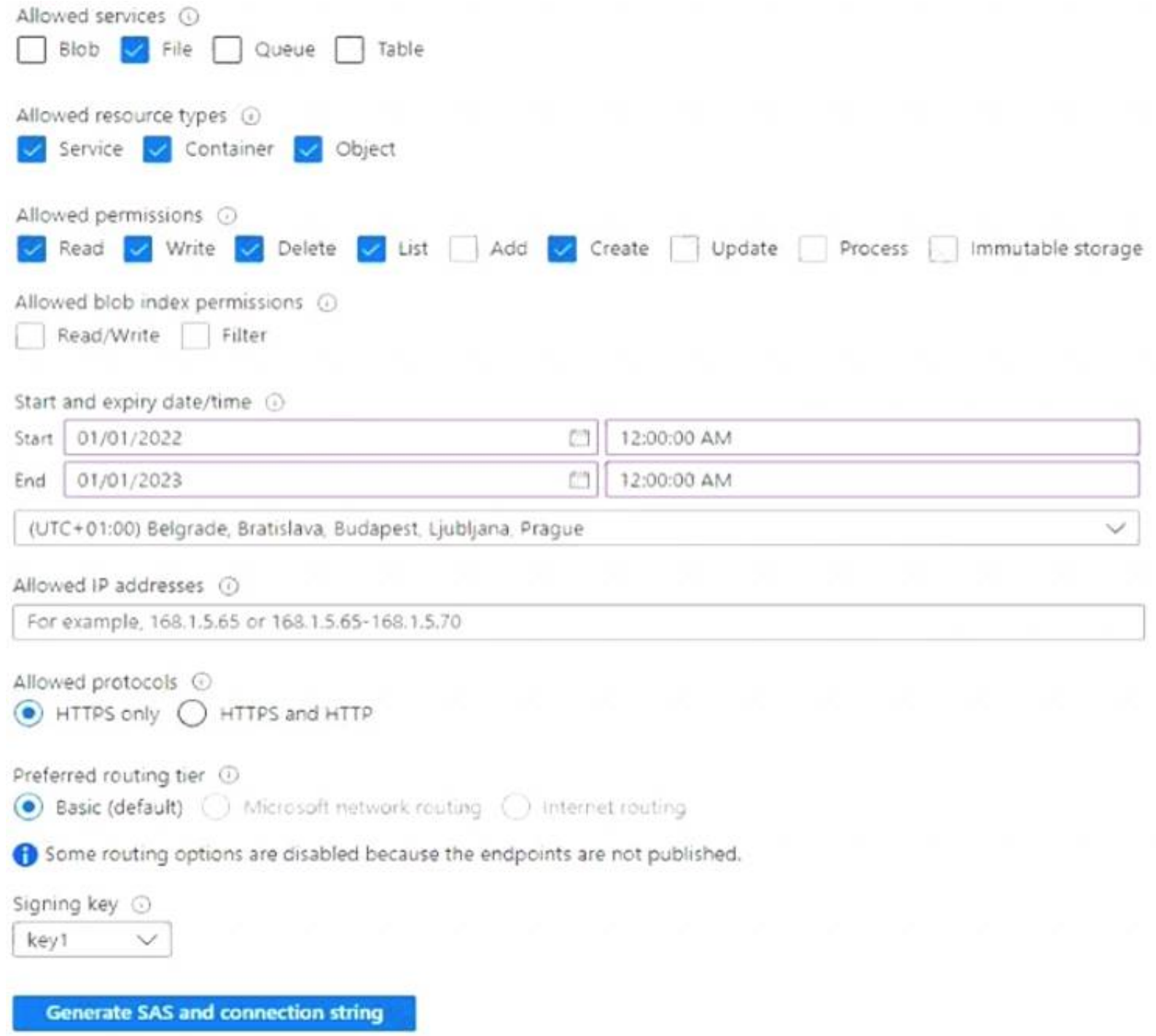
Answer: A

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

NEW QUESTION 97
- (Exam Topic 4)
You have an Azure subscription that contains a user named User1 and a storage account named storage1. The storage1 account contains the resources shown in the following table.

Name	Type
container1	Container
folder1	File Share
table1	Table

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



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

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

NEW QUESTION 98
- (Exam Topic 4)
You have an Azure subscription that contains a
You need to grant user1 access to blob1. The solution must ensure that the access expires after six days. What should you use?

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

Answer: C

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

NEW QUESTION 99
- (Exam Topic 4)
You have an Azure subscription.
You plan to implement Azure DDoS Protection. The solution must meet the following requirement:
* Provide access to DDoS rapid response support during active attacks.
* Project Basic SKU public IP addresses.
You need to recommend which type of DDoS projection to use for each requirement.
What should you recommend? To answer, drag the appropriate DDoS projection types to the correct requirements. Each DDoS Projection type may be used once, or not at all. You may need to drag the split bar between panes or scroll to view connect.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

DDoS Protection types

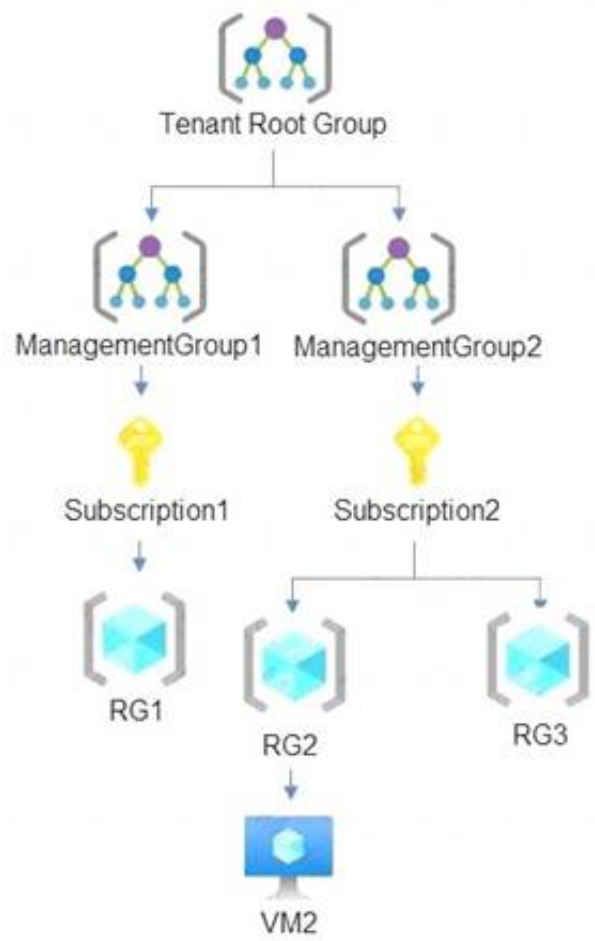
- DDoS infrastructure protection
- DDoS IP Protection
- DDoS Network Protection

Answer Area

Provide access to DDoS rapid response support during active attacks: DDoS Network Protection

Protect Basic SKU public IP addresses: DDoS IP Protection

NEW QUESTION 102
- (Exam Topic 4)
You have the hierarchy of Azure resources shown in the following exhibit.



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

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

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

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

A. Mastered
B. Not Mastered

Answer: A

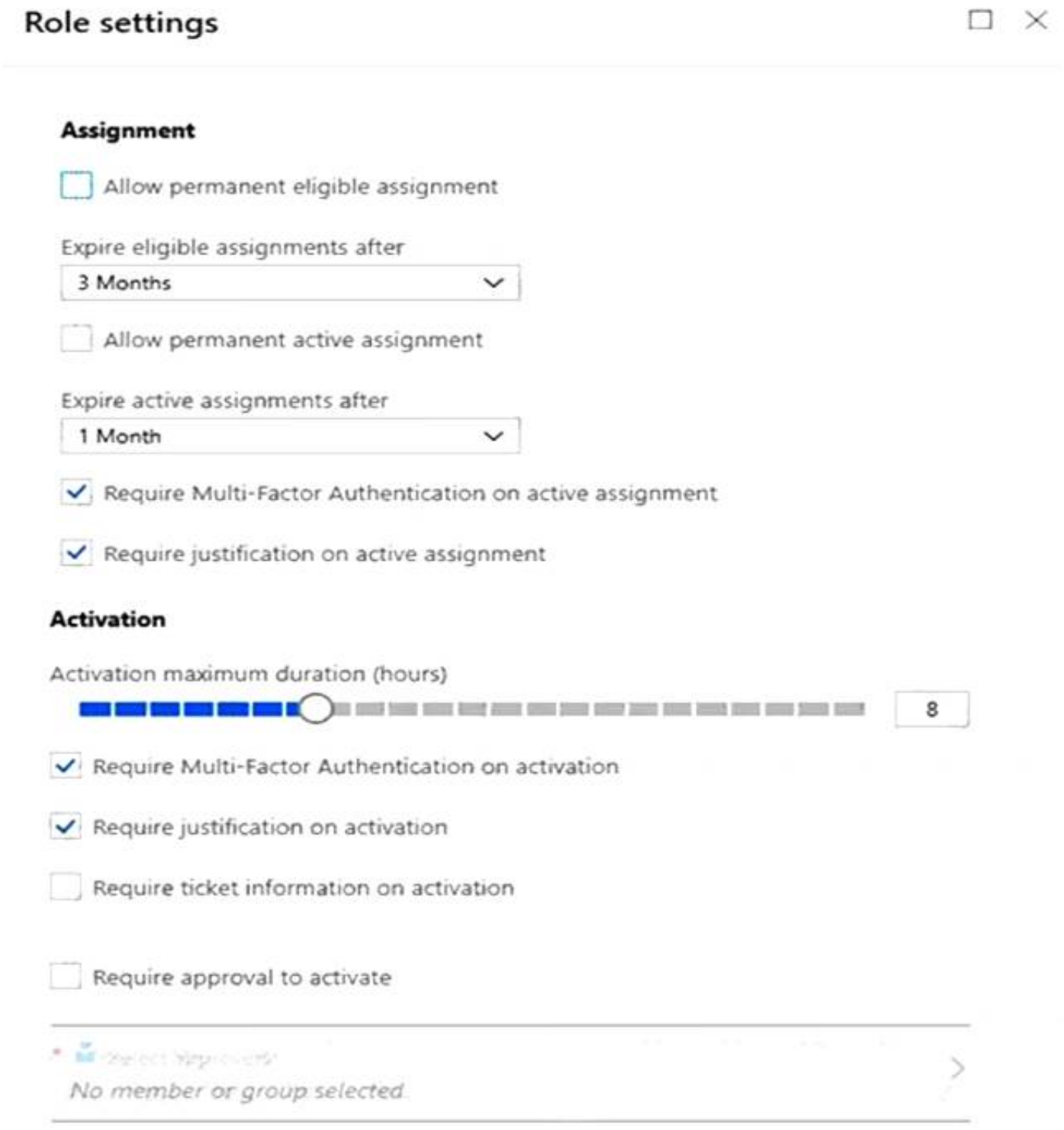
Explanation:

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

NEW QUESTION 104
- (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

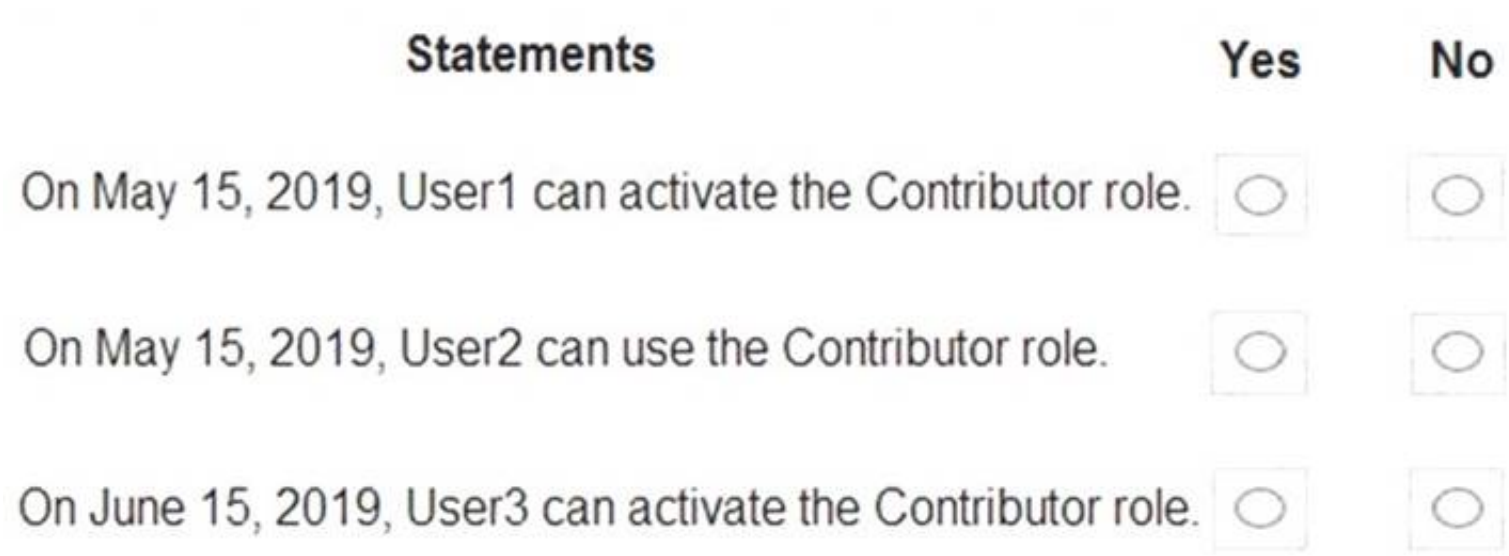
In Azure AD Privileged Identity Management (PIM), the Role settings for the Contributor role are configured as shown in the exhibit. (Click the Exhibit tab.)



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.

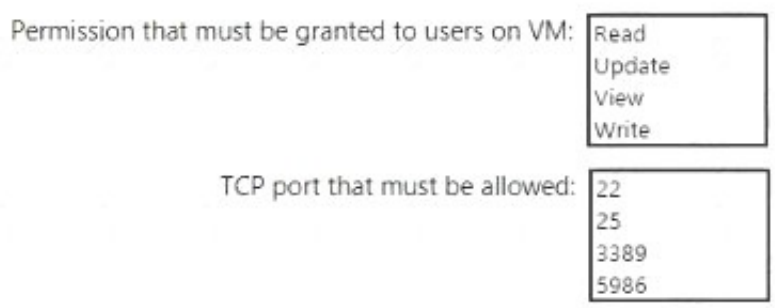


A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 108
- (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



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 109
- (Exam Topic 4)
You have an Azure AD turned that contains a user named User1. You purchase an App named App1.
User1 needs to publish App1 by using Azure AD Application Proxy. Which role should you assign to User1?

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

Answer: C

NEW QUESTION 112
- (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

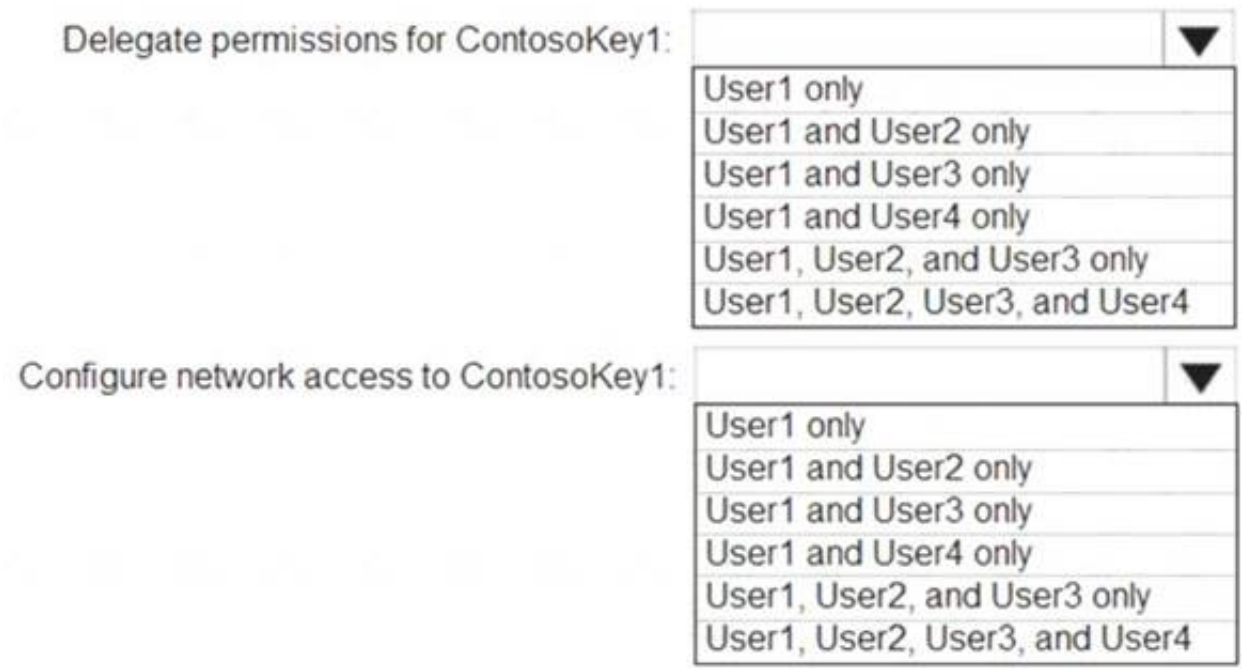
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

NEW QUESTION 113
- (Exam Topic 4)
You have an Azure subscription that contains an Azure key vault named ContosoKey1. You create users and assign them roles as shown in the following table.

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

You need to identify which users can perform the following actions:
- Delegate permissions for ContsosKey1.
- Configure network access to ContosoKey1.

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



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 116
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant. The tenant contains users that are assigned Azure AD Premium Plan 2 licenses.
You have an partner company that has a domain named The fabrikam.com domain contains a user named user'. User' has an email address of userl@tabrikam.com.
You to provide User1 with to the resources in the tenant The solution must meet the following requirements:
- user1 must be able to sign in by using the userl@fabrikam.com credentials
- You must be able to grant User1 access to the resources in the tenant
- Administrative effort must be minimized.

What should you do?

A. Create a user account for user1.
B. Create an invite for User1.
C. To the tenant add fabrikamcom as a custom domain
D. Set Enable guest self-service sign up via user flows to Yes for the tenant.

Answer: B

NEW QUESTION 117
- (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 118
- (Exam Topic 4)
You have an Azure Active directory tenant that syncs with an Active Directory Domain Services (AD DS) domain.
You plan to create an Azure file share that will contain folders and files.
Which identity store can you use to assign permissions to the Azure file share and folders within the share? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Azure files share:

Folders in the file share:

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Azure files share: AD DS only

Folders in the file share: AD DS and Azure AD

NEW QUESTION 120
- (Exam Topic 4)
You have an Azure subscription that contains a web app named App1.
Users must be able to select between a Google identity or a Microsoft identity when authenticating to App1. You need to add Google as an identity provider in Azure AD.
Which two pieces of information should you configure? Each correct answer presents part of the solution. Each correct selection is worth one point

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

Answer: DE

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

NEW QUESTION 125
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Security Center for the centralized policy management of three Azure subscriptions. You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create a resource graph and an assignment that is scoped to a management group. Does this meet the goal?

A. Yes

B. No

Answer: B

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

NEW QUESTION 126
- (Exam Topic 4)
You have an Azure subscription that contains the virtual machines shown in the following table.

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

You create the Azure policies shown in the following table.

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

You create the resource locks shown in the following table.

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

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

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 129
- (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 132

- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains a group named Group1 You need to ensure that the members of Group1 sign in by using passwordless authentication What should you do?

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

Answer: A

NEW QUESTION 134
- (Exam Topic 4)
You company has an Azure Active Directory (Azure AD) tenant named contoso.com. You plan to create several security alerts by using Azure Monitor.
You need to prepare the Azure subscription for the alerts. What should you create first?

A. An Azure Storage account
B. an Azure Log Analytics workspace
C. an Azure event hub
D. an Azure Automation account

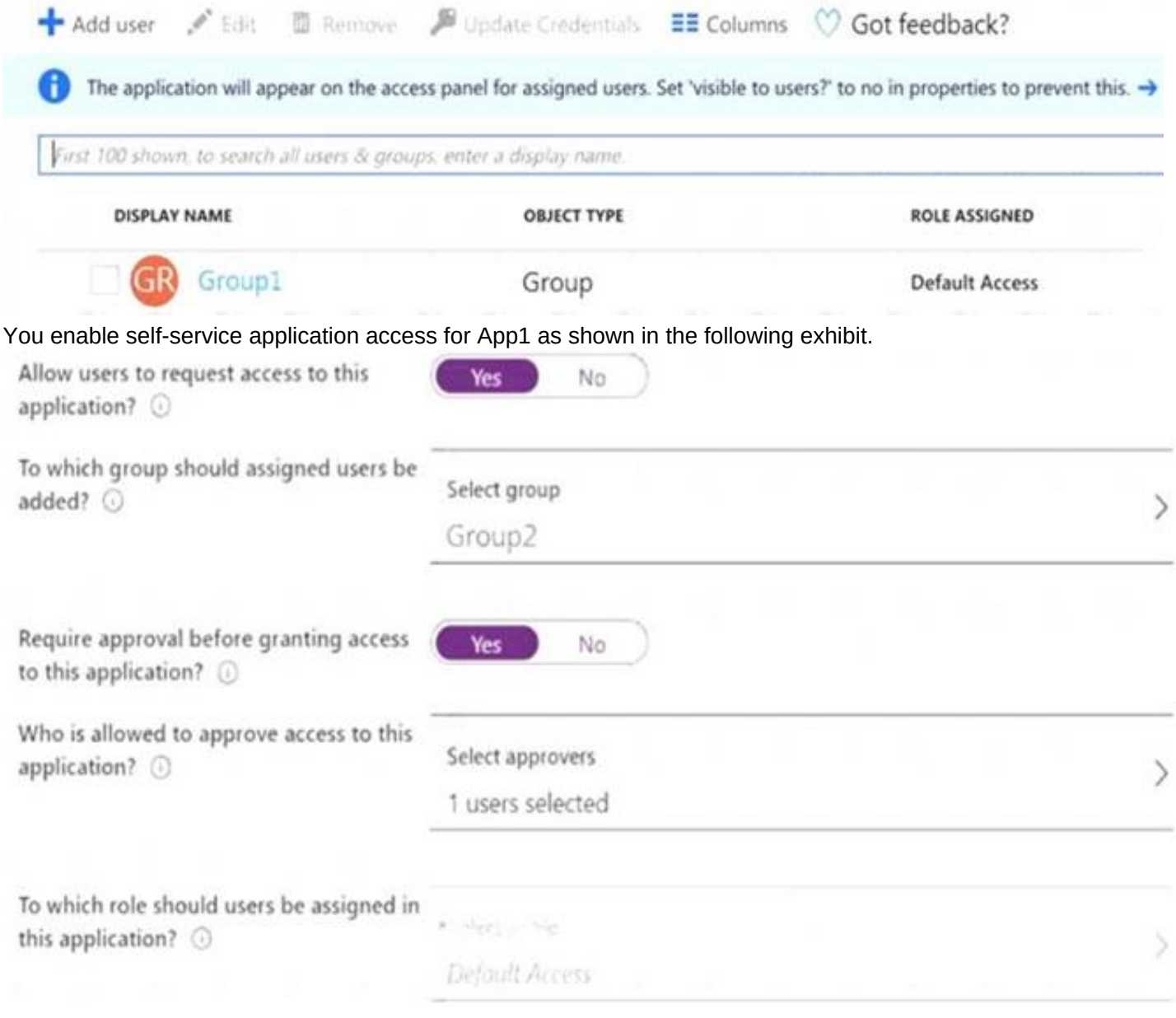
Answer: B

Explanation:
https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-create-workspace

NEW QUESTION 138
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains the resources shown in the following table.

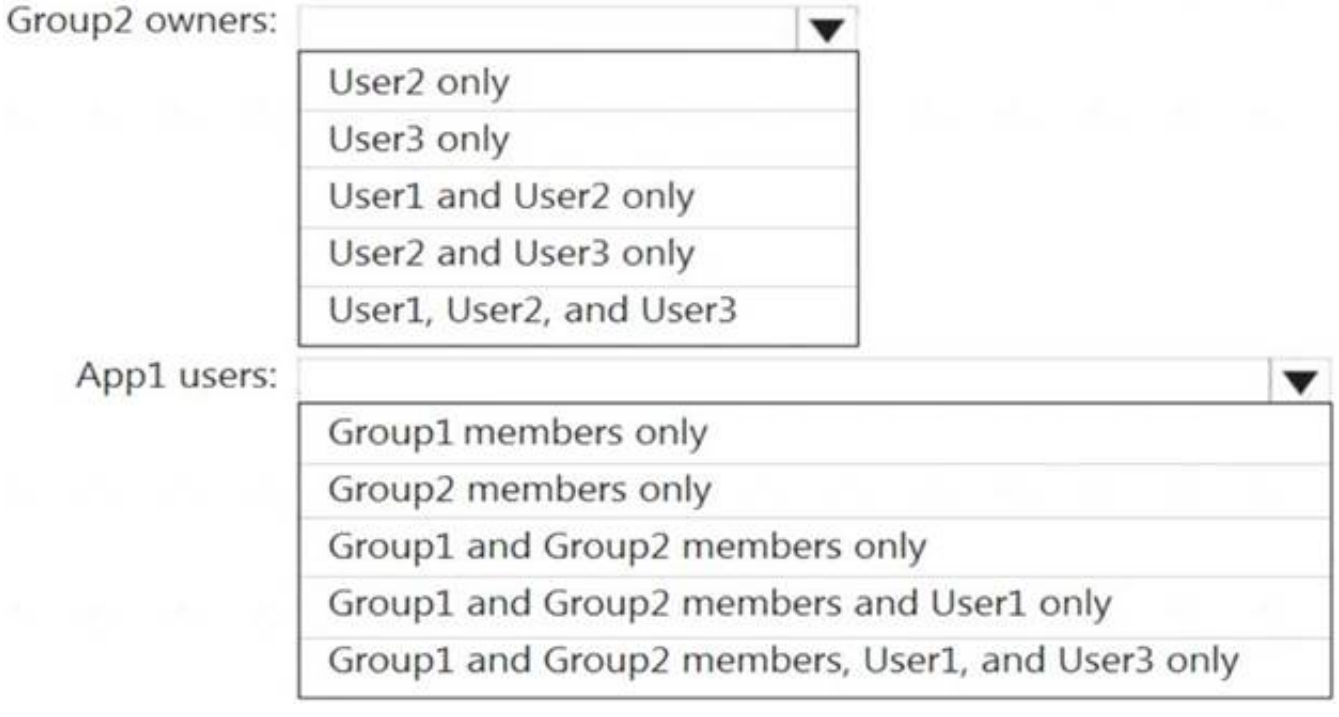
Name	Type
User1	User
User2	User
User3	User
Group1	Security group
Group2	Security group
App1	Enterprise application

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



User3 is configured to approve access to Appl.
You need to identify the owners of Group2 and the users of Appl.
What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 143
- (Exam Topic 4)
You are troubleshooting a security issue for an Azure Storage account You enable Azure Storage Analytics logs and archive It to a storage account. What should you use to retrieve the diagnostics logs?

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

Answer: A

NEW QUESTION 148
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Security Center for the centralized policy management of three Azure subscriptions. You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create a policy definition and assignments that are scoped to resource groups. Does this meet the goal?
A. Yes
B. No

Answer: B

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

NEW QUESTION 150
- (Exam Topic 4)
You have the Azure resource shown in the following table.

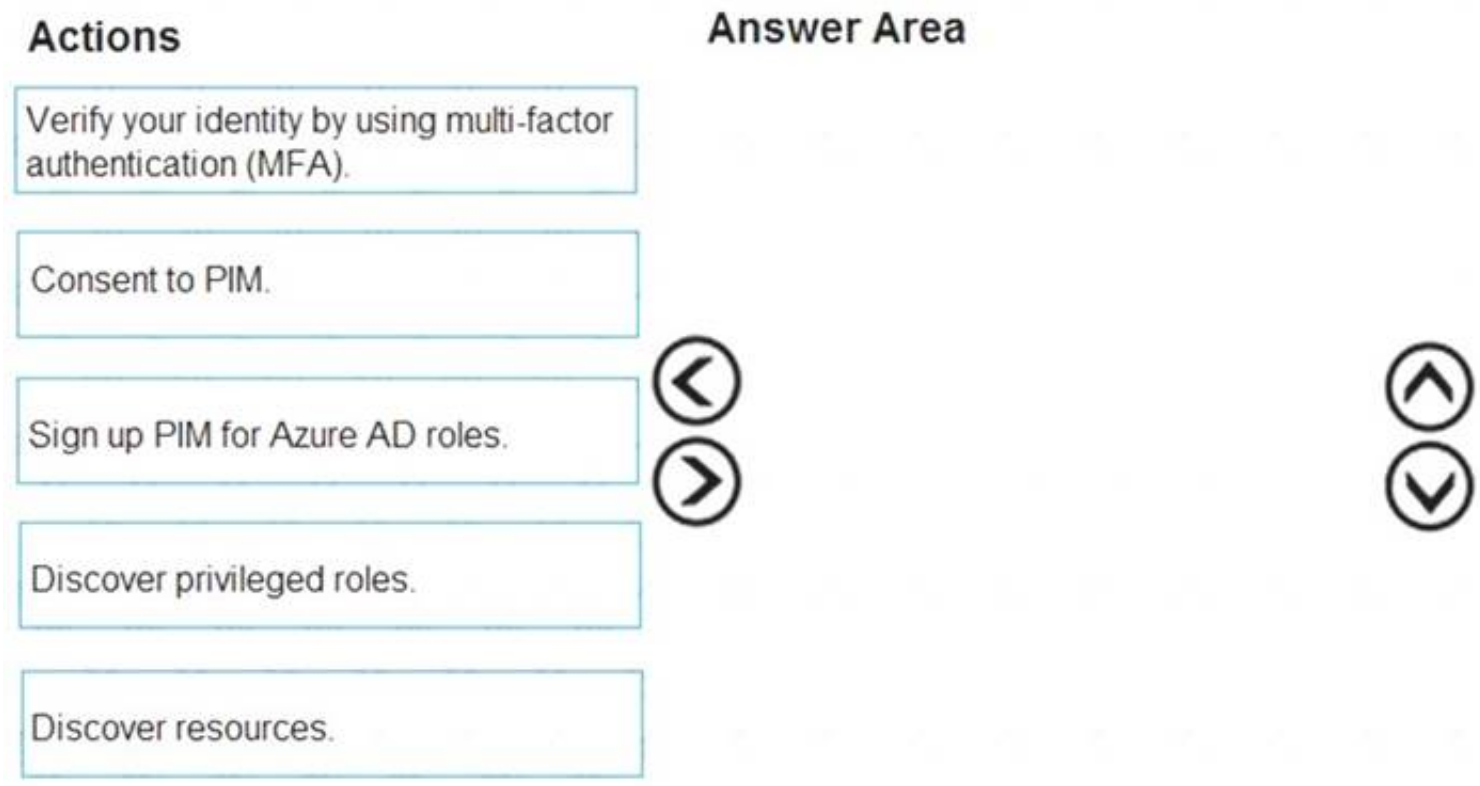
Name	Type	Parent
Management1	Management group	Tenant Root Group
Subscription1	Subscription	Management1
RG1	Resource group	Subscription1
RG2	Resource group	Subscription1
VM1	Virtual machine	RG1
VM2	Virtual machine	RG2

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

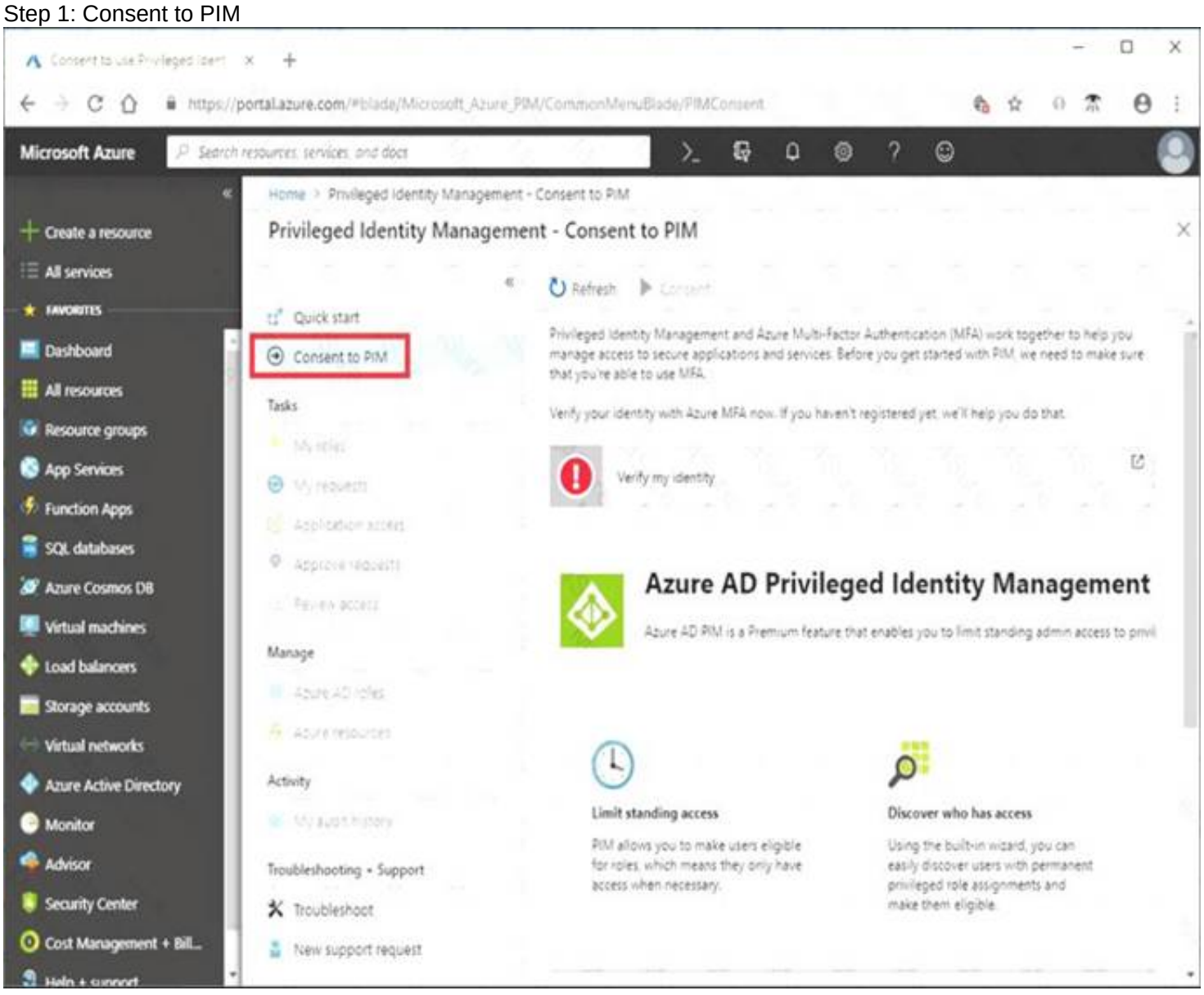
NEW QUESTION 155
- (Exam Topic 4)
DRAG DROP
You create an Azure subscription.
You need to ensure that you can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to secure Azure AD roles.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

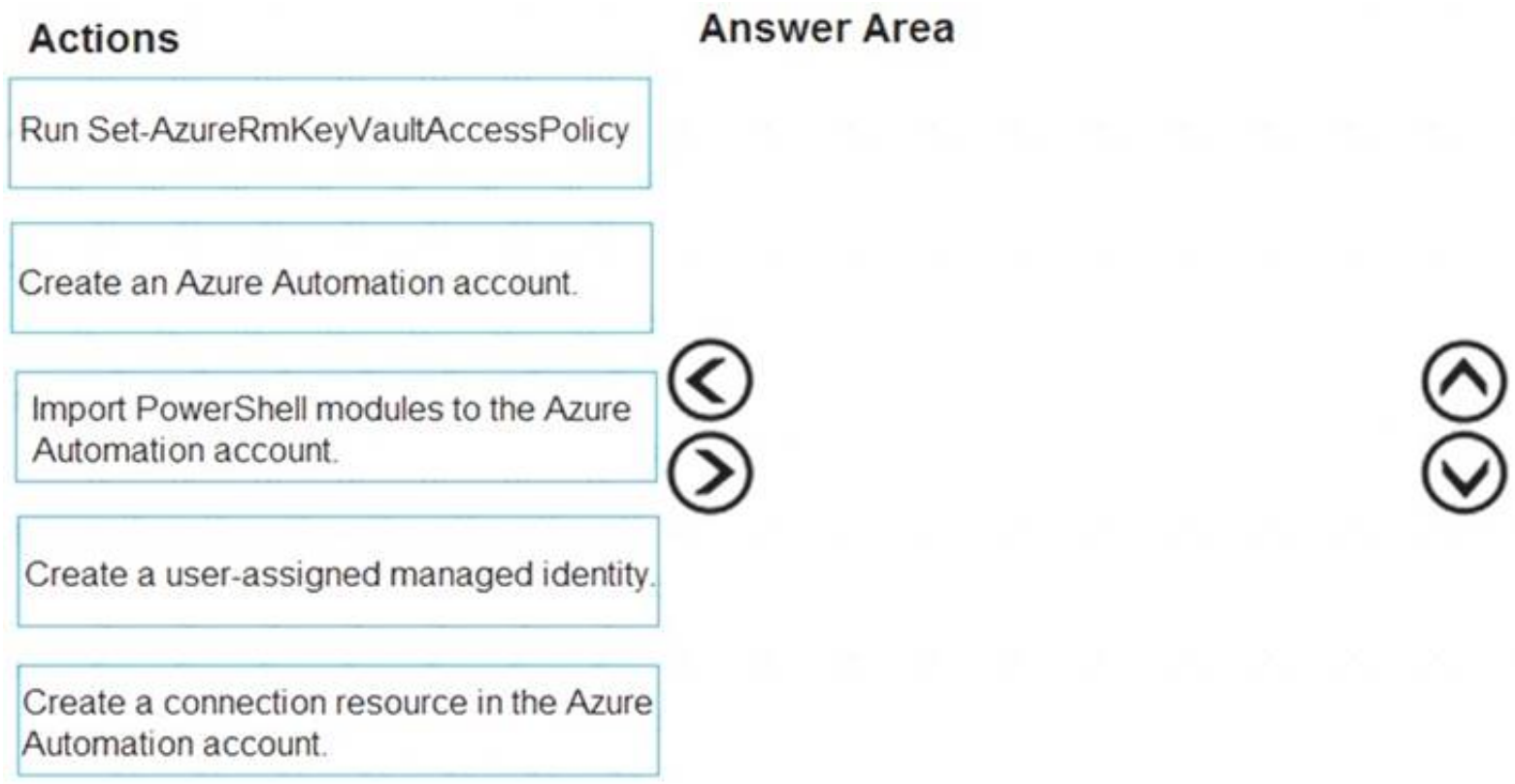
Explanation:
Step 1: Consent to PIM



Step: 2 Verify your identity by using multi-factor authentication (MFA)
Click Verify my identity to verify your identity with Azure MFA. You'll be asked to pick an account. Step 3: Sign up PIM for Azure AD roles

Once you have enabled PIM for your directory, you'll need to sign up PIM to manage Azure AD roles. References:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started

NEW QUESTION 159
- (Exam Topic 4)
You have an Azure subscription named Sub1 that contains an Azure Storage account named Contosostorage1 and an Azure key vault named Contosokeyvault1.
You plan to create an Azure Automation runbook that will rotate the keys of Contosostorage1 and store them in Contosokeyvault1.
You need to implement prerequisites to ensure that you can implement the runbook.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Step 1: Create an Azure Automation account
Runbooks live within the Azure Automation account and can execute PowerShell scripts. Step 2: Import PowerShell modules to the Azure Automation account
Under 'Assets' from the Azure Automation account Resources section select 'to add in Modules to the runbook. To execute key vault cmdlets in the runbook, we need to add AzureRM.profile and AzureRM.key vault.
Step 3: Create a connection resource in the Azure Automation account
You can use the sample code below, taken from the AzureAutomationTutorialScript example runbook, to authenticate using the Run As account to manage Resource Manager resources with your runbooks. The AzureRunAsConnection is a connection asset automatically created when we created 'run as accounts' above. This can be found under Assets -> Connections. After the authentication code, run the same code above to get all the keys from the vault.
$connectionName = "AzureRunAsConnection" try
{
# Get the connection "AzureRunAsConnection "
$servicePrincipalConnection=Get-AutomationConnection -Name $connectionName "Logging in to Azure..."
Add-AzureRmAccount `
-ServicePrincipal `
-TenantId $servicePrincipalConnection.TenantId `
-ApplicationId $servicePrincipalConnection.ApplicationId `
-CertificateThumbprint $servicePrincipalConnection.CertificateThumbprint
}
References:
https://www.rahulpnath.com/blog/accessing-azure-key-vault-from-azure-runbook/

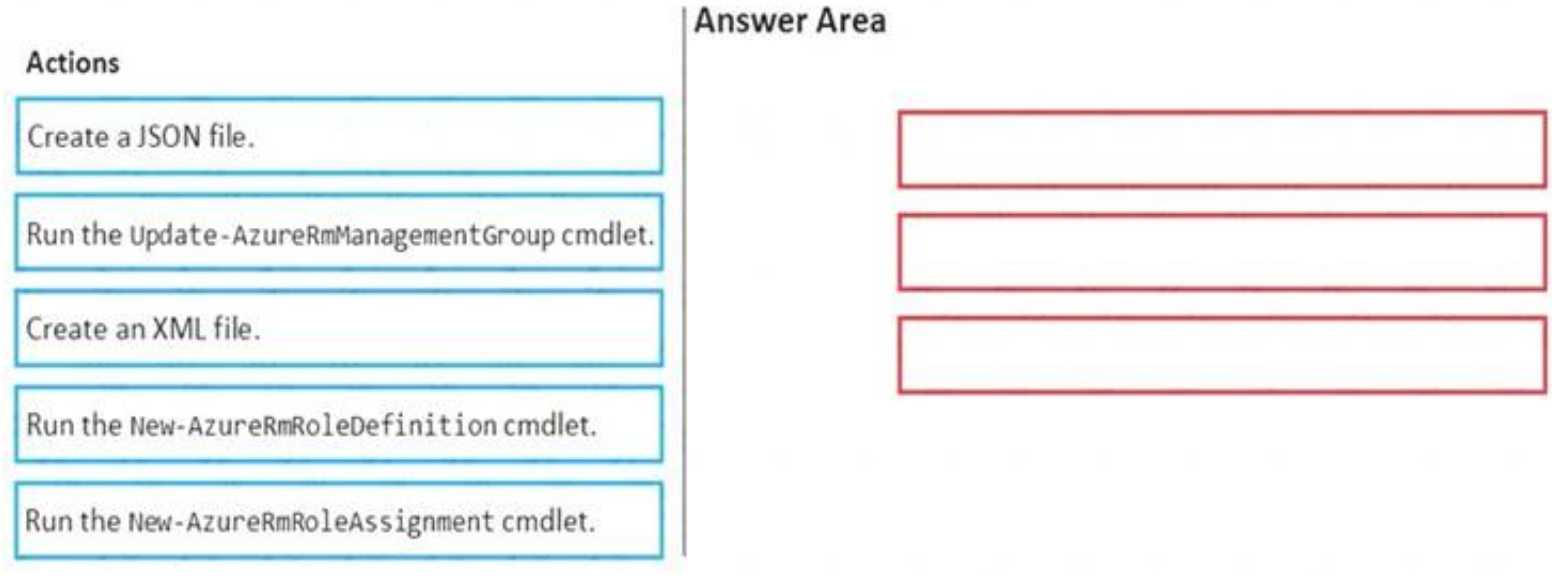
NEW QUESTION 164
- (Exam Topic 4)
Your network contains an on-premises Active Directory domain named corp.contoso.com.
You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
You sync all on-premises identities to Azure AD.
You need 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 165
- (Exam Topic 4)
You have an Azure subscription named Sub1.
You have an Azure Active Directory (Azure AD) group named Group1 that contains all the members of your IT team.
You need to ensure that the members of Group1 can stop, start, and restart the Azure virtual machines in Sub1. The solution must use the principle of least privilege.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 166
- (Exam Topic 4)
You have an Azure Sentinel deployment.
You need to create a scheduled query rule named Rule1. What should you use to define the query rule logic for Rule1?

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

Answer: D

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

NEW QUESTION 170
- (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 174
- (Exam Topic 4)
You have an Azure environment.
You need to identify any Azure configurations and workloads that are non-compliant with ISO 27001:2013 standards.
What should you use?

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

Answer: B

NEW QUESTION 179
- (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

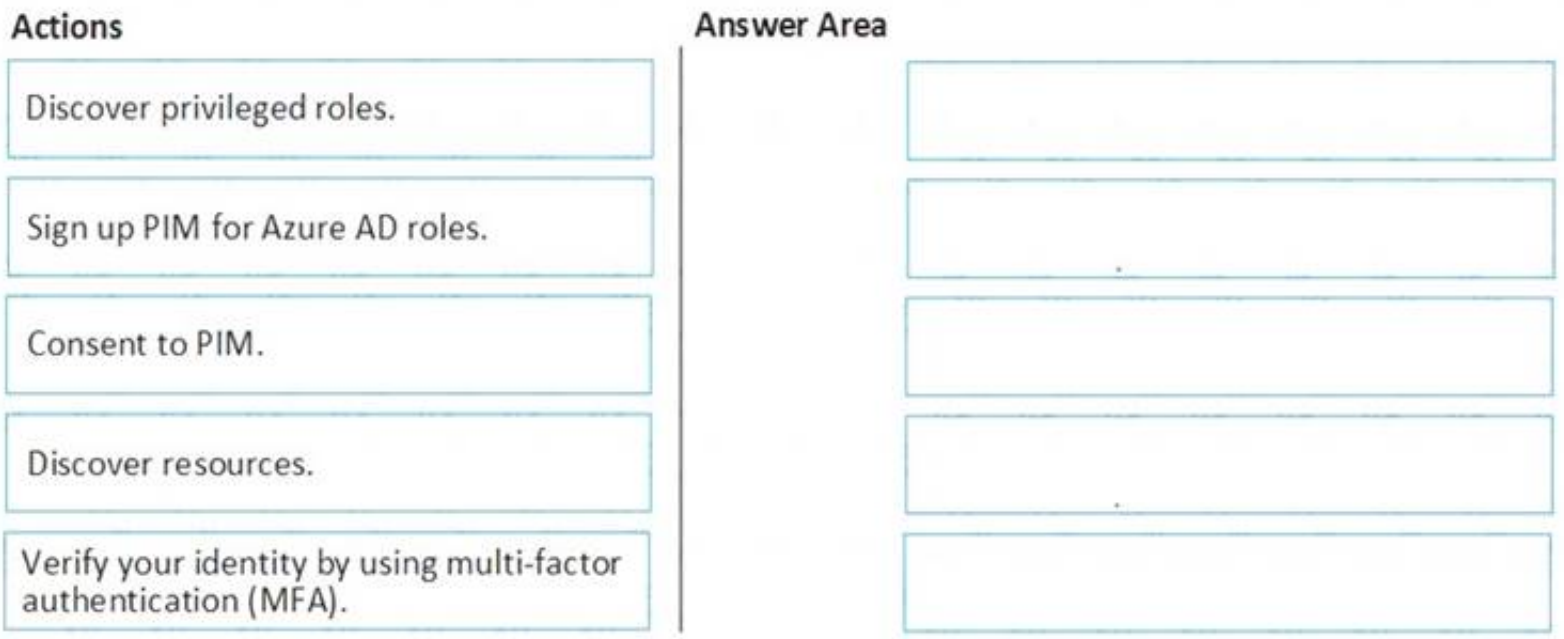
On May 4, 2020, you attempt to restore the deleted objects by using the Azure Active Directory admin center. Which two objects can you restore? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

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 181
- (Exam Topic 4)
You create an Azure subscription with Azure AD Premium P2.
You need to ensure that you can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to secure Azure roles.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 185
- (Exam Topic 4)
You have an Azure subscription that contains the virtual machines shown in the following table.

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

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

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

On which virtual machines is the Microsoft Monitoring agent installed?

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

Answer: D

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

NEW QUESTION 190
- (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 195
- (Exam Topic 4)
HOTSPOT
You suspect that users are attempting to sign in to resources to which they have no access.
You need to create an Azure Log Analytics query to identify failed user sign-in attempts from the last three days. The results must only show users who had more than five failed sign-in attempts.
How should you configure the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

```
let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AcccountType == 'User' and [ ▼ ] ==4625
```

- ActivityID
- DataType
- EventID
- QuantityUnit

```
| Summarie failed_login_attempts= [ ▼ ]
```

- Count(),
- Countif(),
- Makeset(),
- Split(),

```
    latest_failed_login=arg_max(TimeGenerated by Account
| where failed login attempts > 5
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:
The following example identifies user accounts that failed to log in more than five times in the last day, and when they last attempted to log in.
let timeframe = 1d; SecurityEvent
| where TimeGenerated > ago(1d)
| where AccountType == 'User' and EventID == 4625 // 4625 - failed log in
| summarize failed_login_attempts=count(), latest_failed_login=arg_max(TimeGenerated, Account) by Account
| where failed_login_attempts > 5
| project-away Account1 References:
https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/examples

NEW QUESTION 198
- (Exam Topic 4)
You have an Azure subscription named Sub 1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

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

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

Users who can onboard Azure AD Identity Protection: [User1 only / User1 and User2 only / User1, User 2, and User3 only / User1, User 2, User3, and User 4 only]

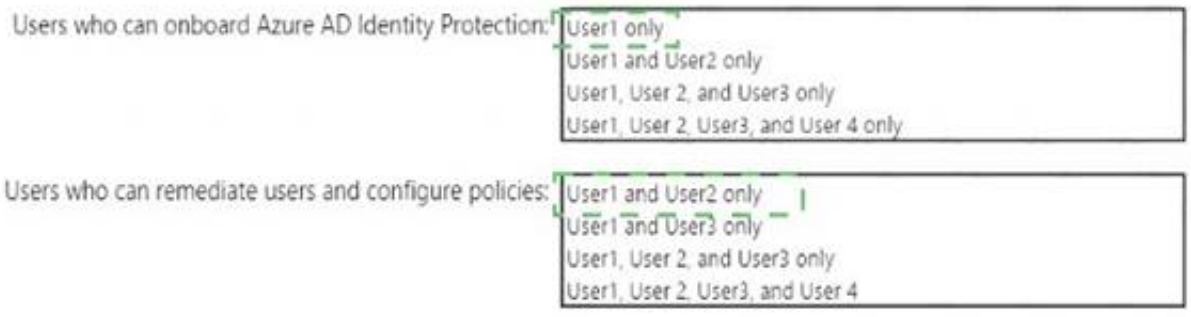
Users who can remediate users and configure policies: [User1 and User2 only / User1 and User3 only / User1, User 2, and User3 only / User1, User 2, User3, and User 4]

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

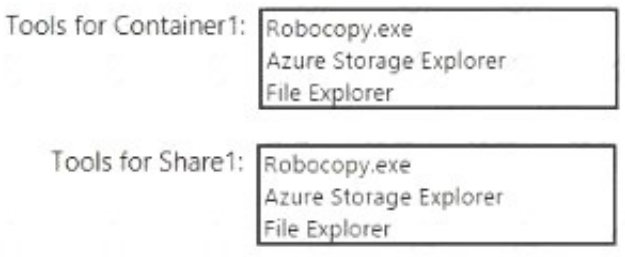


NEW QUESTION 201
- (Exam Topic 4)
You have an Azure subscription named Sub1. Sub1 has an Azure Storage account named Storage1 that contains the resources shown in the following table.

Name	Type
Container1	Blob container
Share1	File share

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

Answer Area

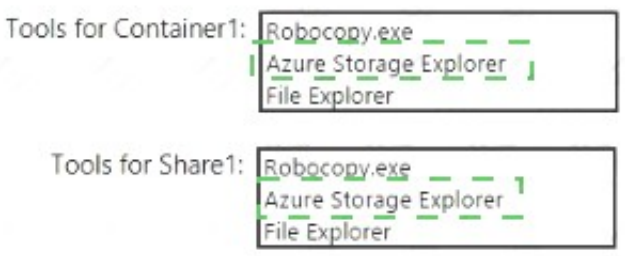


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 205
- (Exam Topic 4)
You have an Azure subscription that contains the virtual networks shown in the following table.

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

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

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

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

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

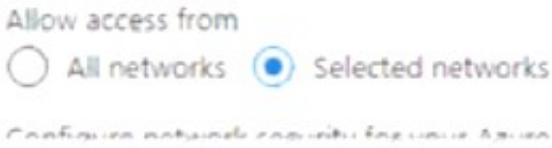
Answer: C

Explanation:
Only network interfaces in NVET1, which consists of Subnet11 and Subnet12, can be configured in ASG1, as all network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in.
Reference:
https://azure.microsoft.com/es-es/blog/applicationsecuritygroups/

NEW QUESTION 206
- (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.



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 208
- (Exam Topic 4)
You work at a company named Contoso, Ltd. that has the offices shown in the following table.

Name	IP address space
Boston	180.15.10.0/24
Seattle	132.32.15.0/24

Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com. All contoso.com users have Azure Multi-Factor Authentication (MFA) enabled. The tenant contains the users shown in the following table.

Name	User device	Last sign-in	During last sign-in, user selected Don't ask again for 14 days
User1	Device1	June 1	Yes
User2	Device2	June 3	No

The multi-factor settings for contoso.com are configured as shown in the following exhibit.

multi-factor authentication

users service settings

app passowrds (learn more)

- (•) Allow users to create app paswords to sign in to non-browser apps
- ( ) Do not allow users to create app passwords to sign in to non-browser apps

trusted ips (learn more)

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

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

180.15.10.0/24

verification options (learn more)

Methods available to users:

- [ ] call to phone
- [x] Text message to phone
- [x] Notification through mobile app
- [x] Verification code from mobile app or hardware token

remember multi-factor authentication (learn more)

- [x] Allow users to remember multi-factor authentication on devices they trust

Days before a device must re-authenticate (1-60): 14

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 to Device1 from the Seattle office on June 10, the user will be prompted for MFA.	○	○
When User2 signs in to Device2 from the Boston office on June 5, the user will be prompted for MFA.	○	○
When User1 signs in to to a new device from the Seattle office on June 7, the user will be prompted for MFA.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 210
- (Exam Topic 4)
You have an Azure subscription that uses Microsoft Defender for Cloud.
You have an Amazon Web Services (AWS) account.
You need to ensure that when you deploy a new AWS Elastic Compute Cloud (EC2) instance, the Microsoft Defender for Servers agent installs automatically.
What should you configure first?

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

Answer: A

NEW QUESTION 212
- (Exam Topic 4)
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 216
- (Exam Topic 4)
You plan to use Azure Resource Manager templates to perform multiple deployments of identically configured Azure virtual machines. The password for the administrator account of each deployment is stored as a secret in different Azure key vaults.
You need to identify a method to dynamically construct a resource ID that will designate the key vault containing the appropriate secret during each deployment.
The name of the key vault and the name of the secret will be provided as inline parameters.
What should you use to construct the resource ID?

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

Answer: C

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

NEW QUESTION 218
- (Exam Topic 4)
You have an Azure subscription that contains a storage account named storage1 and a virtual machine named VM1.
VM1 is connected to a virtual network named VNet1 that contains one subnet and uses Azure DNS.
You need to ensure that VM1 connects to storage1 by using a private IP address. The solution must minimize administrative effort.
What should you do?

A. For storage1, disable public network access.
B. Create an Azure Private DNS zone.

C. On VNet1. create a new subnet.
D. For storage1, create a new private endpoint.

Answer: D

NEW QUESTION 222
- (Exam Topic 4)
You have an Azure resource group that contains 100 virtual machines.
You have an initiative named Initiative1 that contains multiple policy definitions. Initiative1 is assigned to the resource group.
You need to identify which resources do NOT match the policy definitions.
What should you do?

A. From Azure Security Center, view the Regulatory compliance assessment.
B. From the Policy blade of the Azure Active Directory admin center, select Compliance.
C. From Azure Security Center, view the Secure Score.
D. From the Policy blade of the Azure Active Directory admin center, select Assignments.

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/how-to/get-compliance-data#portal

NEW QUESTION 226
- (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 227
- (Exam Topic 4)
You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant. From the Azure portal, you register an enterprise application.
Which additional resource will be created in Azure AD?

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

Answer: A

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

NEW QUESTION 231
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant named contoso.com
You need to configure diagnostic settings for contoso.com. The solution must meet the following requirements:
• Retain loqs for two years.
• Query logs by using the Kusto query language
• Minimize administrative effort. Where should you store the logs?

A. an Azure Log Analytics workspace
B. an Azure event hub

C. an Azure Storage account

Answer: A

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

NEW QUESTION 236
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Security Center for the centralized policy management of three Azure subscriptions. You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create an initiative and an assignment that is scoped to the Tenant Root Group management group.
Does this meet the goal?

A. Yes
B. No

Answer: A

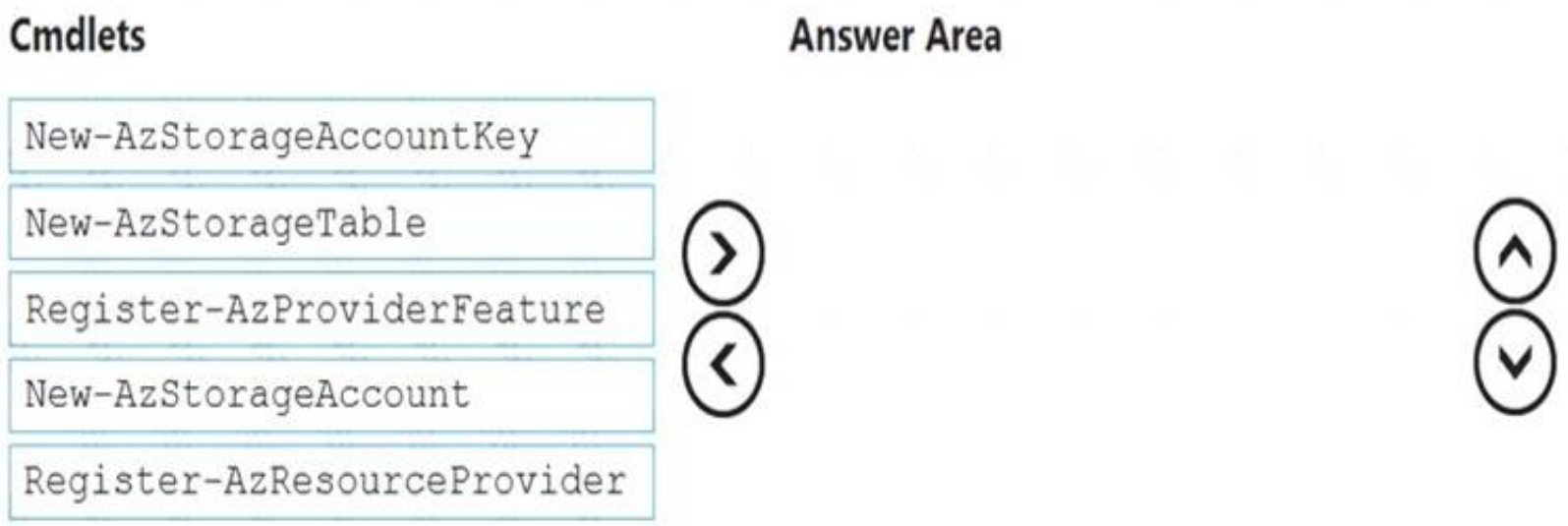
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/overview
https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-group

NEW QUESTION 239
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.
You need to ensure that User1 can create and manage administrative units. The solution must use the principle of least privilege.
Which role should you assign to User1?

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

Answer: A

NEW QUESTION 243
- (Exam Topic 4) You have an Azure subscription. You plan to create a storage account.
You need to use customer-managed keys to encrypt the tables in the storage account.
From Azure Cloud Shell, which three cmdlets should you run in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 244
- (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

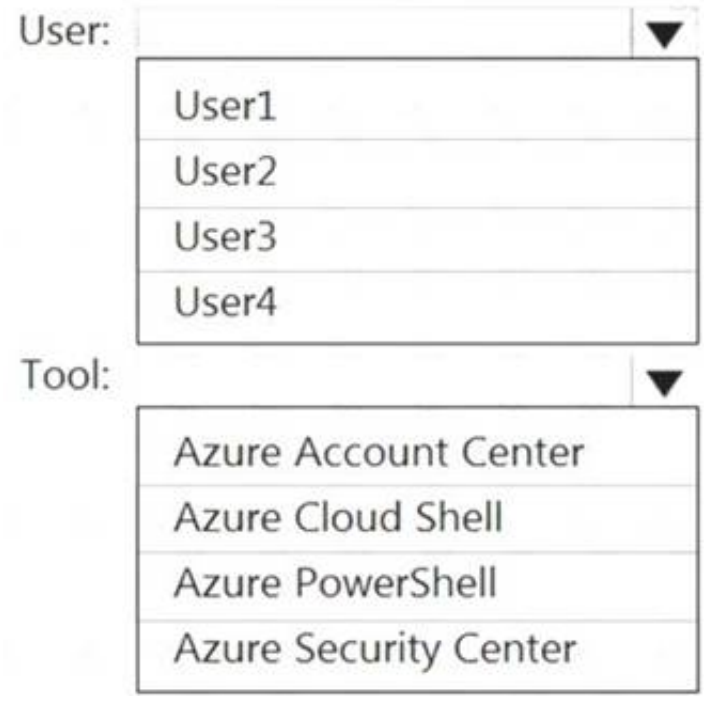
Answer: B

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 246
- (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 249
- (Exam Topic 4)
Lab Task
use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password. place your cursor in the Enter password box and click on the password below. Azure Username: Userl -28681041@ExamUsers.com
Azure Password: GpOAe4@lDg
If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only: Lab Instance: 28681041
Task 5
You need to ensure that only devices connected to a 131-107.0.0/16 subnet can access data in the rg1lod28681041 Azure Storage account.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
To ensure that only devices connected to a 131-107.0.0/16 subnet can access data in the rg1lod28681041 Azure Storage account, you can follow these steps:
- In the Azure portal, search for and select the storage account named rg1lod28681041.
- In the left pane, select Firewalls and virtual networks.

- In the Firewalls and virtual networks pane, select Selected networks.
- In the Selected networks pane, select Add existing virtual network.
- In the Add existing virtual network pane, select the virtual network that contains the 131-107.0.0/16 subnet.
- Select Add.

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

NEW QUESTION 253
- (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 258
- (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 262
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains a user named Admin1. Admin1 is assigned the Application developer role.
You purchase a cloud app named App1 and register App1 in Azure AD.

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

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

Answer: C

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

NEW QUESTION 265
- (Exam Topic 4)
You have an Azure subscription named Sub1 that contains the resource groups shown in the following table.

Name	Location
RG1	West US
RG2	East US

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

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

You assign the policy to Sub1.
You plan to create the resources shown in the following table.

Name	Type	Location	Resource group
IPobject1	Public IP address	East US	RG2
obj1	Resource group	West US	*Not applicable*
OBJ3	Virtual network	West US	RG1

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

Statements	Yes	No
You can create IPobject1.	○	○
You can create obj1.	○	○
You can create OBJ3.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
You can create IPobject1.	○	○
You can create obj1.	○	○
You can create OBJ3.	○	○

NEW QUESTION 268
- (Exam Topic 4)
You have an Azure subscription that contains a storage account named storage1 and several virtual machines. The storage account and virtual machines are in the same Azure region. The network configurations of the virtual machines are shown in the following table.

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

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

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

You configure the following Firewall and virtual networks settings for storage1:
- Allow access from: Selected networks
- Virtual networks: VNET3\Subnet3
- Firewall – Address range: 52.233.129.0/24

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

Statements	Yes	No
VM1 can connect to storage1.	○	○
VM2 can connect to storage1.	○	○
VM3 can connect to storage1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: No
VNet1 has a service endpoint configure for Azure Storage. However, the Azure storage does not allow access from VNet1 or the public IP address of VM1.
Box 2: Yes
VNet2 does not have a service endpoint configured. However, the Azure storage allows access from the public IP address of VM2.
Box 3: No
Azure storage allows access from VNet3. However, VNet3 does not have a service endpoint for Azure storage. The Azure storage also does not allow access from the public IP of VM3.

NEW QUESTION 271
- (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 274
- (Exam Topic 4)
You create resources in an Azure subscription as shown in the following table.

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

VNET1 contains two subnets named Subnet1 and Subnet2. Subnet1 has a network ID of 10.0.0.0/24. Subnet2 has a network ID of 10.1.1.0/24.
Contoso1901 is configured as shown in the exhibit. (Click the Exhibit tab.)

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

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

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

Action  IPAddressOrRange
------  ----------------
Allow   193.77.0.0/16


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

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

PS C:\> _
```

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

Statements	Yes	No
An Azure virtual machine on Subnet1 can access data in Contoso1901.	○	○
An Azure virtual machine on Subnet2 can access data in Contoso1901.	○	○
A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Yes
Access from Subnet1 is allowed. Box 2: No
No access from Subnet2 is allowed. Box 3: Yes
Access from IP address 193.77.10.2 is allowed.

NEW QUESTION 275
- (Exam Topic 4)
You have an Azure subscription that contains an Azure key vault and an Azure Storage account. The key vault contains customer-managed keys. The storage account is configured to use the customer-managed keys stored In the key vault.
You plan to store data in Azure by using the following services:
* Azure Files
* Azure Blob storage
* Azure Log Analytics
* Azure Table storage
* Azure Queue storage
Which two services data encryption by using the keys stored in the key vault? Each correct answer present a complete solution.

NOTE: Each correct selection is worth one point.

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

Answer: AC

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

NEW QUESTION 278
- (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 280
- (Exam Topic 4)
You have an Azure subscription that contains a user named User1. User1 is assigned the Reader role for the subscription.
You plan to create a custom role named Role1 and assign Role1 to User1.
You need to ensure that User1 can create and manage application security groups by using the Azure portal. Which two permissions should you add to Role1? To answer, select the appropriate permission in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Add permissions

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 285
- (Exam Topic 4)
Your company uses Azure DevOps.
You need to recommend a method to validate whether the code meets the company's quality standards and code review standards.
What should you recommend implementing in Azure DevOps?

A. branch folders
B. branch permissions
C. branch policies

D. branch locking

Answer: C

Explanation:
Branch policies help teams protect their important branches of development. Policies enforce your team's code quality and change management standards.
References:
https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies?view=azuredevops&
viewFallbackFrom=vsts

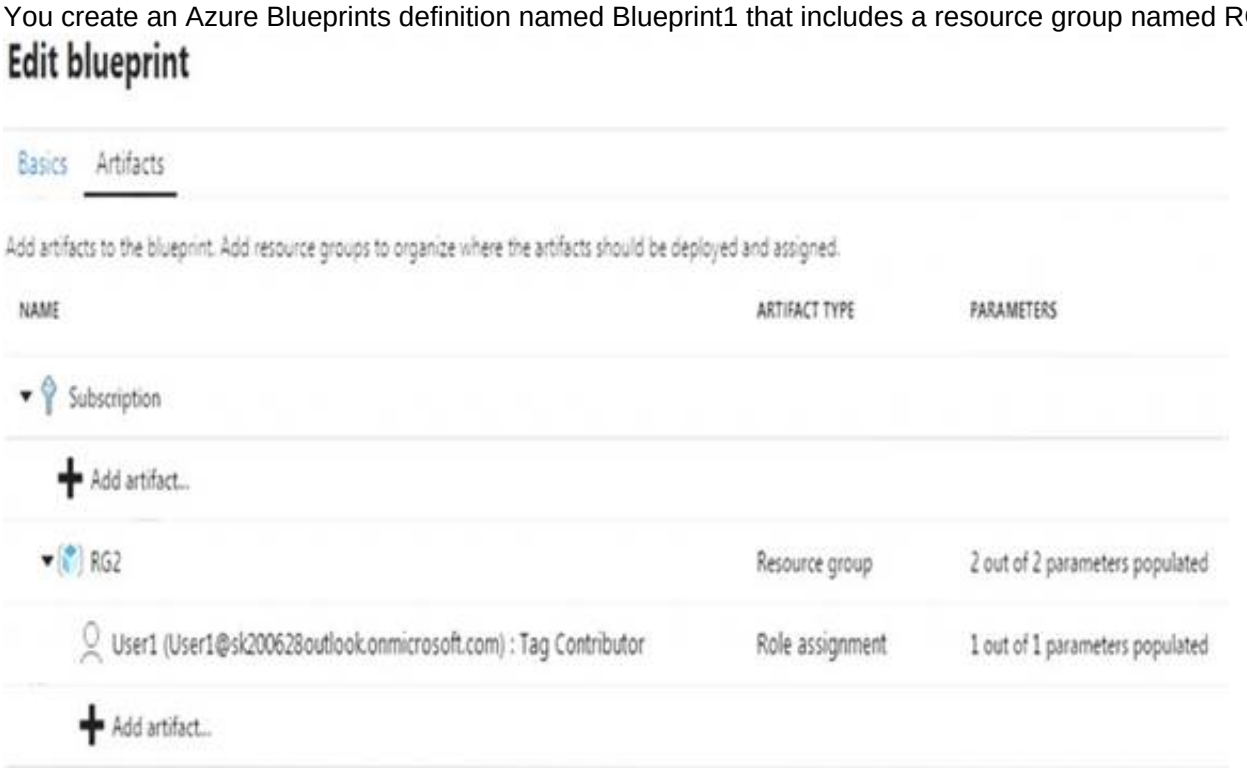
NEW QUESTION 289
- (Exam Topic 4)
Lab Task
use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password. place your cursor in the Enter password box and click on the password below. Azure Username: Userl -28681041@ExamUsers.com
Azure Password: GpOAe4@lDg
If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only: Lab Instance: 28681041
Task 8
You need to prevent HTTP connections to the rg1lod28681041n1 Azure Storage account.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
To prevent HTTP connections to the rg1lod28681041n1 Azure Storage account, you can follow these steps:
- In the Azure portal, search for and select the storage account named rg1lod28681041n1.
- In the left pane, select Firewalls and virtual networks.
- In the Firewalls and virtual networks pane, select Selected networks.
- In the Selected networks pane, select Add existing virtual network.
- In the Add existing virtual network pane, select the virtual network that does not allow HTTP connections.
- Select Add.

NEW QUESTION 290
- (Exam Topic 4)
You have an Azure subscription named Subscription1 that contains a resource group named RG1 and a user named User1. User1 is assigned the Owner role for RG1.
You create an Azure Blueprints definition named Blueprint1 that includes a resource group named RG2 as shown in the following exhibit.



You assign Blueprint1 to Subscription1 by using the following settings:
- Lock assignment: Read Only
- Managed Identity: System assigned

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

Statements	Yes	No
A locking mode of Read Only will be assigned to RG1.	○	○
User1 can add tags to RG2.	○	○
You can remove User1 from the Tag Contributor role for RG2.	○	○

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 295
- (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 296
- (Exam Topic 4)
You have an Azure key vault named Vault1 that stores the resources shown in following table.

Name	Type
Key1	Key
Secret1	Secret
Cert1	Certificate

Which resources support the creation of a rotation policy?

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

Answer: C

NEW QUESTION 301
- (Exam Topic 4)
You have an Azure subscription that contains a Microsoft Defender External Attack Surface Management (Defender EASM) resource named EASM1. EASM1 has discovery enabled and contains several inventory assets.
You need to identify which inventory assets are vulnerable to the most critical web app security risks. Which Defender EASM dashboard should you use?

A. Attack Surface Summary
B. GDPRCompliance
C. Security Posture
D. OWASPToplO

Answer: D

NEW QUESTION 306
- (Exam Topic 4)
You have an Azure virtual machine named VM1.
From Azure Security Center, you get the following high-severity recommendation: “Install endpoint protection solutions on virtual machine”.
You need to resolve the issue causing the high-severity recommendation. What should you do?

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

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-endpoint-protection

NEW QUESTION 310
- (Exam Topic 4)
You are configuring and securing a network environment.
You deploy an Azure virtual machine named VM1 that is configured to analyze network traffic. You need to ensure that all network traffic is routed through VM1.
What should you configure?

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

Answer: C

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

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

NEW QUESTION 314
- (Exam Topic 4)
You are configuring an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry.
You need to use the auto-generated service principal to authenticate to the Azure Container Registry. What should you create?

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

Answer: B

Explanation:
When you create an AKS cluster, Azure also creates a service principal to support cluster operability with other Azure resources. You can use this auto-generated service principal for authentication with an ACR registry. To do so, you need to create an Azure AD role assignment that grants the cluster's service principal access to the container registry.
References:
https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-auth-aks

NEW QUESTION 315
- (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 319
- (Exam Topic 4)
You have an Azure Sentinel workspace that contains an Azure Active Directory (Azure AD) connector, an Azure Log Analytics query named Query1 and a playbook named Playbook1.
Query1 returns a subset of security events generated by Azure AD.
You plan to create an Azure Sentinel analytic rule based on Query1 that will trigger Playbook1. You need to ensure that you can add Playbook1 to the new rule.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Create the rule and set the type to:

Fusion
Microsoft Security incident creation
Scheduled

Configure the playbook to include:

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 321
- (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/listKevs/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 326
- (Exam Topic 4)
Your company has an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
The company develops an application named App1. App1 is registered in Azure AD.
You need to ensure that App1 can access secrets in Azure Key Vault on behalf of the application users. What should you configure?

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

Answer: B

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

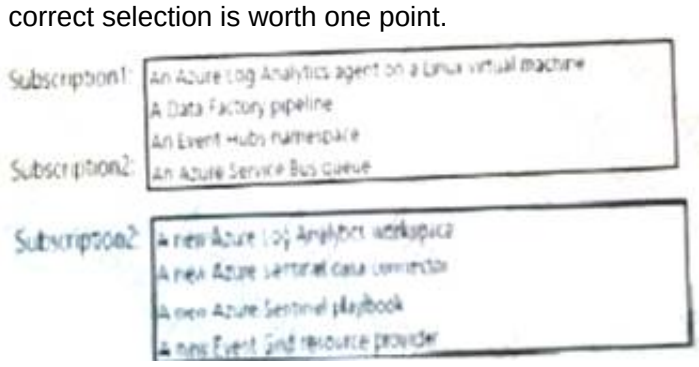
NEW QUESTION 328
- (Exam Topic 4)
You have an Azure subscription named Subcription1 that contains the resources shown in the following table.

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 Subcription2 that contains the following resources:
- An Azure Sentinel workspace
- An Azure Event Grid instance

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

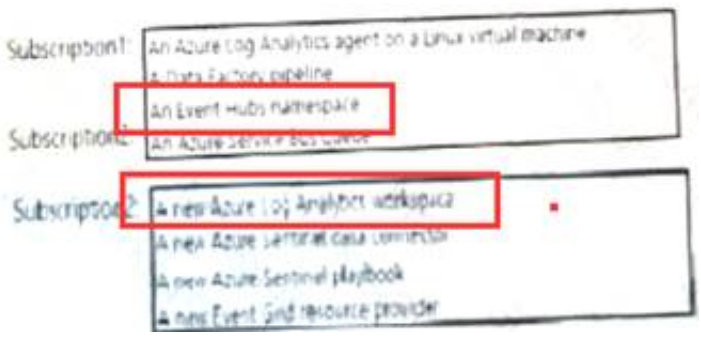
Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area



NEW QUESTION 330
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.

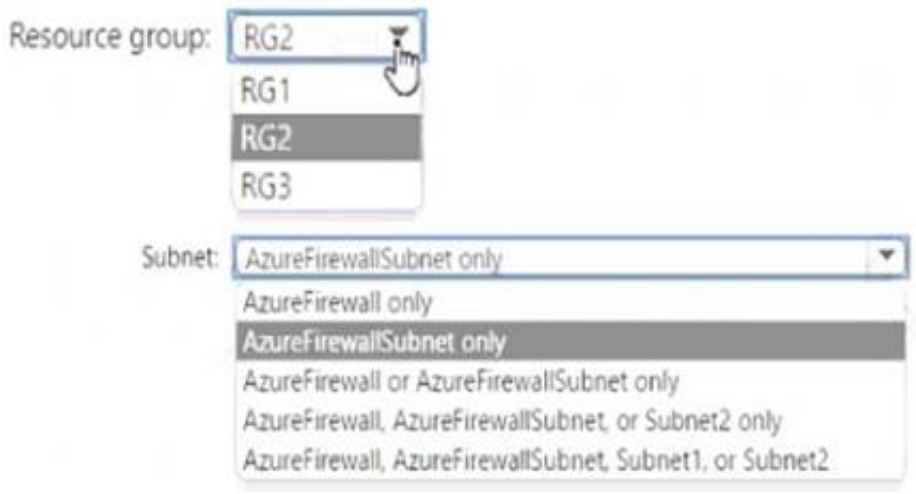
Name	Type	Location	In resource group
RG1	Resource group	East US	*Not applicable*
RG2	Resource group	West US	*Not applicable*
RG3	Resource group	Central US	*Not applicable*
VNet1	Virtual network	Central US	RG2

VNet1 contains the subnets shown in the following table.

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

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

Answer Area

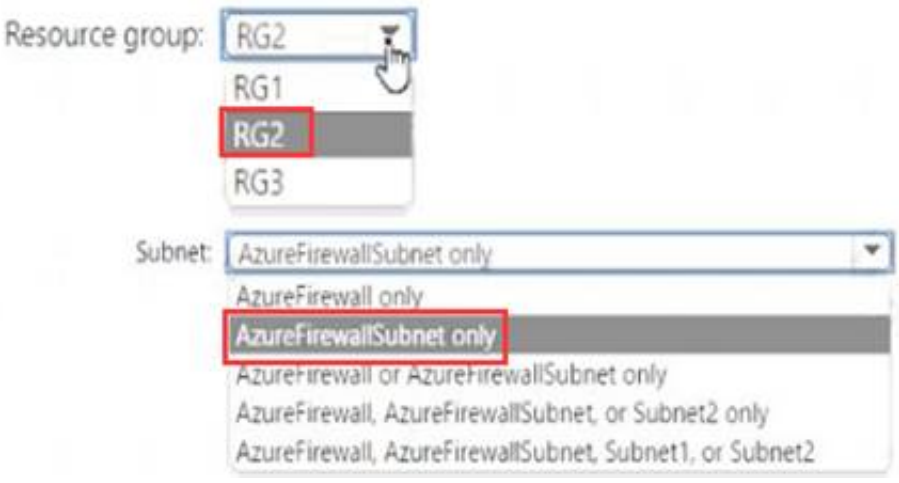


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 335
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Role
Admin1	Global administrator
Admin2	Group administrator
Admin3	User administrator

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 340
- (Exam Topic 4)
You have an Azure key vault named KeyVault1 that contains the items shown in the following table.

Name	Type
Item1	Key
Item2	Secret
Policy1	Access policy

In KeyVault, the following events occur in sequence:
- Item1 is deleted
- Administrator enables soft delete
- Item2 and Policy1 are deleted.

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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
NO. Policies cannot be recovered YES, Item1 is permanently deleted
NO, You cannot use the same name cause Item2 is in Seoft-deleted status https://docs.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview

NEW QUESTION 345
- (Exam Topic 4)
From Azure Security, you create a custom alert rule.
You need to configure which users will receive an email message when the alert is triggered. What should you do?

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

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups

NEW QUESTION 347
- (Exam Topic 4)
You have an Azure subscription. That contains the virtual machines shown in the following table.

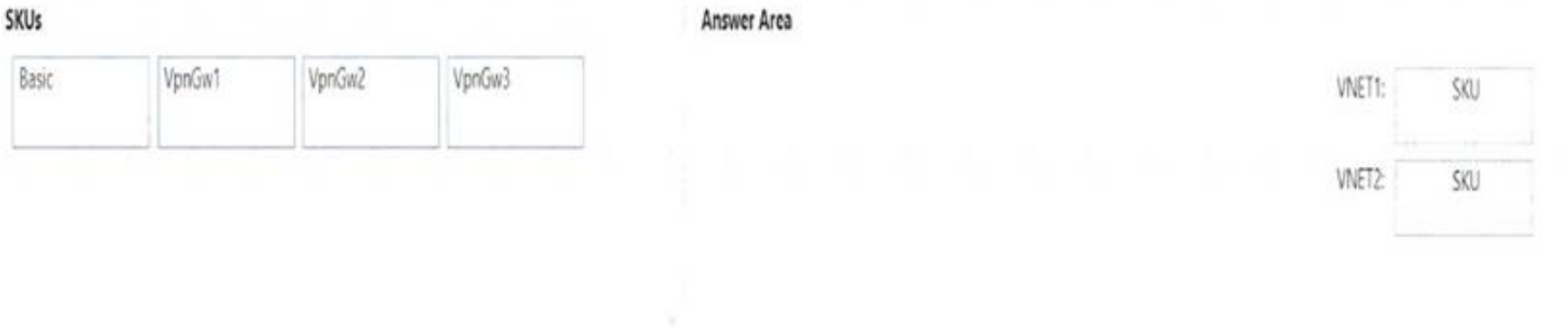
Name	Operating system
Computer1	Windows 10
Computer2	Windows Server 2022
Computer3	SUSE Linux Enterprise Server (SLES)

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

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

Answer: B

NEW QUESTION 352
- (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



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 355
- (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 357
- (Exam Topic 4)
You have an Azure subscription named Subscription1 that contains a resource group named RG1 and the users shown in the following table.

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

You perform the following tasks:
- Assign User1 the Network Contributor role for Subscription1.
- Assign User2 the Contributor role for RG1.

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

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

Answer: A

NEW QUESTION 362
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

az-500 Practice Exam Features:

* az-500 Questions and Answers Updated Frequently

* az-500 Practice Questions Verified by Expert Senior Certified Staff

* az-500 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* az-500 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year