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 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 3
- (Exam Topic 4)
You have an Azure subscription that contains the virtual machines shown in the following table.
Subnet1 and Subnet2 have a network security group {NSG). The NSG has an outbound rule that has the following configurations:
• Port; Any
• Source: Any
• Priority: 100
• Action: Deny
• Protocol: Any
• Destination: Storage
The subscription contains a storage account named storage1.
You create a private endpoint named Private1 that has the following settings:
• Resource type: Microsoft.Storage/storageAccounts
• Resource: storage1
• Target sub-resource: blob
• Virtual network: VNet1
• Subnet: Subnet1
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
From VM2, you can create a container in storage1.	○	○
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 4
- (Exam Topic 4)
Lab Task
Task 5
A user named Debbie has the Azure app installed on her mobile device.
You need to ensure that debbie@contoso.com is alerted when a resource lock is deleted.

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 5
- (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.)

Protection
Contoso1812 - Azure Information Protection

Protections settings

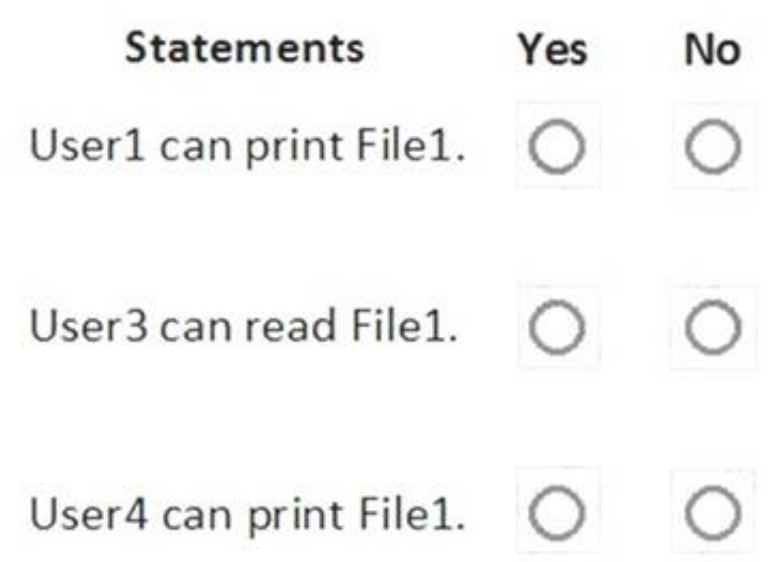
Azure (cloud key) | HYOK (AD RMS)

Select the protection action type
- (●) Set permissions
- ( ) Set user-defined permissions (Preview)

USERS	PERMISSIONS
AuthenticatedUsers	Viewer
User1@contoso1812.onmicrosoft.com	Co-Author
User2@contoso1812.onmicrosoft.com	Reviewer

+Add permissions

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

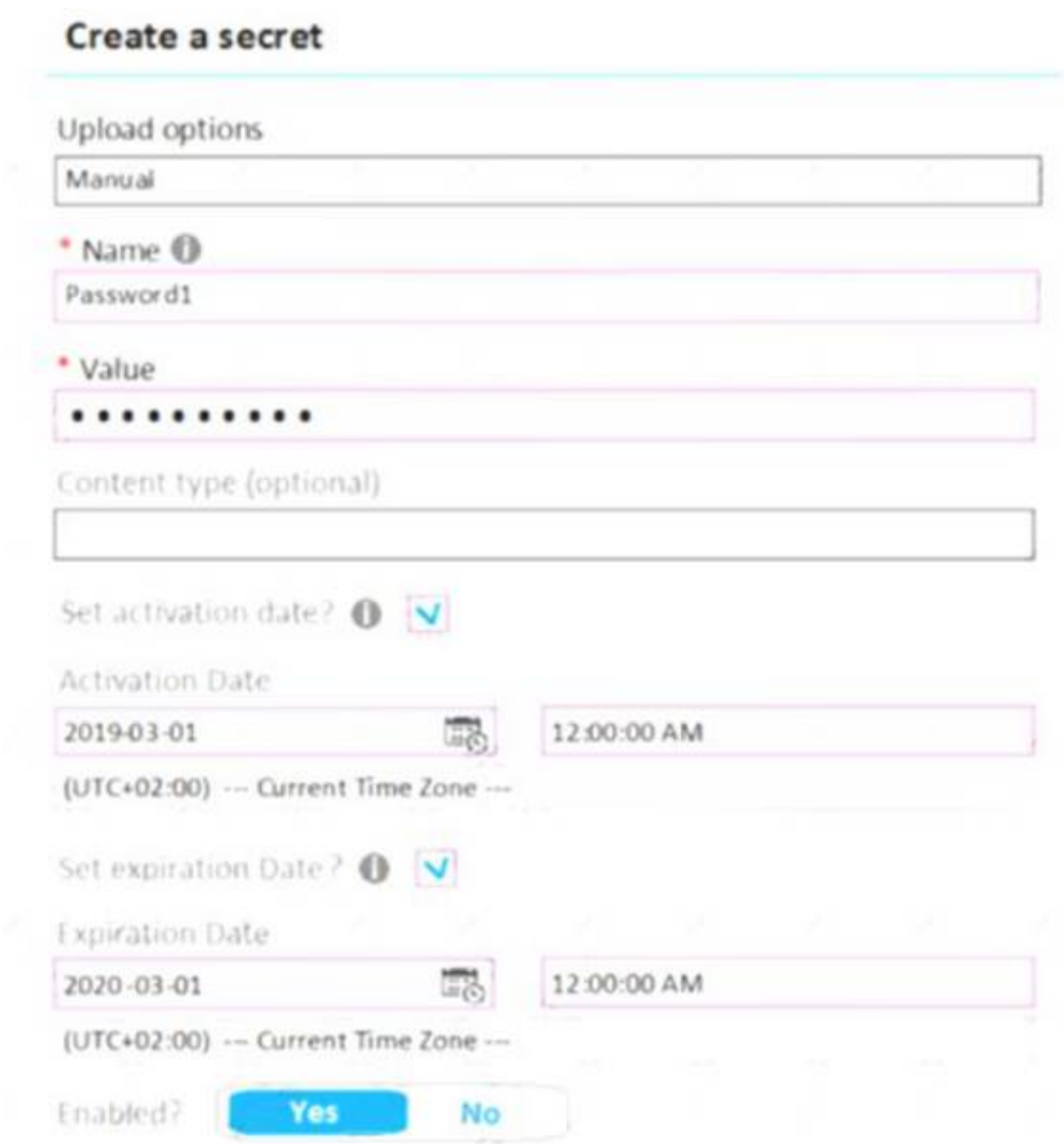
Answer: A

Explanation:

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

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

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



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 7
- (Exam Topic 4)
You have an Azure subscription that contains a web app named App1 and an Azure key vault named Vault1. You need to configure App1 to store and access the secrets in Vault1.
How should you configure App1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Configure App1 to authenticate by using a:

- Key
- Certificate
- Passphrase
- User-assigned managed identity
- System-assigned managed identity

Configure a Key Vault reference for App1 from the:

- Extensions blade
- General settings tab
- TLS/SSL settings blade
- Application settings tab

A. Mastered
B. Not Mastered

Answer: A

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

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

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

Answer: C

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

NEW QUESTION 9
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.

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

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

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

You plan to deploy Azure SQL databases by using an Azure Resource Manager (ARM) template. The databases will be configured as shown in the following table.
NOTE: Each correct selection is worth one point.
Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

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

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

Resource Providers
- Microsoft.Compute
- Microsoft.Network
- Microsoft.Security
- Microsoft.Solutions

Answer Area
- Role1:
- Role2:

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Resource Providers
- Microsoft.Compute
- Microsoft.Network
- Microsoft.Security
- Microsoft.Solutions

Answer Area
- Role1: Microsoft.Network
- Role2: Microsoft.Network

NEW QUESTION 10
- (Exam Topic 4)
You have an Azure subscription that contains three storage accounts, an Azure SQL managed instance named SQL and three Azure SQL databases. The storage accounts are configured as shown in the following table.
SQ11 has the following settings:
• Auditing: On
• Audit tog destination: storage1
The Azure SQL databases are configured as shown in the following table.
Answer Area

Statements	Yes	No
Audit events for DB1 are written to storage1.	○	○
Audit events for DB2 are written to storage1 and storage2.	○	○
Storage3 can be used as an audit log destination for DB3.	○	○

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 15
- (Exam Topic 4)
You have an Azure Sentinel workspace that has the following data connectors:
- Azure Active Directory Identity Protection
- Common Event Format (CEF)
- Azure Firewall

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

Azure Active Directory Identity Protection: ▼
- AzureDiagnostics
- CommonSecurityLog
- SecurityAlert
- SecurityEvent
- Syslog

Azure Firewall: ▼
- AzureDiagnostics
- CommonSecurityLog
- SecurityAlert
- SecurityEvent
- Syslog

CEF: ▼
- AzureDiagnostics
- CommonSecurityLog
- SecurityAlert
- SecurityEvent
- Syslog

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application, table Description automatically generated

NEW QUESTION 16
- (Exam Topic 4)
You are testing an Azure Kubernetes Service (AKS) cluster. The cluster is configured as shown in the exhibit. (Click the Exhibit tab.)

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

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

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

Answer: A

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

NEW QUESTION 17
- (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 20
- (Exam Topic 4)
You have an Azure subscription named Subscription1.
You need to view which security settings are assigned to Subscription1 by default. Which Azure policy or initiative definition should you review?

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

Answer: B

Explanation:
Reference:

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

NEW QUESTION 23
- (Exam Topic 4)
You have an Azure subscription that contains a resource group named RG1. RG1 contains a virtual machine named VM1 that uses Azure Active Directory (Azure AD) authentication.
You have two custom Azure roles named Role1 and Role2 that are scoped to RG1.
The permissions for Role1 are shown in the following JSON code.

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

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

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

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

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

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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

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

NEW QUESTION 25
- (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 29
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Subscription. The subscription contains 50 virtual machines that run Windows Server 2012 R2 or Windows Server 2016.
You need to deploy Microsoft Antimalware to the virtual machines. Solution: You connect to each virtual machine and add a Windows feature. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Microsoft Antimalware is deployed as an extension and not a feature. References:
https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware

NEW QUESTION 30
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.

Name	Type
RG1	Resource group
VM1	Virtual machine

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

Answer Area

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

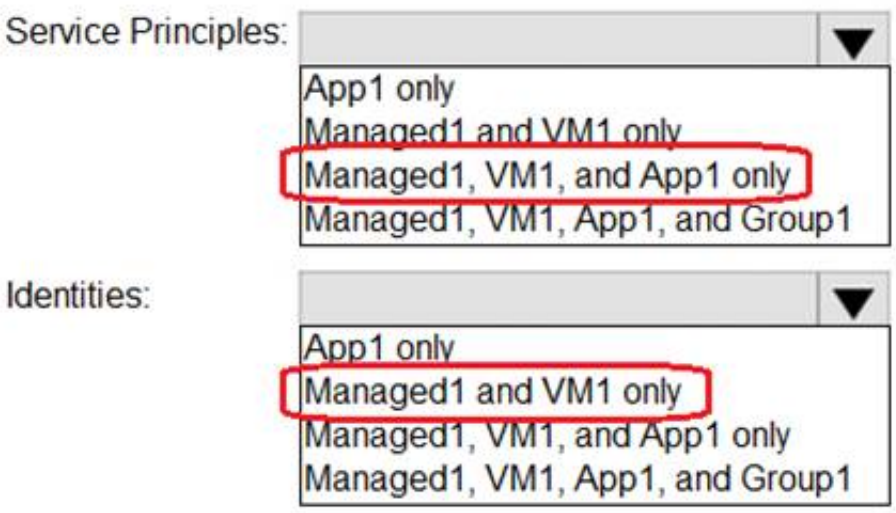
Identities:
- App1 only
- Managed1 and VM1 only
- Managed1, VM1, and App1 only
- Managed1, VM1, App1, and Group1

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 35
- (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 37
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant and a root management group. You create 10 Azure subscriptions and add the subscriptions to the rout management group.
You need to create an Azure Blueprints definition that will be stored in the root management group. What should you do first?

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

Answer: B

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

NEW QUESTION 40
- (Exam Topic 4)
You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

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

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

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

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

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 43
- (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 44
- (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 48
- (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 52
- (Exam Topic 4)
You have an Azure subscription that contains an Azure SQL database named sql1. You plan to audit sql1.
You need to configure the audit log destination. The solution must meet the following requirements:
- Support querying events by using the Kusto query language.
- Minimize administrative effort. What should you configure?

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

Answer: C

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

NEW QUESTION 56
- (Exam Topic 4)
Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD). Azure AD Connect is installed on a domain member server named Server1.
You need to ensure that a domain administrator for the adatum.com domain can modify the synchronization options. The solution must use the principle of least privilege.
Which Azure AD role should you assign to the domain administrator?

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

Answer: B

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

NEW QUESTION 58
- (Exam Topic 4)
You have an Azure subscription that contains an instance of Azure Firewall Standard named AzFWL You need to identify whether you can use the following features with AzFW1:
• TLS inspection
• Threat intelligence
• The network intrusion detection and prevention systems (IDPS) What can you use?

A. TLS inspection only
B. threat intelligence only
C. TLS inspection and the IDPS only
D. threat intelligence and the IDPS only
E. TLS inspection, threat intelligence, and the IDPS

Answer: E

NEW QUESTION 62
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a hybrid configuration of Azure Active Directory (Azure AD).
You have an Azure HDInsight cluster on a virtual network.
You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials. You need to configure the environment to support the planned authentication.
Solution: You deploy Azure Active Directory Domain Services (Azure AD DS) to the Azure subscription. Does this meet the goal?

A. Yes
B. No

Answer: A

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

NEW QUESTION 63
- (Exam Topic 4)
You have an Azure subscription that contains a storage account and an Azure web app named App1. App1 connects to an Azure Cosmos DB database named Cosmos1 that uses a private endpoint named
Endpoint1. Endpoint1 has the default settings.
You need to validate the name resolution to Cosmos1. Which DNS zone should you use?

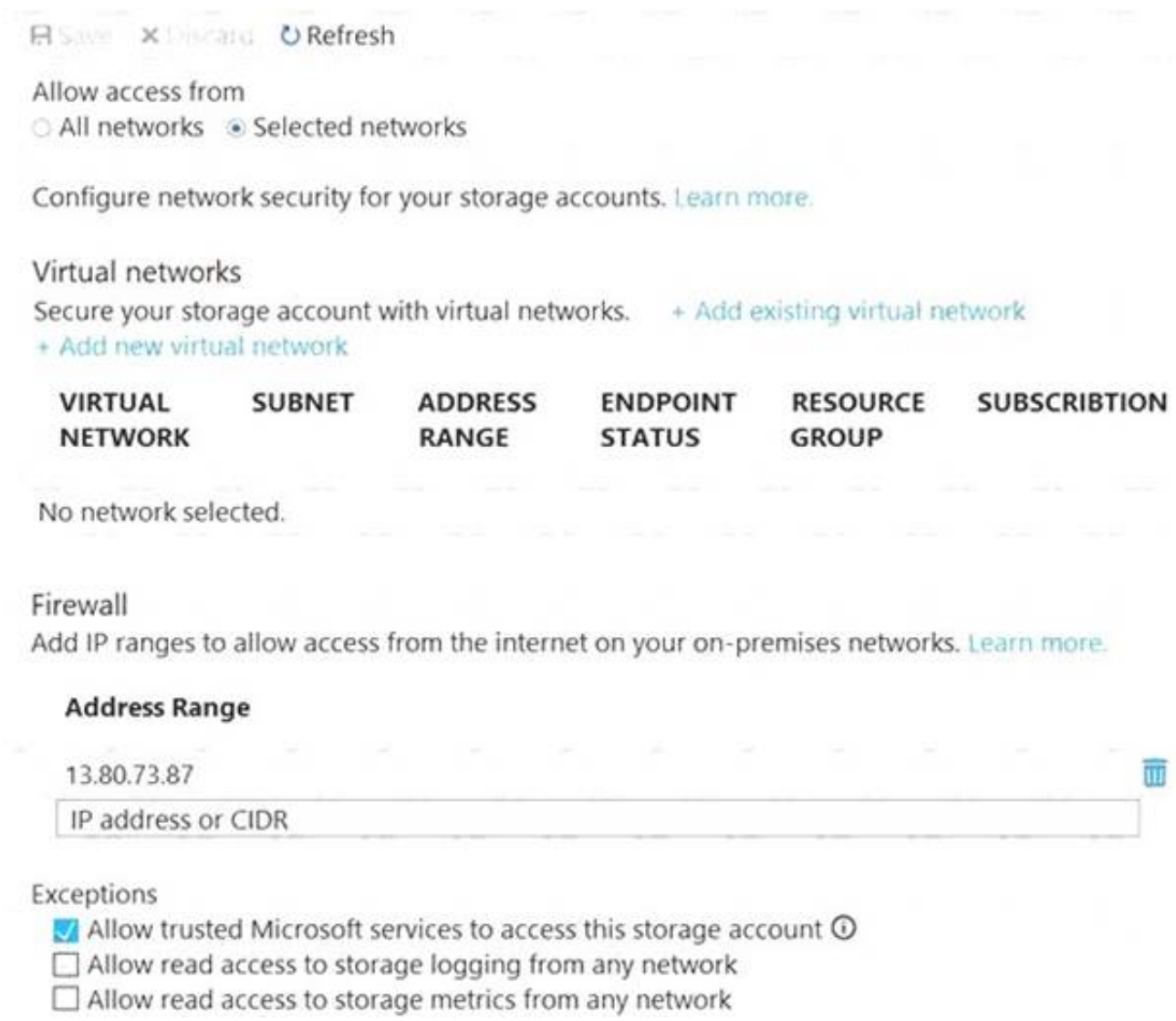
A. Endpoint1. Privatelink,blob,core,windows,net
B. Endpoint1. Privatelink,database,azure,com
C. Endpoint1. Privatelink,azurewebsites,net
D. Endpoint1. Privatelink,documents,azure,com

Answer: D

NEW QUESTION 66
- (Exam Topic 4)
You have an Azure subscription that contains the virtual machines shown in the following table.

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

Subnet1 and Subnet2 have a Microsoft.Storage service endpoint configured.
You have an Azure Storage account named storageacc1 that is configured as shown in the following exhibit.



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

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 69
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Member of	Mobile phone	Multi-factor authentication (MFA) status
User1	Group1	123 555 7890	Disabled
User2	Group1, Group2	*None*	Enabled
User3	Group1	123 555 7891	Required

You create and enforce an Azure AD Identity Protection user risk policy that has the following settings:
- Assignment: Include Group1, Exclude Group2
- Conditions: Sign-in risk of Medium and above
- Access: Allow access, Require password change

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

Statements	Yes	No
If User1 signs in from an unfamiliar location, he must change his password.	○	○
If User2 signs in from an anonymous IP address, she must change her password.	○	○
If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Yes
User1 is member of Group1. Sign in from unfamiliar location is risk level Medium. Box 2: Yes
User2 is member of Group1. Sign in from anonymous IP address is risk level Medium. Box 3: No
Sign-ins from IP addresses with suspicious activity is low. Note:

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

Azure AD Identity protection can detect six types of suspicious sign-in activities:

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

These six types of events are categorized in to 3 levels of risks – High, Medium & Low: References:
http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/

NEW QUESTION 74
- (Exam Topic 4)
You have an Azure subscription that contains the Azure virtual machines shown in the following table.

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

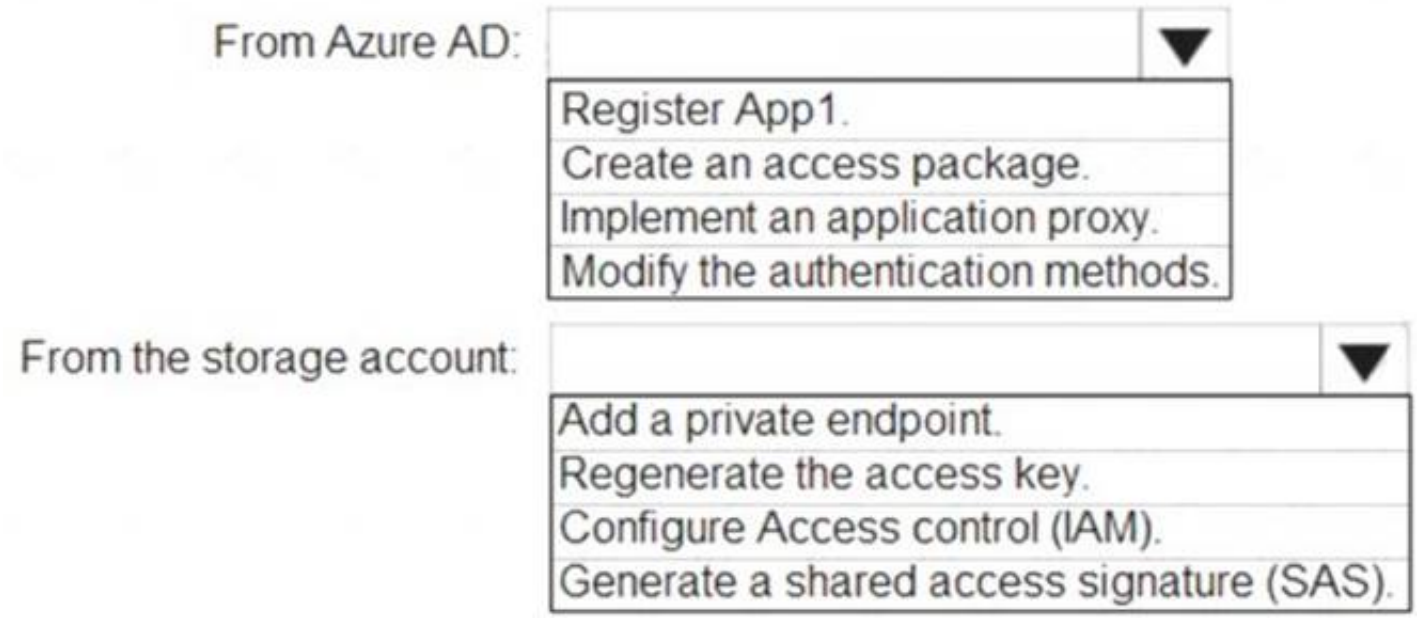
You create an MDM Security Baseline profile named Profile1.
You need to identify to which virtual machines Profile1 can be applied. Which virtual machines should you identify?

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

Answer: A

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

NEW QUESTION 78
- (Exam Topic 4)
You have an Azure Storage account that contains a blob container named container1 and a client application named App1.
You need to enable App1 access to container1 by using Azure Active Directory (Azure AD) authentication.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 82
- (Exam Topic 4)
You have an Azure subscription that uses Azure Active Directory (Azure AD) Privileged Identity Management (PIM).
A PIM user that is assigned the User Access Administrator role reports receiving an authorization error when performing a role assignment or viewing the list of assignments.
You need to resolve the issue by ensuring that the PIM service principal has the correct permissions for the subscription. The solution must use the principle of least privilege.
Which role should you assign to the PIM service principle?

A. Contributor
B. User Access Administrator
C. Managed Application Operator
D. Resource Policy Contributor

Answer: B

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 90
- (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 95
- (Exam Topic 4)
You have an Azure subscription that uses Azure AD Privileged Identity Management (PIM). A user named User1 is eligible for the Billing administrator role.
You need to ensure that the role can only be used for a maximum of two hours. What should you do?

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

Answer: B

NEW QUESTION 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

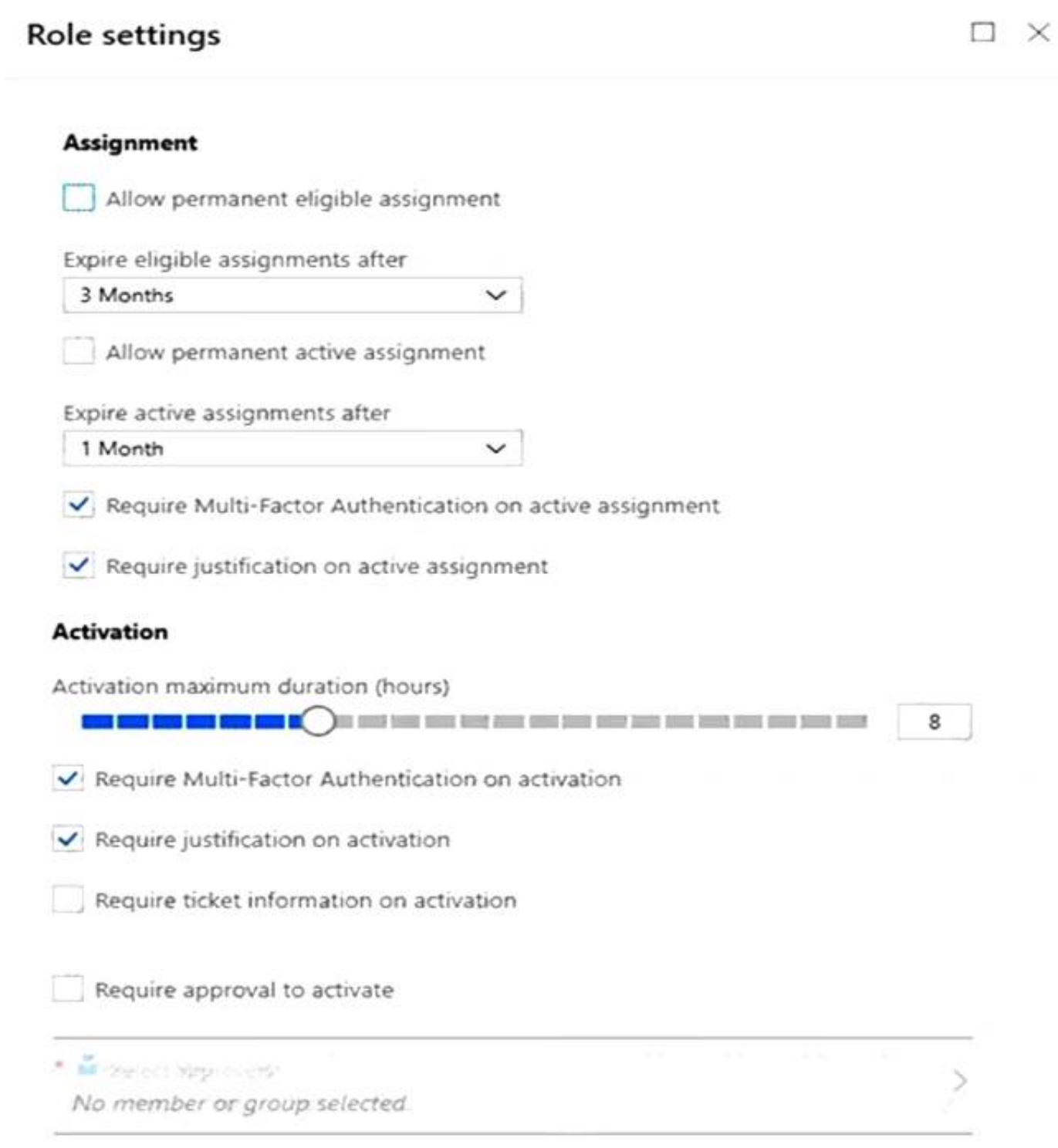
Answer: A

Explanation:

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

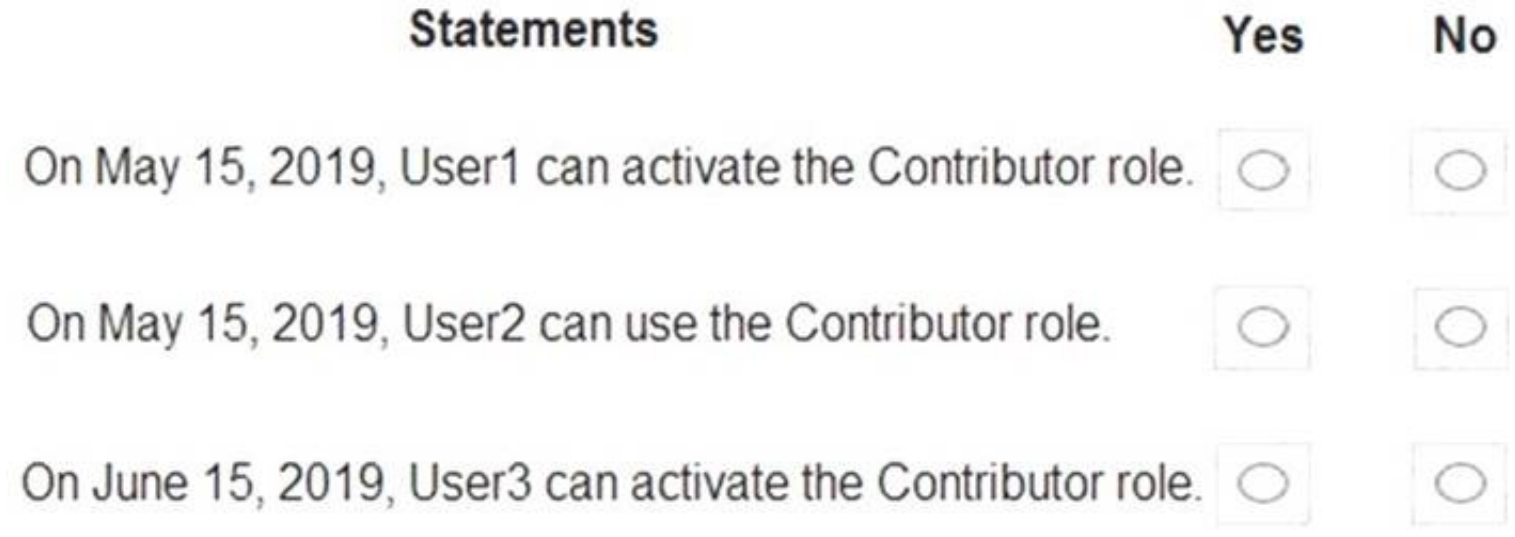
In Azure AD Privileged Identity Management (PIM), the Role settings for the Contributor role are configured as shown in the exhibit. (Click the Exhibit tab.)



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 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

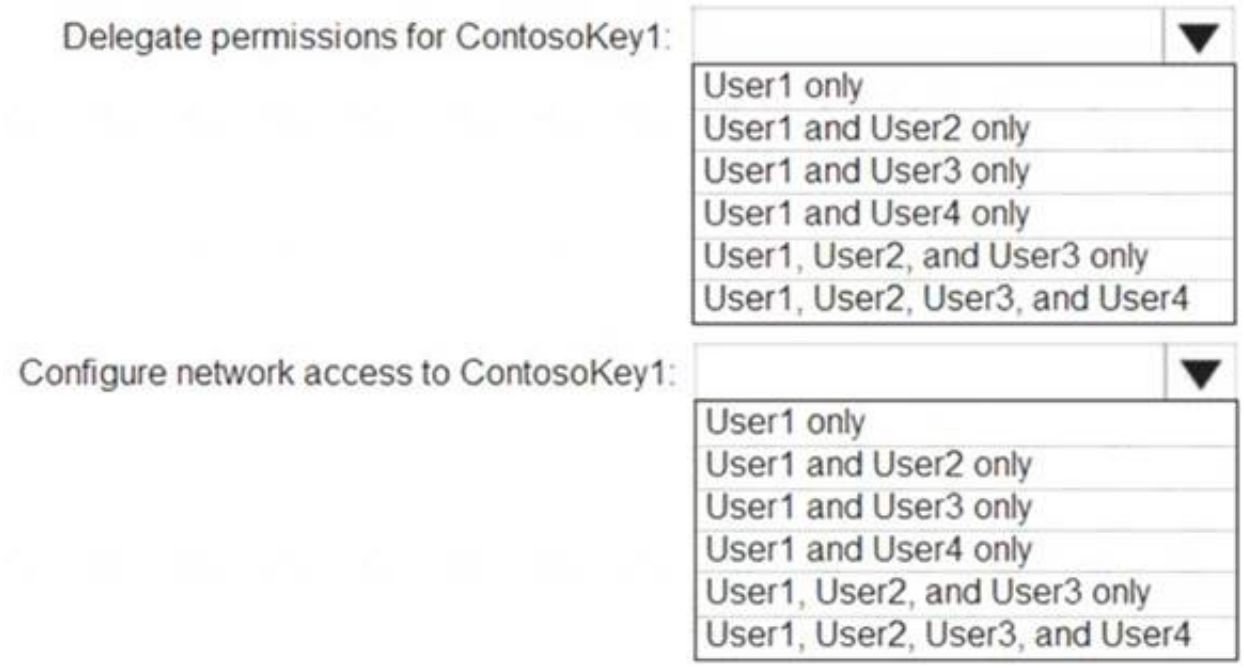
Answer: C

NEW QUESTION 110
- (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 111
- (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 116
- (Exam Topic 4)
You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	In resource group
8372f433-2dcd-4361-b5ef-5b188fed87d0	Subscription ID	*Not applicable*
RG1	Resource group	*Not applicable*
VM1	Virtual machine	RG1
VNET1	Virtual network	RG1
storage	Storage account	RG1
User1	User account	*Not applicable*

You create an Azure role by using the following JSON file.

```
{
    "properties":{
        "roleName": "Role1",
    "description": "",
    "assignableScopes": [
        "/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0",
        "/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0/resourceGroups/RG1"
    ],
        "permissions": [
            {
                "actions": [
                    "Microsoft.Compute/*"
                ],
                "notActions": [],
                "dataActions": [],
                "notDataActions": []
            }
        ]
    }
}
```

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

Statements	Yes	No
User1 can create a new virtual machine in RG1.	○	○
User can modify the properties of storage1.	○	○
User1 can attach the network interface of VM1 to VNET1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
NO NO NO
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#compute

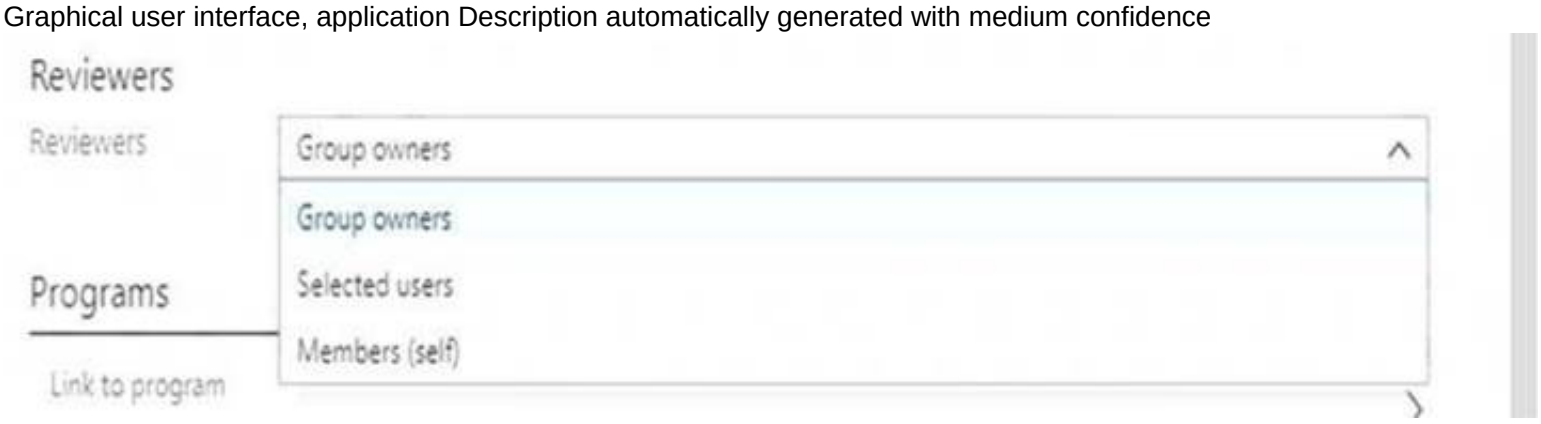
NEW QUESTION 121
- (Exam Topic 4)
You have been tasked with configuring an access review, which you plan to assigned to a new collection of reviews. You also have to make sure that the reviews can be reviewed by resource owners.
You start by creating an access review program and an access review control. You now need to configure the Reviewers.
Which of the following should you set Reviewers to?

A. Selected users.
B. Members (Self).
C. Group Owners.
D. Anyone.

Answer: C

Explanation:

In the Reviewers section, select either one or more people to review all the users in scope. Or you can select to have the members review their own access. If the resource is a group, you can ask the group owners to review.
Graphical user interface, application Description automatically generated with medium confidence



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

NEW QUESTION 122
- (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 127
- (Exam Topic 4)
You onboard Azure Sentinel. You connect Azure Sentinel to Azure Security Center.
You need to automate the mitigation of incidents in Azure Sentinel. The solution must minimize administrative effort.
What should you create?

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

Answer: B

NEW QUESTION 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?

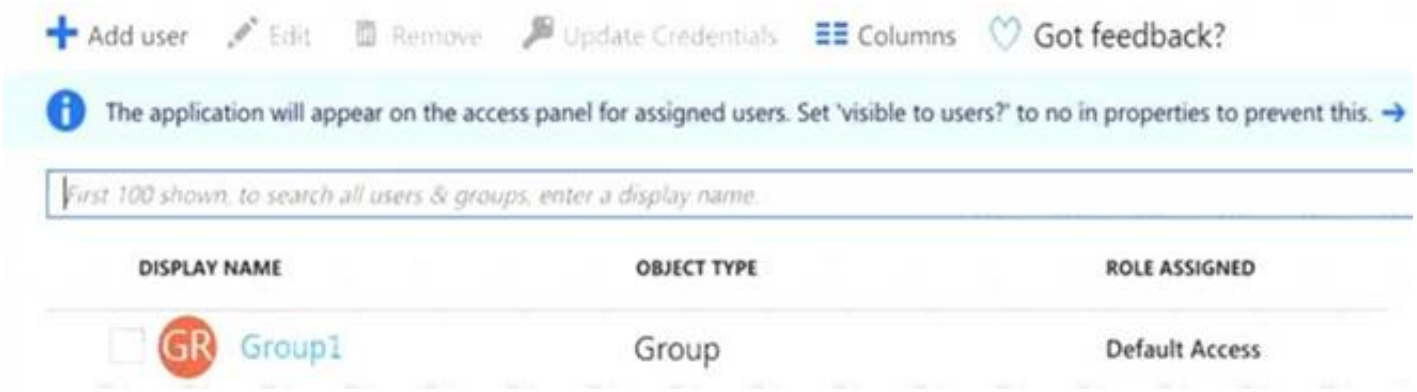
A. Securing the Cloud
B. Sensitive Services
C. attack surface composition
D. Attack Surface Priorities

Answer: C

NEW QUESTION 132
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains the resources shown in the following table.

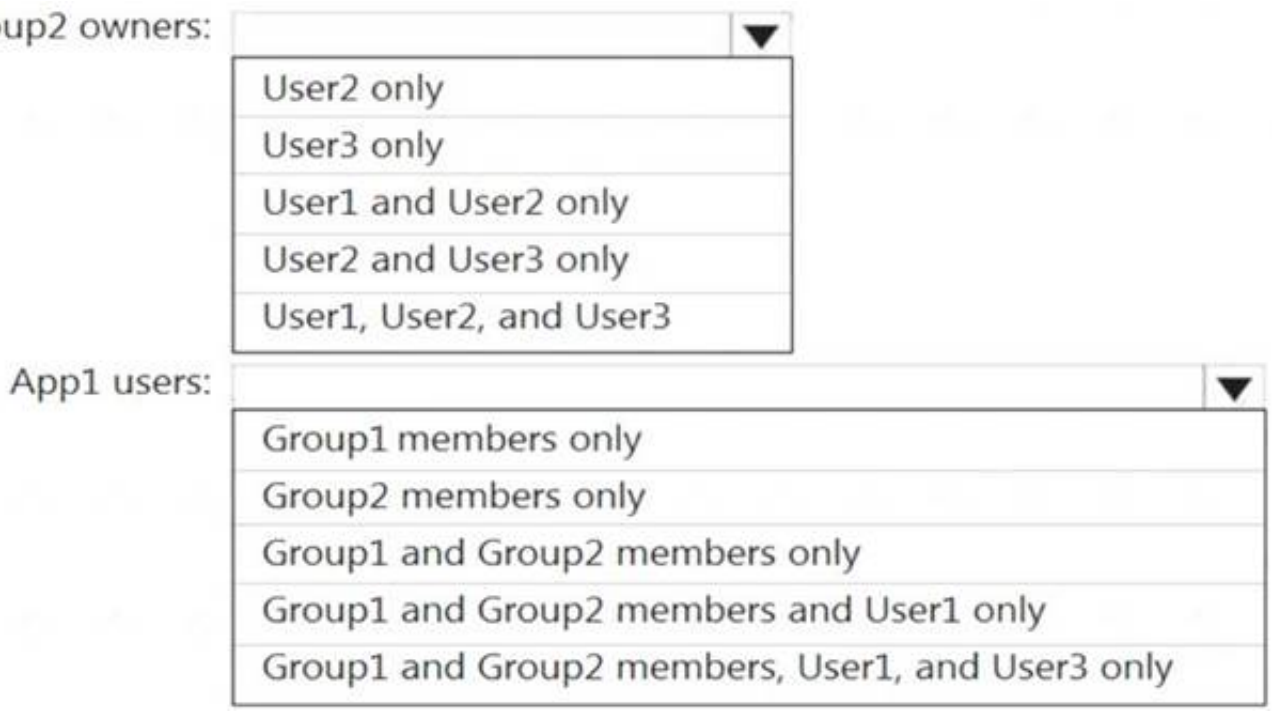
Name	Type
User1	User
User2	User
User3	User
Group1	Security group
Group2	Security group
App1	Enterprise application

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



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

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

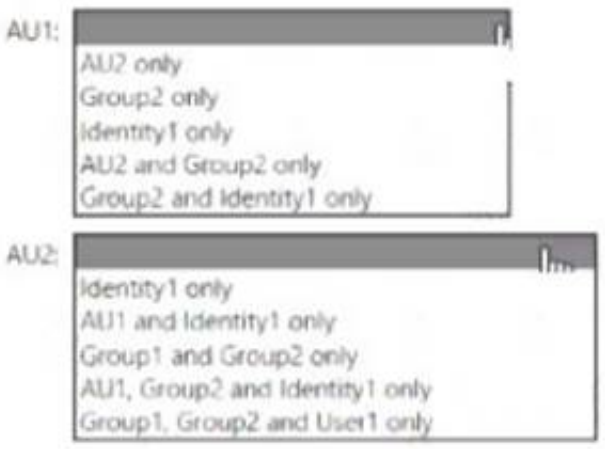
Explanation:
Reference:

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

NEW QUESTION 135
- (Exam Topic 4)
You have an Azure subscription that has a managed identity named identity and is linked to an Azure Active Directory (Azure AD) tenant. The tenant contains the resources shown in the following table.
Which resources can be added to AUI and AU2? To answer, select the appropriate options in the answer area.

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

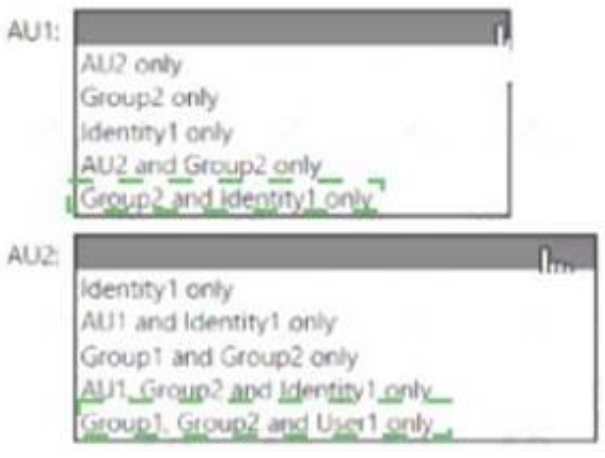
Which resources can be added to AU1 and AU2? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.
Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area



NEW QUESTION 136
- (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)

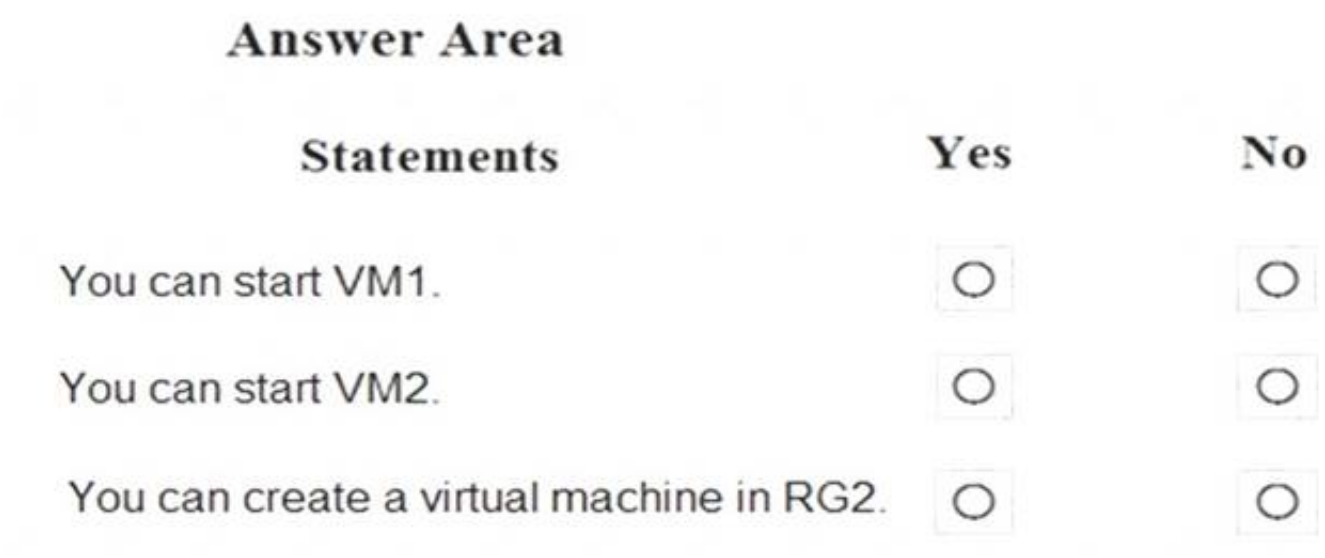
You create the Azure policies shown in the following table.

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.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 137
- (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 138
- (Exam Topic 4)
You create an alert rule that has the following settings:
- Resource: RG1
- Condition: All Administrative operations
- Actions: Action groups configured for this alert rule: ActionGroup1
- Alert rule name: Alert1

You create an action rule that has the following settings:
- Scope: VM1
- Filter criteria: Resource Type = "Virtual Machines"
- Define on this scope: Suppression
- Suppression config: From now (always)
- Name: ActionRule1

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 139
- (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?

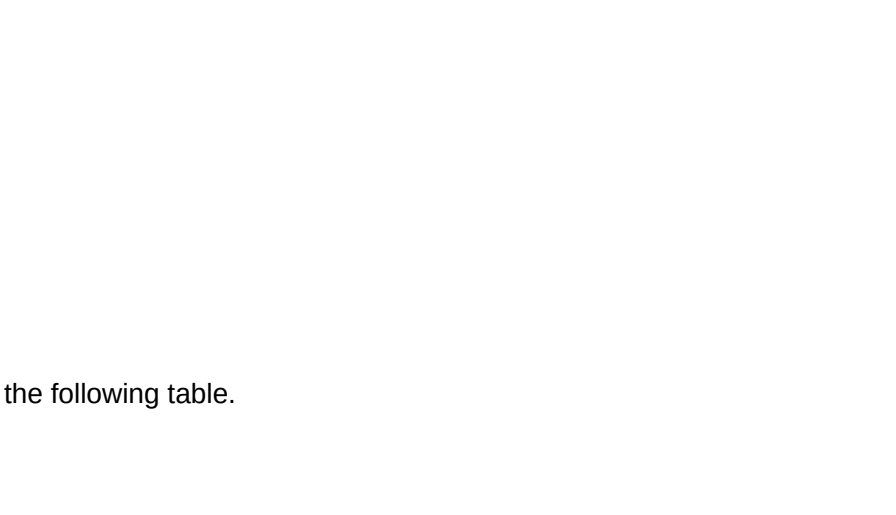
A. 1
B. 2
C. 3
D. 4

Answer: D

NEW QUESTION 141
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.

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

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

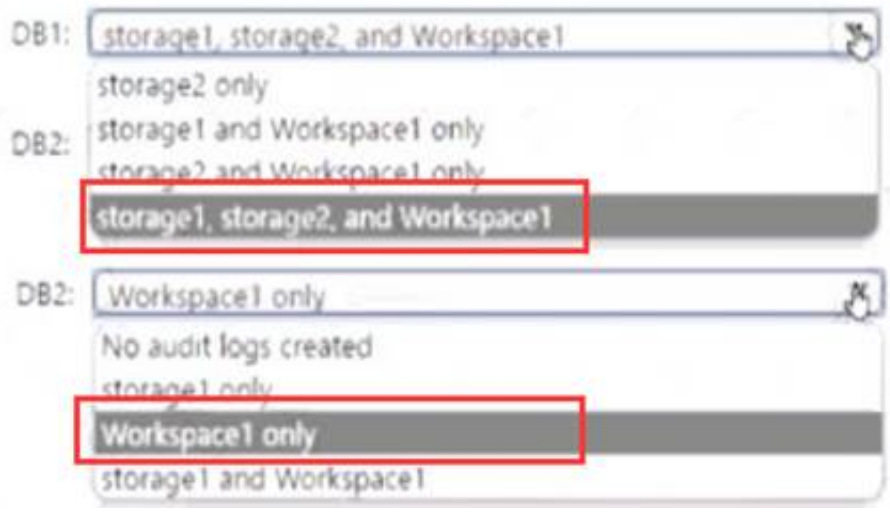


A. Mastered
B. Not Mastered

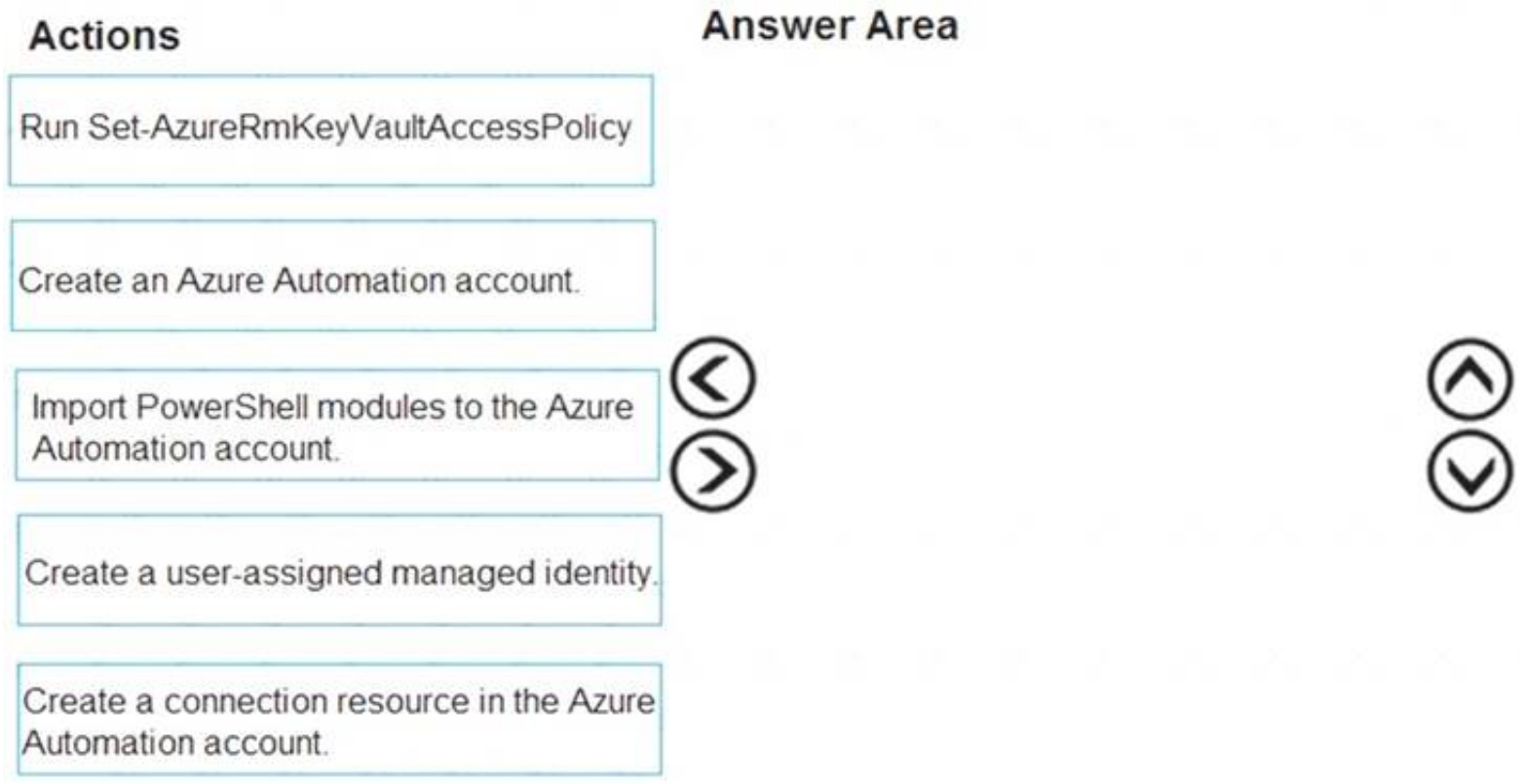
Answer: A

Explanation:

Answer Area



NEW QUESTION 142
- (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
}
```

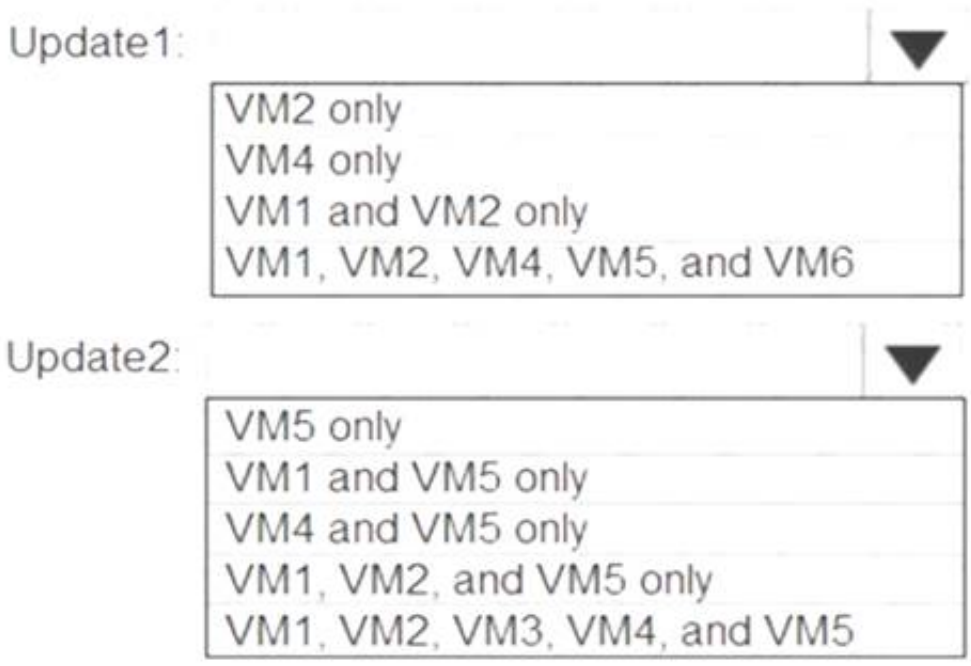
References:
https://www.rahulpnath.com/blog/accessing-azure-key-vault-from-azure-runbook/

NEW QUESTION 146
- (Exam Topic 4)

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

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

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



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 149
- (Exam Topic 4)
You have an Azure subscription that uses Microsoft Defender for Cloud. You have accounts for the following cloud services:
• Alibaba Cloud
• Amazon Web Services (AWS)
• Google Cloud Platform (GCP)
What can you add to Defender for Cloud?

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

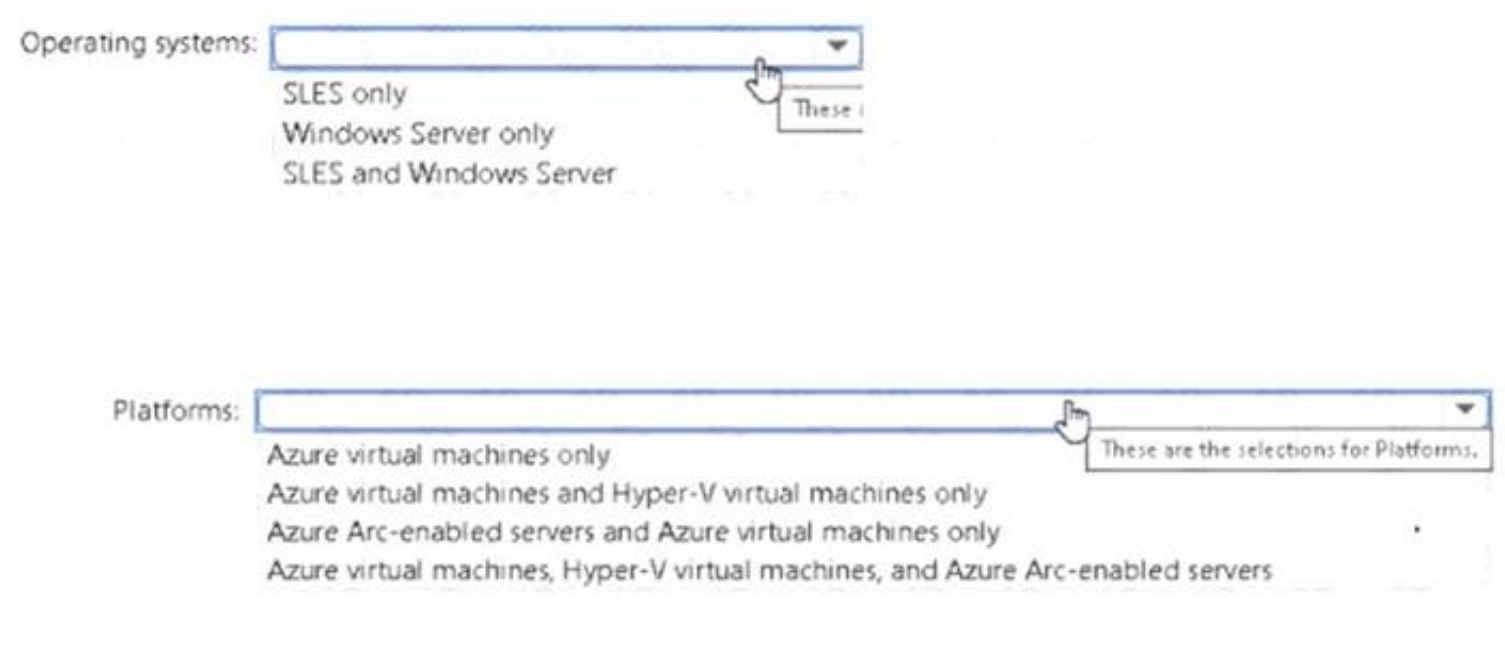
Answer: A

NEW QUESTION 150
- (Exam Topic 4)
Your on-premises network contains the servers shown in the following table.

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

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

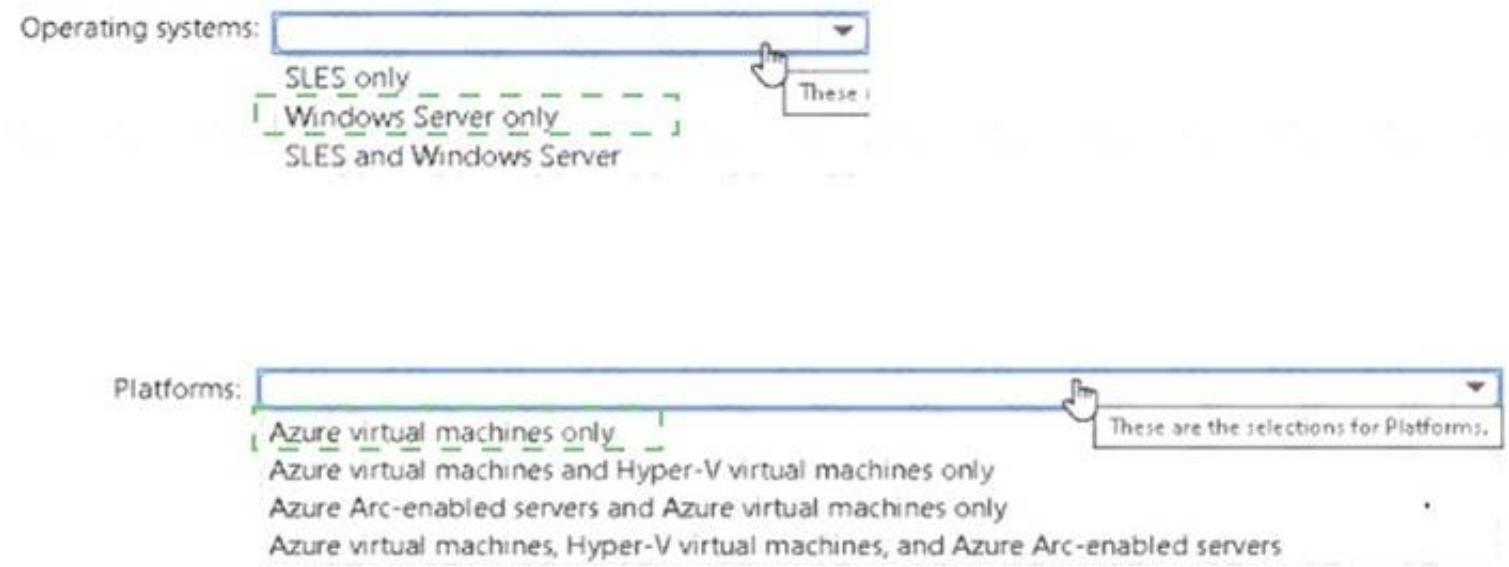
area.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 155
- (Exam Topic 4)
You have an Azure subscription that contains a virtual network. The virtual network contains the subnets shown in the following table.

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

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

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

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

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

Answer: C

Explanation:
An NSG needs to be enabled, either at the VM level or the subnet level. Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time

NEW QUESTION 157
- (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 162
- (Exam Topic 4)
You have an Azure subscription named Sub1 that contains the storage accounts shown in the following table

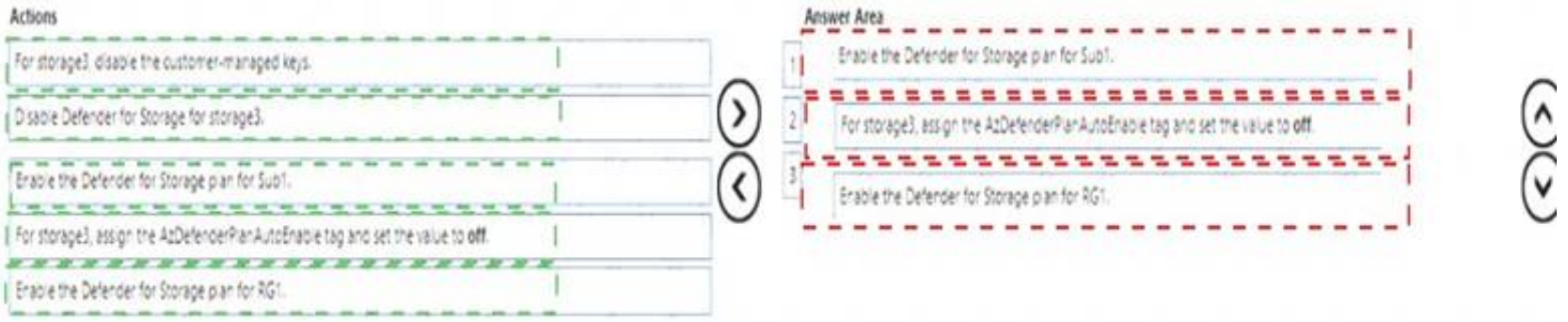
Name	Resource group
storage1	RG1
storage2	RG1
storage3	RG2

The storage3 storage account is encrypted by using customer-managed keys.
YOU need to enable Microsoft Defender for storage to meet the following requirements.
* The storage1 and storage2 account must be include in the defender for storage requirement.
* The storage3 account must be exclude from the Defender for Storage protections.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and them in the correct order.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 166
- (Exam Topic 4)
You have an Azure Container Registry named ContReg1 that contains a container image named image1. You enable content trust for ContReg1.
After content trust is enabled, you push two images to ContReg1 as shown in the following table.

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

Which images are trusted images?

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

Answer: B

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

NEW QUESTION 169
- (Exam Topic 4)
Lab Task
use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password. place your cursor in the Enter password box and click on the password below. Azure Username: Userl -28681041@ExamUsers.com
Azure Password: GpOAe4@lDg
If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only: Lab Instance: 28681041
Task 6
You need to email an alert to a user named adminl@contoso.com if the average CPU usage of a virtual machine named VM1 is greater than 70 percent for a period of 15 minutes.

A. Mastered
B. Not Mastered

Answer: A

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

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

NEW QUESTION 173
- (Exam Topic 4)
You have an Azure subscription and the computers shown in the following table.

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

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

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

Answer: A

NEW QUESTION 177
- (Exam Topic 4)
You have an Azure web app named webapp1.
You need to configure continuous deployment for webapp1 by using an Azure Repo. What should you create first?

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

Answer: B

Explanation:
To use Azure Repos, make sure your Azure DevOps organization is linked to your Azure subscription. Reference:
https://docs.microsoft.com/en-us/azure/app-service/deploy-continuous-deployment

NEW QUESTION 178
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com. The User administrator role is assigned to a user named Admin1.
An external partner has a Microsoft account that uses the user1@outlook.com sign in.
Admin1 attempts to invite the external partner to sign in to the Azure AD tenant and receives the following error message: “Unable to invite user user1@outlook.com Generic authorization exception.”
You need to ensure that Admin1 can invite the external partner to sign in to the Azure AD tenant.
What should you do?

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

Answer: D

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

NEW QUESTION 179
- (Exam Topic 4)
You have a hybrid configuration of Azure Active Directory (Azure AD). You have an Azure SQL Database instance that is configured to support Azure AD authentication.
Database developers must connect to the database instance and authenticate by using their on-premises Active Directory account.
You need to ensure that developers can connect to the instance by using Microsoft SQL Server Management Studio. The solution must minimize authentication prompts.
Which authentication method should you recommend?

A. Active Directory - Password
B. Active Directory - Universal with MFA support
C. SQL Server Authentication
D. Active Directory - Integrated

Answer: D

Explanation:
References:
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure

NEW QUESTION 183
- (Exam Topic 4)
You have the Azure Information Protection conditions shown in the following table.

Name	Pattern	Case sensitivity
Condition1	White	On
Condition2	Black	Off

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

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

You need to identify how Azure Information Protection will label files.
What should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

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

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

A. Mastered
B. Not Mastered

Answer: A

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

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

Box 2: No Label
Automatic classification applies to Word, Excel, and PowerPoint when documents are saved, and apply to Outlook when emails are sent. Automatic classification does not apply to Microsoft Notepad.
References:
https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification

NEW QUESTION 186
- (Exam Topic 4)
You have an Azure subscription that contains a user named UseR1. You need to ensure that UseR1 can perform the following tasks:
• Create groups.
• Create access reviews for role-assignable groups.
• Assign Azure AD roles to groups.
The solution must use the principle of least privilege. Which role should you assign to User1?

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

Answer: C

NEW QUESTION 190
- (Exam Topic 4)
You have an Azure subscription that contains an Azure SQL server named SQL1. SQL1 contains. You need to use Microsoft Defender for Cloud to complete a vulnerability assessment for DB1. What should you do first?

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

Answer: A

NEW QUESTION 195
- (Exam Topic 4)
You have an Azure subscription that contains the subnets shown in the following table.

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

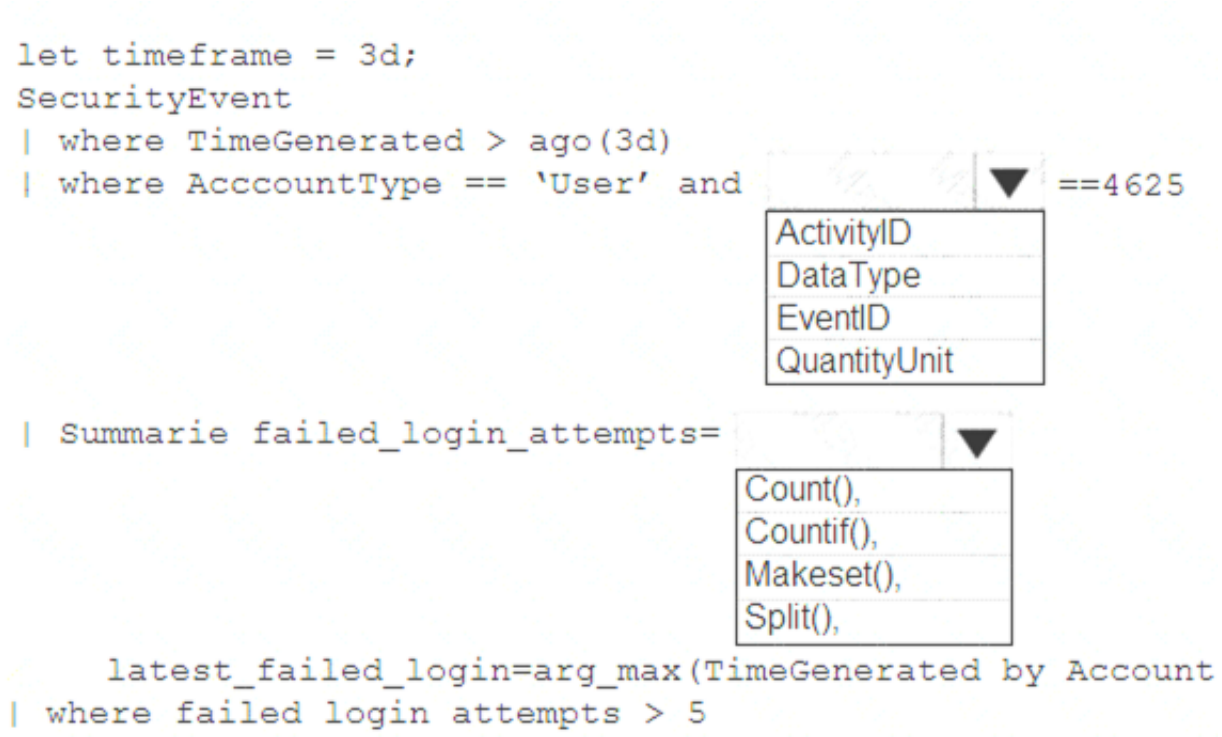
The subscription contains Azure web app named WebApp1 that has the following configurations.
* Region West Us
* Virtual network VNet1
* VNet integration on: Enabled

* Outbound subnet: Subnet11
* Windows plan (West US): ASP1
You plan to deploy an Azure web app named WebApp2 that will have the following settings:
* Region: West US
* VNet integration on-Enabled
* Windows plan (West UAS): WebApp2?
To which subnets can you integrate WebApp2?

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

Answer: C

NEW QUESTION 200
- (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.



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 202
- (Exam Topic 4)
You have an Azure subscription.
You need to deploy an Azure virtual WAN to meet the following requirements:
• Create three secured virtual hubs located in the East US, West US, and North Europe Azure regions.
• Ensure that security rules sync between the regions. What should you use?

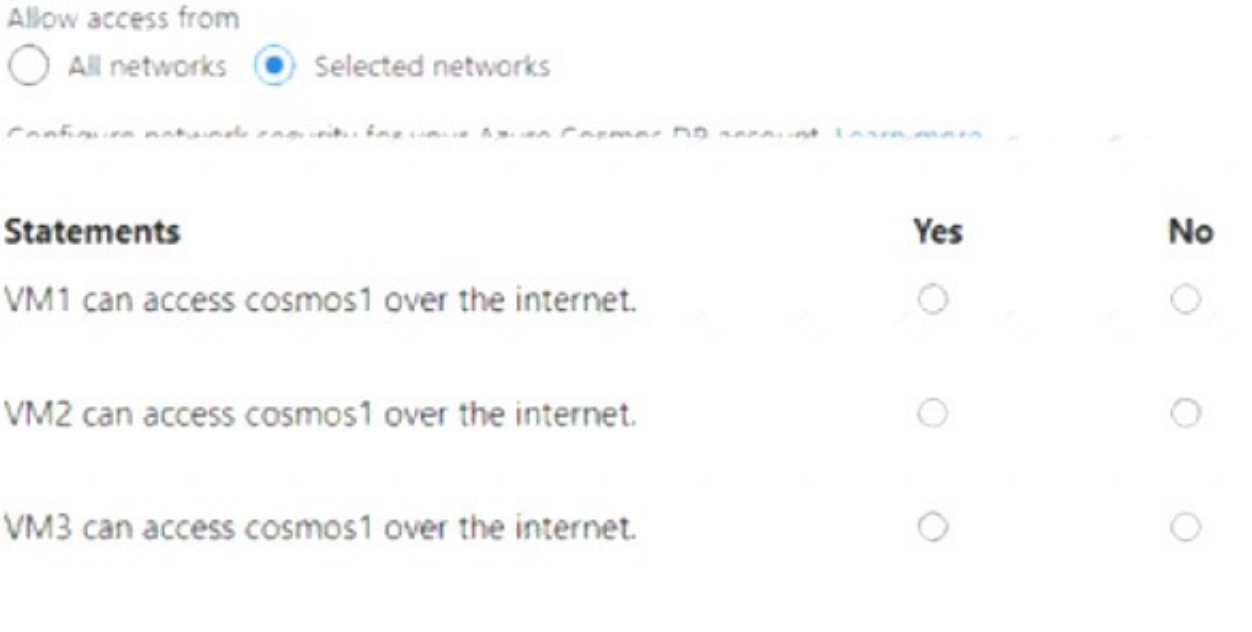
A. Azure Firewall Manager
B. Azure Virtual Network Manager
C. Azure Network Function Manager
D. Azure Front Door

Answer: A

NEW QUESTION 207
- (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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Yes, Yes, No

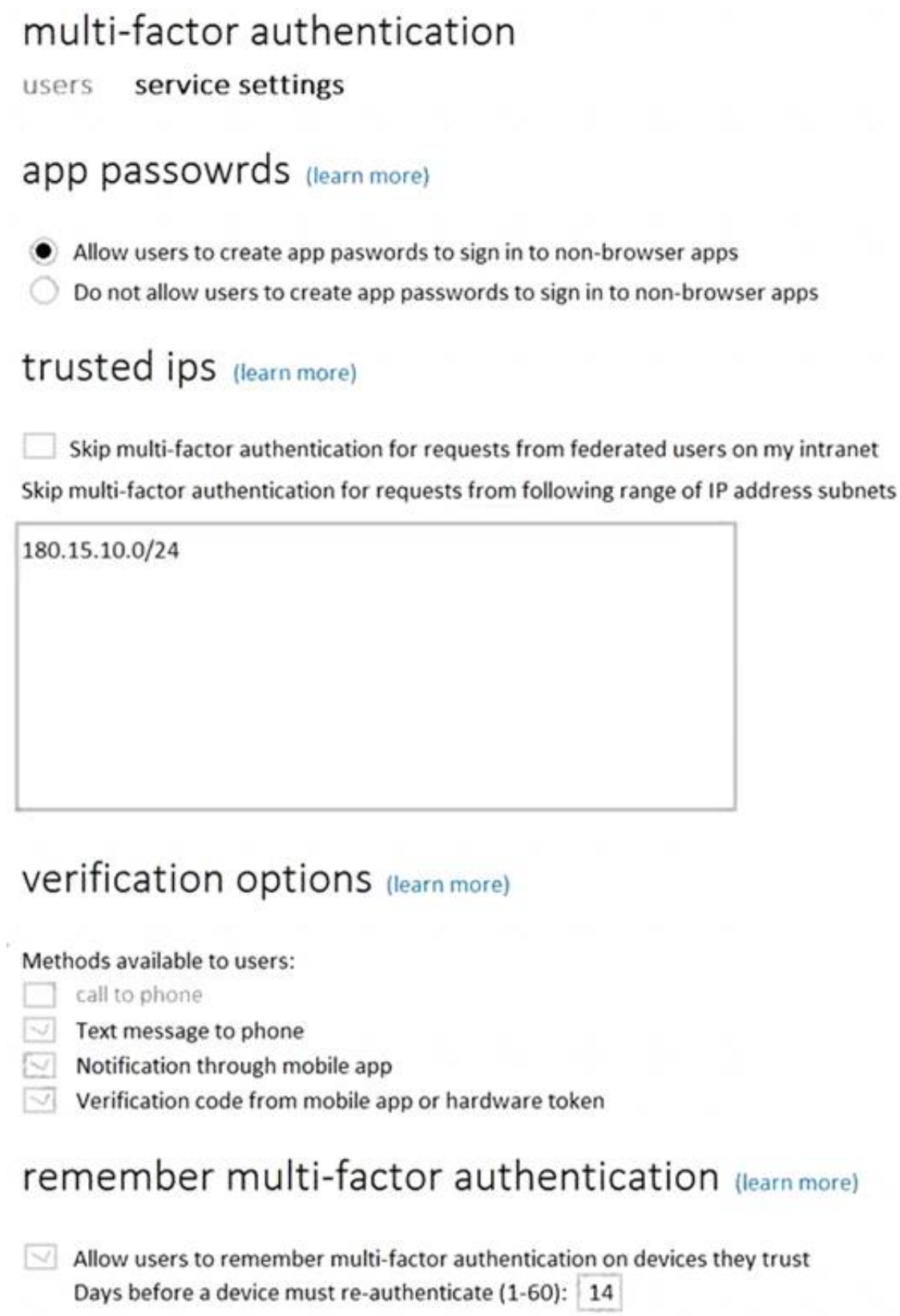
NEW QUESTION 210
- (Exam Topic 4)
You work at a company named Contoso, Ltd. that has the offices shown in the following table.

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.



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:

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.	○	○

NEW QUESTION 214
- (Exam Topic 4)
Lab Task
Task 1
You need to ensure that connections from the Internet to VNET1\subnet0 are allowed only over TCP port 7777. The solution must use only currently deployed resources.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
You need to configure the Network Security Group that is associated with subnet0.
* 1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET1. Alternatively, browse to Virtual Networks in the left navigation pane.
* 2. In the properties of VNET1, click on Subnets. This will display the subnets in VNET1 and the Network Security Group associated to each subnet. Note the name of the Network Security Group associated to Subnet0.
* 3. Type Network Security Groups into the search box and select the Network Security Group associated with Subnet0.
* 4. In the properties of the Network Security Group, click on Inbound Security Rules.
* 5. Click the Add button to add a new rule.
* 6. In the Source field, select Service Tag.
* 7. In the Source Service Tag field, select Internet.
* 8. Leave the Source port ranges and Destination field as the default values (* and All).
* 9. In the Destination port ranges field, enter 7777.
* 10.Change the Protocol to TCP.
* 11.Leave the Action option as Allow.
* 12.Change the Priority to 100.
* 13. Change the Name from the default Port_8080 to something more descriptive such as Allow_TCP_7777_from_Internet. The name cannot contain spaces.
* 14. Click the Add button to save the new rule.

NEW QUESTION 217
- (Exam Topic 4)
Lab Task
use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password. place your cursor in the Enter password box and click on the password below. Azure Username: Userl -28681041@ExamUsers.com
Azure Password: GpOAe4@lDg
If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only: Lab Instance: 28681041
Task 9
You need to ensure that the rg1lod28681041n1 Azure Storage account is encrypted by using a key stored in the KeyVault28681041 Azure key vault.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
To ensure that the rg1lod28681041n1 Azure Storage account is encrypted by using a key stored in the KeyVault28681041 Azure key vault, you can follow these steps:
- In the Azure portal, search for and select the storage account named rg1lod28681041n1.
- In the left pane, select Encryption.
- In the Encryption pane, select Customer-managed key.
- In the Customer-managed key pane, select Select from Key Vault.
- In the Select from Key Vault pane, enter the following information:
- Key vault: Select the KeyVault28681041 Azure key vault.
- Key: Select the key you want to use.
- Select Save.

NEW QUESTION 221
- (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

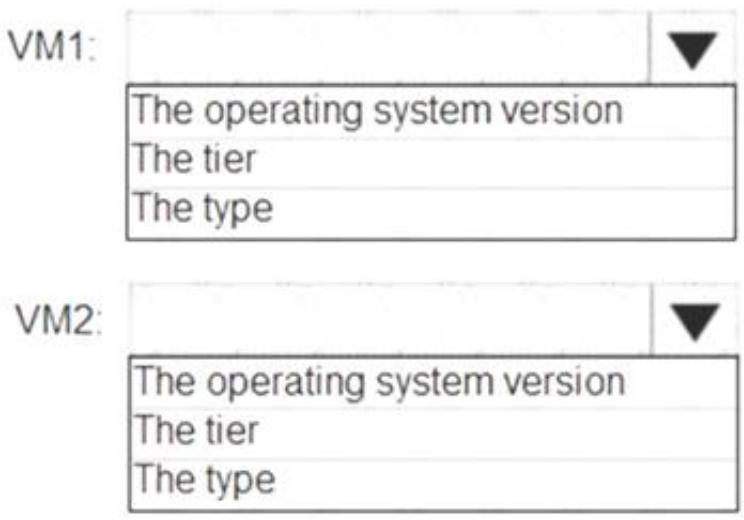
Answer: A

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

NEW QUESTION 223
- (Exam Topic 4)
You have two Azure virtual machines in the East US2 region as shown in the following table.

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

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



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 228
- (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 232
- (Exam Topic 4)
You have an Azure subscription that contains a user named Adminl1 and a virtual machine named VM1. VM1 runs Windows Server 2019 and was deployed by using an Azure Resource Manager template. VM1 is the member of a backend pool of a public Azure Basic Load Balancer.
Admin1 reports that VM1 is listed as Unsupported on the Just in time VM access blade of Azure Security Center.
You need to ensure that Admin1 can enable just in time (JIT) VM access for VM1. What should you do?

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

Answer: D

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

NEW QUESTION 233
- (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 234
- (Exam Topic 4)
You are securing access to the resources in an Azure subscription.
A new company policy states that all the Azure virtual machines in the subscription must use managed disks. You need to prevent users from creating virtual machines that use unmanaged disks.
What should you use?

A. Azure Monitor
B. Azure Policy
C. Azure Security Center
D. Azure Service Health

Answer: B

NEW QUESTION 236
- (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

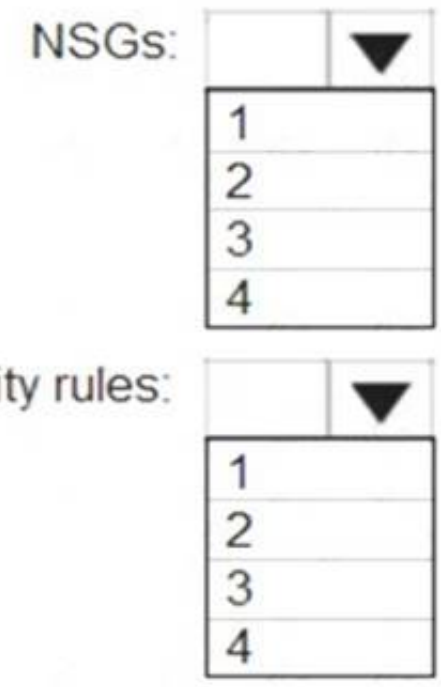
Answer: A

NEW QUESTION 241
- (Exam Topic 4)
You have an Azure subscription named Sub1.
You create a virtual network that contains one subnet. On the subnet, you provision the virtual machines shown in the following table.

Name	Network interface	Application security group assignment	IP address
VM1	NIC1	AppGroup12	10.0.0.10
VM2	NIC2	AppGroup12	10.0.0.11
VM3	NIC3	AppGroup3	10.0.0.100
VM4	NIC4	AppGroup4	10.0.0.200

Currently, you have not provisioned any network security groups (NSGs). You need to implement network security to meet the following requirements:
- Allow traffic to VM4 from VM3 only.
- Allow traffic from the Internet to VM1 and VM2 only.
- Minimize the number of NSGs and network security rules.

How many NSGs and network security rules should you create? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

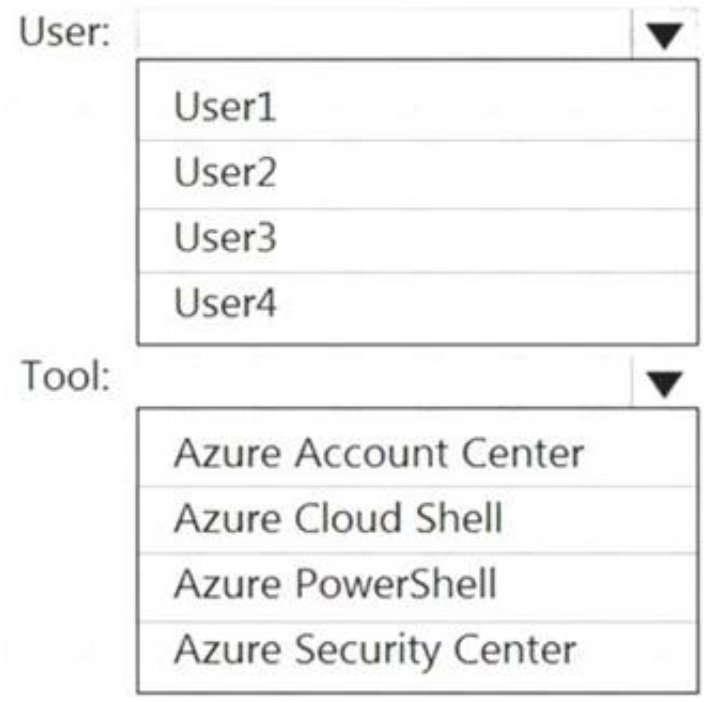
Answer: A

Explanation:
NSGs: 1
Network security rules: 3
Not 2: You cannot specify multiple service tags or application groups) in a security rule. References:
https://docs.microsoft.com/en-us/azure/virtual-network/security-overview

NEW QUESTION 242
- (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 244
- (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 249
- (Exam Topic 4)
From Azure Security Center, you enable Azure Container Registry vulnerability scanning of the images in Registry1.
You perform the following actions:
- Push a Windows image named Image1 to Registry1.
- Push a Linux image named Image2 to Registry1.
- Push a Windows image named Image3 to Registry1.
- Modify Image1 and push the new image as Image4 to Registry1.
- Modify Image2 and push the new image as Image5 to Registry1.

Which two images will be scanned for vulnerabilities? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Image4
B. Image2
C. Image1
D. Image3
E. Image5

Answer: BC

NEW QUESTION 250
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

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

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

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

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

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

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

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 254
- (Exam Topic 4)
You have an Azure subscription that contains a resource group named RG1 and a security group serverless RG1 contains 10 virtual machine, a virtual network VNET1, and a network security group (NSG) named NSG1. ServerAdmins can access the virtual machines by using RDP.
You need to ensure that NSG1 only RDP connections to the virtual for a maximum of 60 minutes when a member of ServerAdmins requests access.
What should you configure?

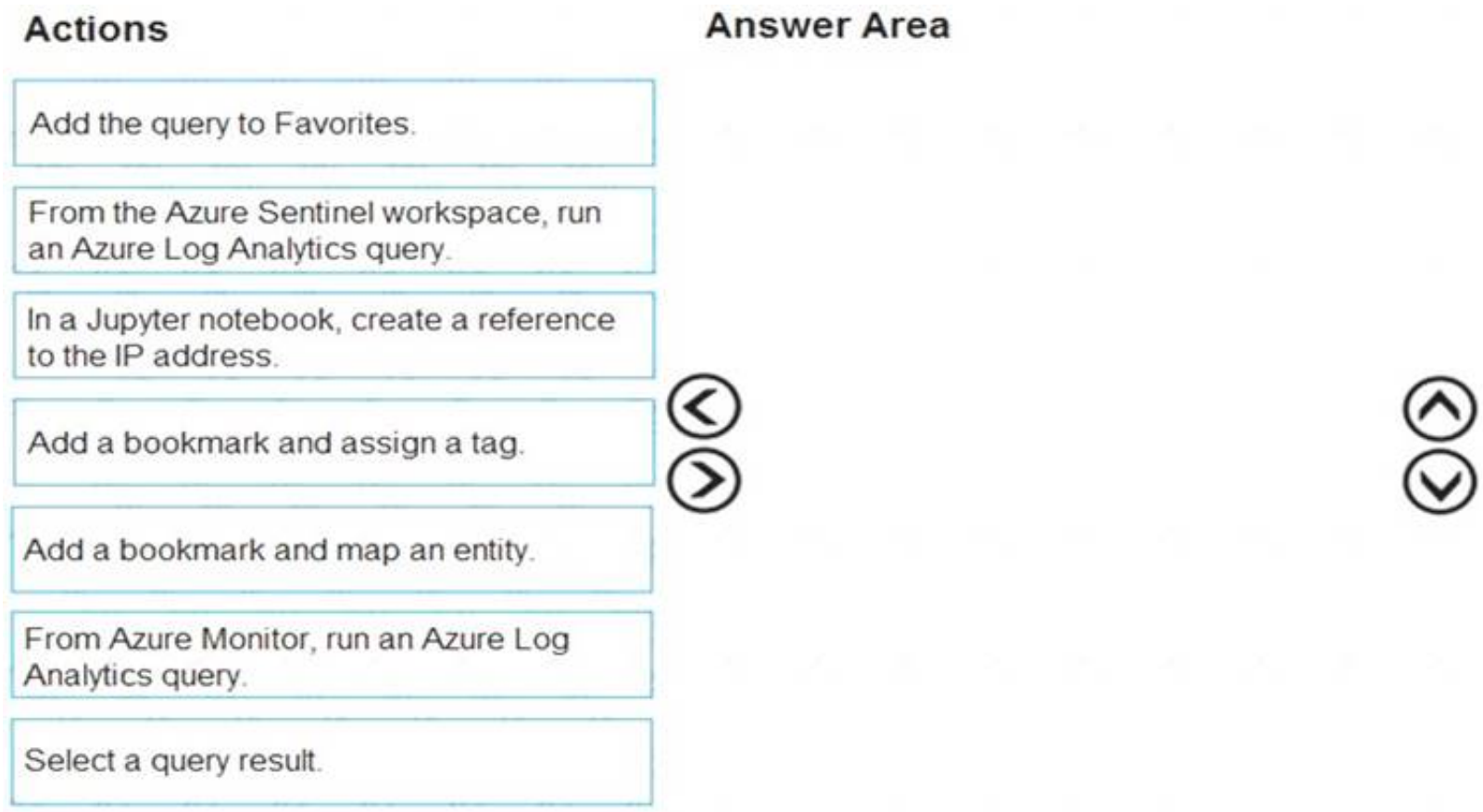
A. an Azure Active Directory (Azure AD) Privileged identity Management (PIM) role assignment.
B. a just in time (JIT) VM access policy in Azure Security Center
C. an azure policy assigned to RG1.
D. an Azure Bastion host on VNET1.

Answer: B

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

NEW QUESTION 257
- (Exam Topic 4)
You have an Azure Sentinel workspace that has an Azure Active Directory (Azure AD) data connector. You are threat hunting suspicious traffic from a specific IP address.

You need to annotate an intermediate event stored in the workspace and be able to reference the IP address when navigating through the investigation graph.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 262
- (Exam Topic 4)
You company has an Azure subscription named Sub1. Sub1 contains an Azure web app named WebApp1 that uses Azure Application Insights. WebApp1 requires users to authenticate by using OAuth 2.0 client secrets.
Developers at the company plan to create a multi-step web test app that preforms synthetic transactions emulating user traffic to Web App1.
You need to ensure that web tests can run unattended. What should you do first?

A. In Microsoft Visual Studio, modify the .webtest file.
B. Upload the .webtest file to Application Insights.
C. Register the web test app in Azure AD.
D. Add a plug-in to the web test app.

Answer: B

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

NEW QUESTION 264
- (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 269
- (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 rt As a result, these questions will not appear in the review screen.
You have an Azure subscription named Sub1.
You have an Azure Storage account named Sa1 in a resource group named RG1.
Users and applications access the blob service and the file service in Sal by using several shared access signatures {SASs) and stored access policies.
You discover that unauthorized users accessed both the rile service and the blob service. You need to revoke all access to Sa1.
Solution: You regenerate the access keys. Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately effects all of the shared access signatures associated with it.
References:
https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

NEW QUESTION 272
- (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

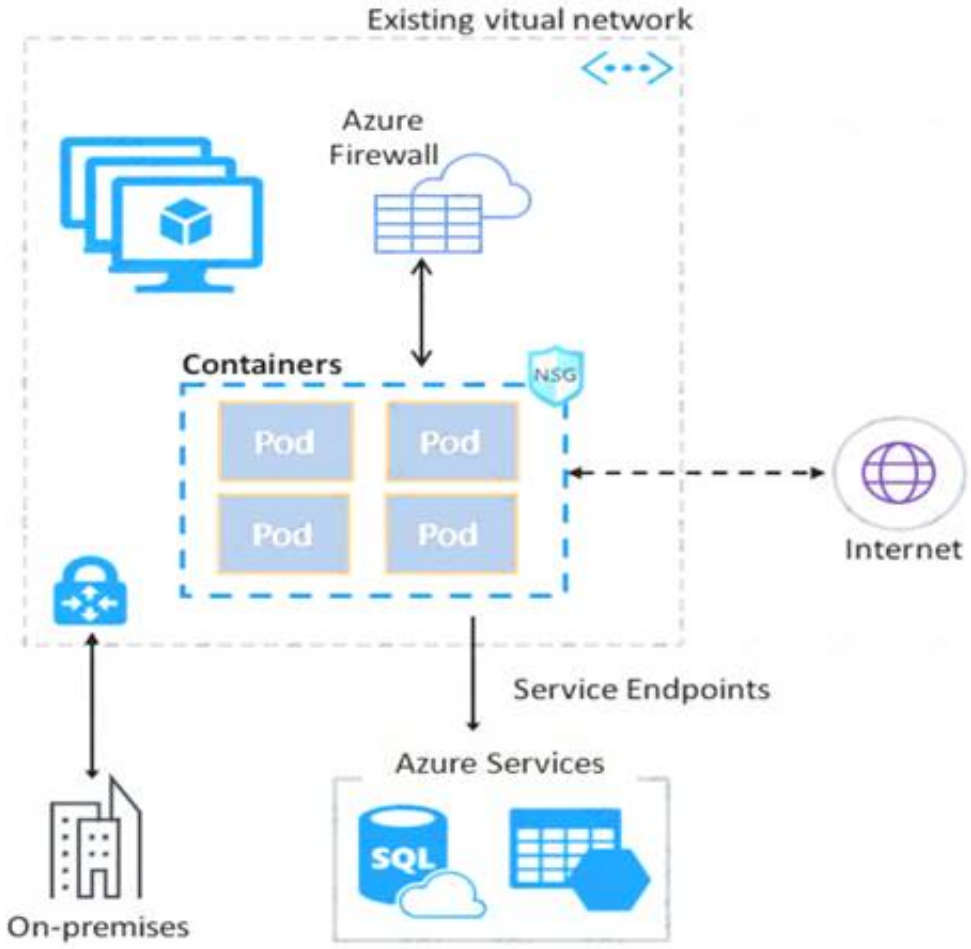
Explanation:
To prevent HTTP connections to the rg1lod28681041n1 Azure Storage account, you can follow these steps: In the Azure portal, search for and select the storage account named rg1lod28681041n1.
- In the left pane, select Firewalls and virtual networks.
- In the Firewalls and virtual networks 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 273
- (Exam Topic 4)
You have an Azure subscription named Sub1. Sub1 contains a virtual network named VNet1 that contains one subnet named Subnet1.
You create a service endpoint for Subnet1.
Subnet1 contains an Azure virtual machine named VM1 that runs Ubuntu Server 18.04.
You need to deploy Docker containers to VM1. The containers must be able to access Azure Storage resources and Azure SQL databases by using the service endpoint.

A. Create an application security group and a network security group (NSG).
B. Edit the docker-compose.yml file.
C. Install the container network interface (CNI) plug-in.

Answer: C

Explanation:
The Azure Virtual Network container network interface (CNI) plug-in installs in an Azure Virtual Machine. The plug-in supports both Linux and Windows platform. The plug-in assigns IP addresses from a virtual network to containers brought up in the virtual machine, attaching them to the virtual network, and connecting them directly to other containers and virtual network resources. The plug-in doesn't rely on overlay networks, or routes, for connectivity, and provides the same performance as virtual machines.
The following picture shows how the plug-in provides Azure Virtual Network capabilities to Pods:



References:
https://docs.microsoft.com/en-us/azure/virtual-network/container-networking-overview

NEW QUESTION 276
- (Exam Topic 4)
You need to recommend which virtual machines to use to host App1. The solution must meet the technical requirements for KeyVault1.
Which virtual machines should you use?

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

Answer: D

NEW QUESTION 278
- (Exam Topic 4)
You have an Azure key vault named Vault1 that stores the resources shown in following table.

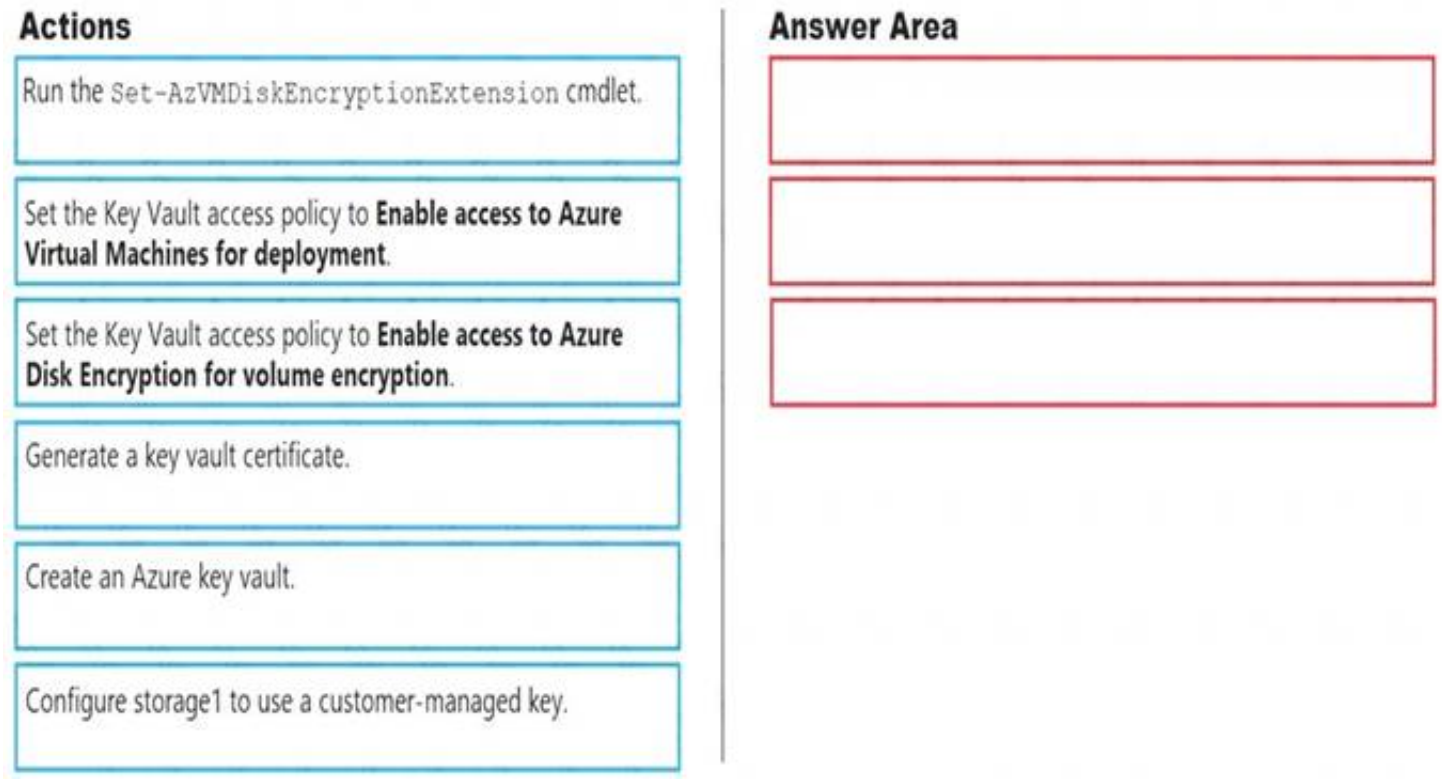
Name	Type
Key1	Key
Secret1	Secret
Cert1	Certificate

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 279
- (Exam Topic 4)
You have an Azure Storage account named storage1 and an Azure virtual machine named VM1. VM1 has a premium SSD managed disk.
You need to enable Azure Disk Encryption for VM1.
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 then in the correct order.



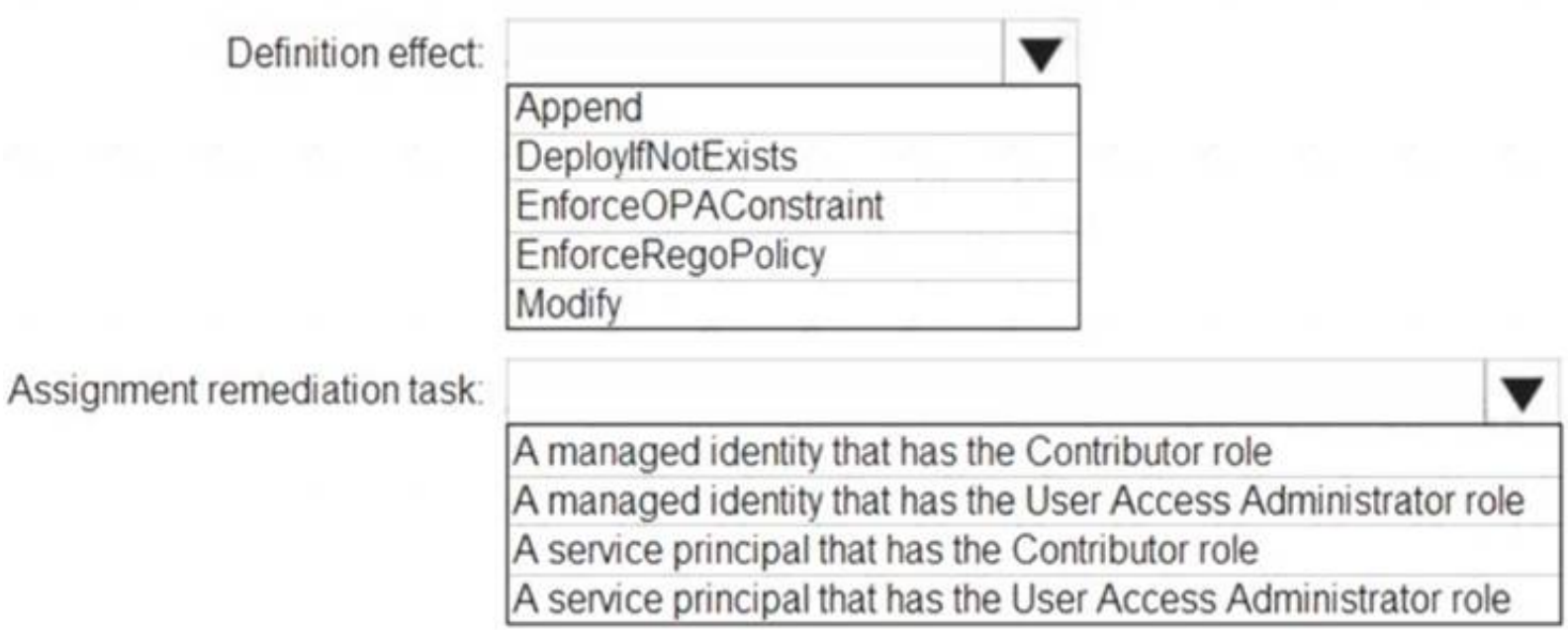
A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated
Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault

NEW QUESTION 283
- (Exam Topic 4)
You have an Azure subscription.
You need to create and deploy an Azure policy that meets the following requirements:
- When a new virtual machine is deployed, automatically install a custom security extension.
- Trigger an autogenerated remediation task for non-compliant virtual machines to install the extension.

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



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 285
- (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 289
- (Exam Topic 4)
You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1. You have 100 on-premises servers that run Windows Server 2012 R2 and Windows Server 2016. The servers
connect to LAW1. LAW1 is configured to collect security-related performance counters from the connected servers.
You need to configure alerts based on the data collected by LAW1. The solution must meet the following requirements:
- Alert rules must support dimensions.
- The time it takes to generate an alert must be minimized.
- resolved.

Which signal type should you use when you create the alert rules?

A. Log
B. Log (Saved Query)
C. Metric
D. Activity Log

Answer: C

Explanation:
Metric alerts in Azure Monitor provide a way to get notified when one of your metrics cross a threshold. Metric alerts work on a range of multi-dimensional platform metrics, custom metrics, Application Insights standard and custom metrics.
Note: Signals are emitted by the target resource and can be of several types. Metric, Activity log, Application Insights, and Log.
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-metric

NEW QUESTION 293
- (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 298
- (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 299
- (Exam Topic 4)
You have an Azure subscription named Subcription1 that contains the resources shown in the following table.

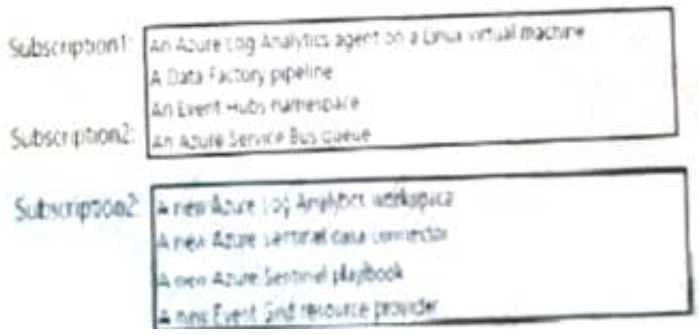
Name	Type	Description
EventHub1	Azure Event Hubs	*Not applicable*
Adf1	Azure Data Factory	*Not applicable*
NVA1	Network virtual appliance (NVA)	The NVA sends security event messages in the Common Event Format (CEF)

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

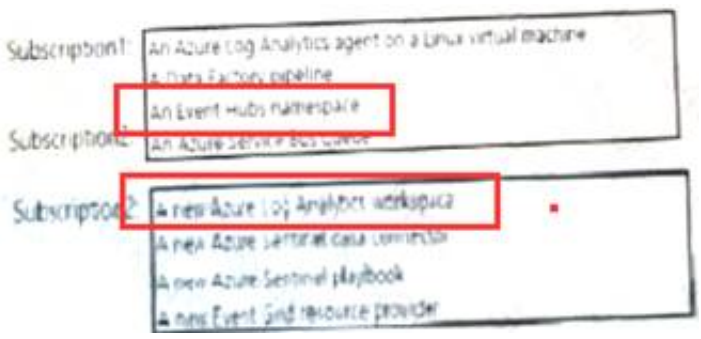


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 302
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.

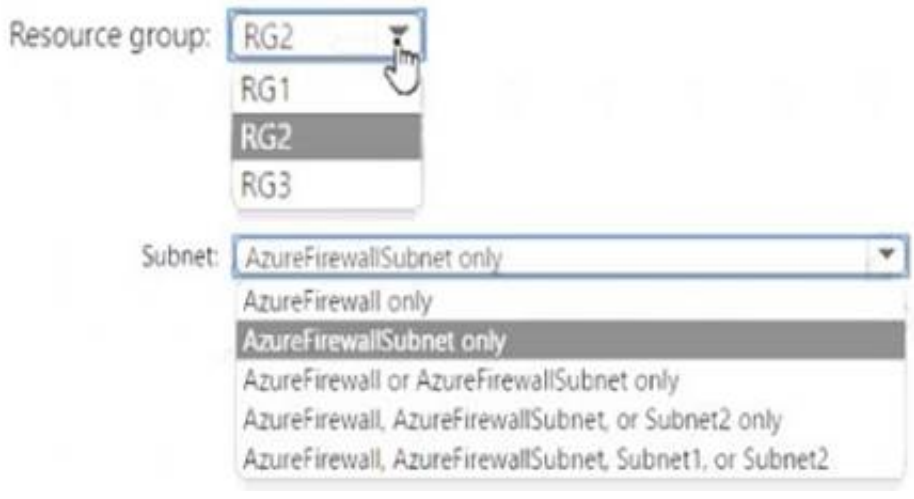
Name	Type	Location	In resource group
RG1	Resource group	East US	*Not applicable*
RG2	Resource group	West US	*Not applicable*
RG3	Resource group	Central US	*Not applicable*
VNet1	Virtual network	Central US	RG2

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.

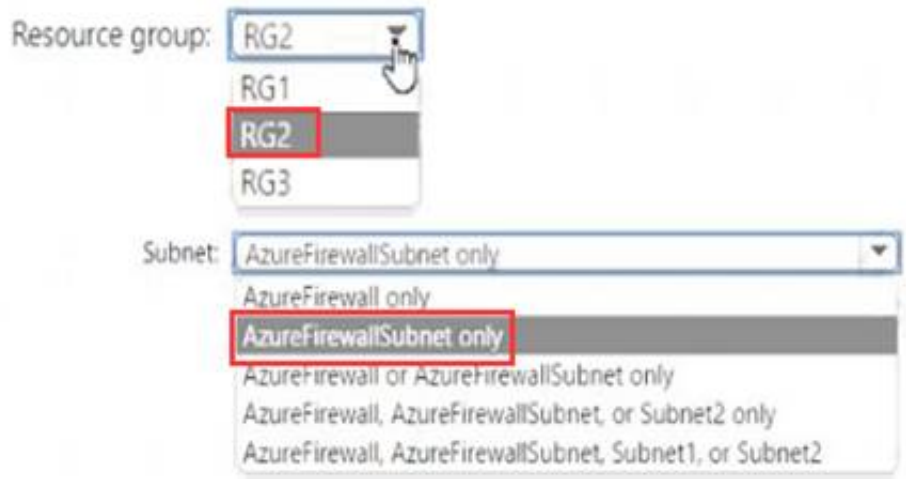
Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area



NEW QUESTION 307
- (Exam Topic 4)
You have an Azure subscription that uses Microsoft Defender for Cloud.
You have an Amazon Web Service (AWS) account named AWS1 that is connected to defender for Cloud.
You need to ensure that AWS foundational Security Best Practices. The solution must minimize administrate effort.
What should do you in Defender for Cloud?

A. Create a new customer assessment.
B. Assign a built-in assessment.
C. Assign a built-in compliance standard.
D. Create a new custom standard.

Answer: C

NEW QUESTION 312
- (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 314
- (Exam Topic 4)
You have an Azure subscription named Sub1 that contains the virtual machines shown in the following table.

Name	Resource group
VM1	RG1
VM2	RG2
VM3	RG1
VM4	RG2

You need to ensure that the virtual machines in RG1 have the Remote Desktop port closed until an authorized user requests access.
What should you configure?

A. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
B. an application security group
C. Azure Active Directory (Azure AD) conditional access
D. just in time (JIT) VM access

Answer: D

Explanation:
Just-in-time (JIT) virtual machine (VM) access can be used to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.
Note: When just-in-time is enabled, Security Center locks down inbound traffic to your Azure VMs by creating an NSG rule. You select the ports on the VM to which inbound traffic will be locked down. These ports are controlled by the just-in-time solution.
When a user requests access to a VM, Security Center checks that the user has Role-Based Access Control (RBAC) permissions that permit them to successfully request access to a VM. If the request is approved, Security Center automatically configures the Network Security Groups (NSGs) and Azure Firewall to allow inbound traffic to the selected ports and requested source IP addresses or ranges, for the amount of time that was specified. After the time has expired, Security Center restores the NSGs to their previous states. Those connections that are already established are not being interrupted, however.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time

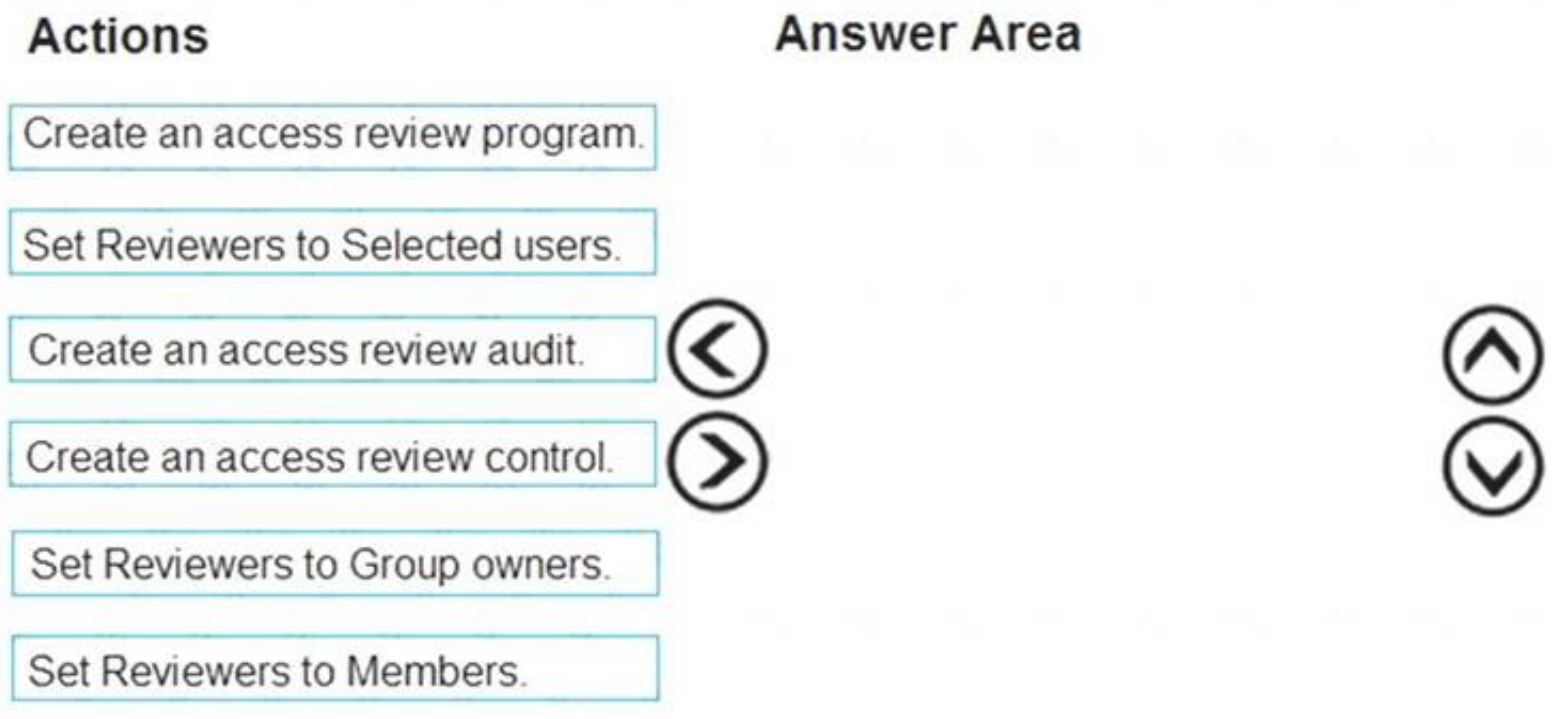
NEW QUESTION 315
- (Exam Topic 4)
From Azure Security, you create a custom alert rule.
You need to configure which users will receive an email message when the alert is triggered. What should you do?

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

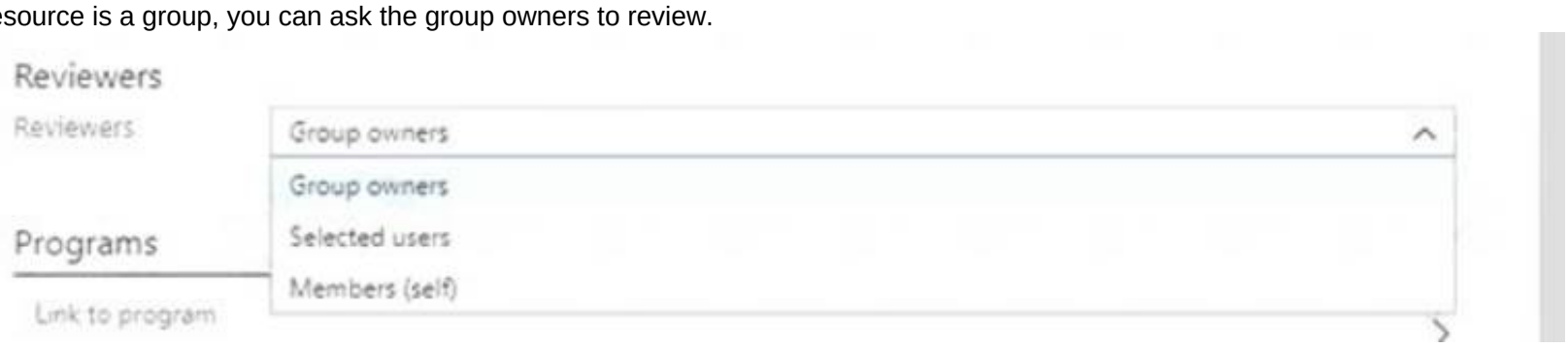
NEW QUESTION 317
- (Exam Topic 4)
You need to configure an access review. The review will be assigned to a new collection of reviews and reviewed by resource owners.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

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

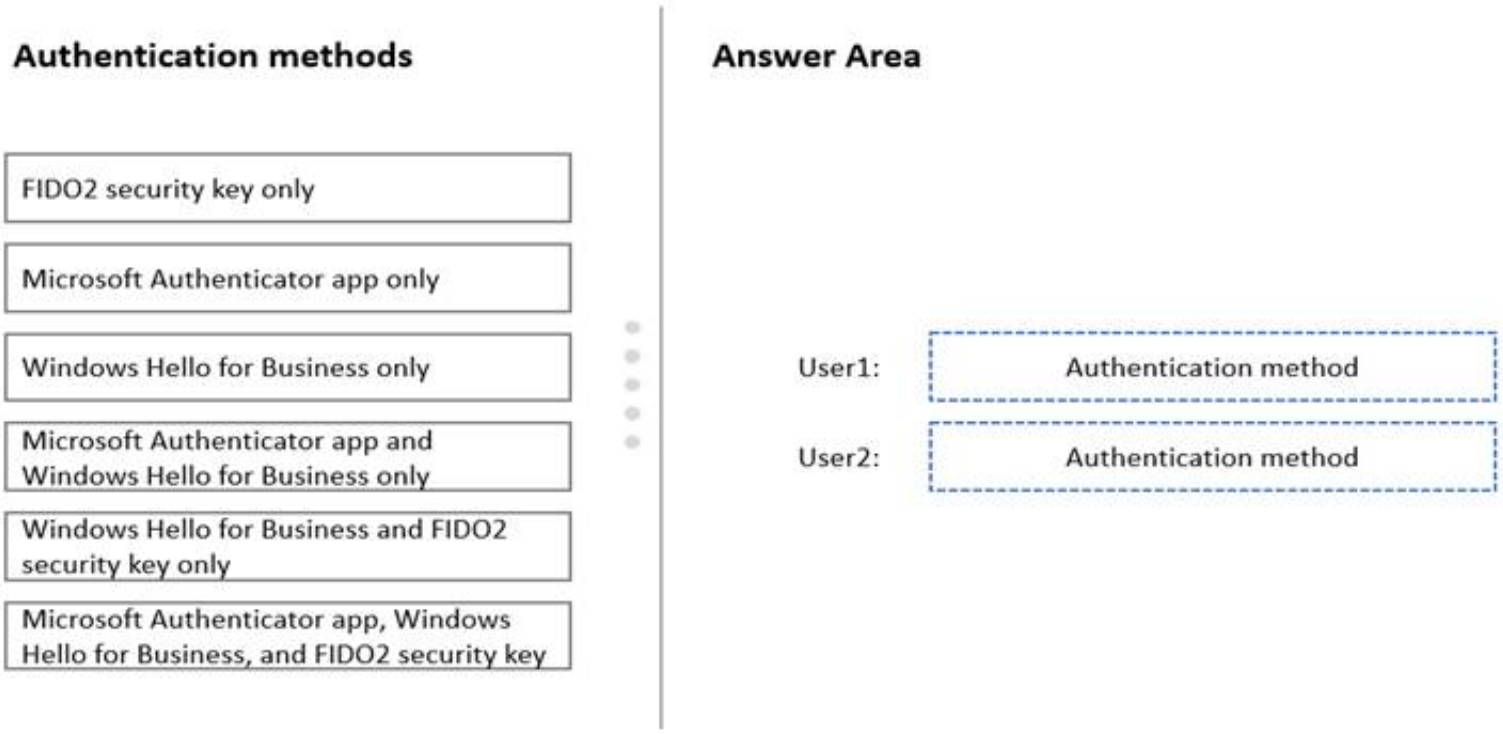


References:
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-programs-controls

NEW QUESTION 322
- (Exam Topic 4)
You have an Azure AD tenant that contains the users shown in the following table.

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

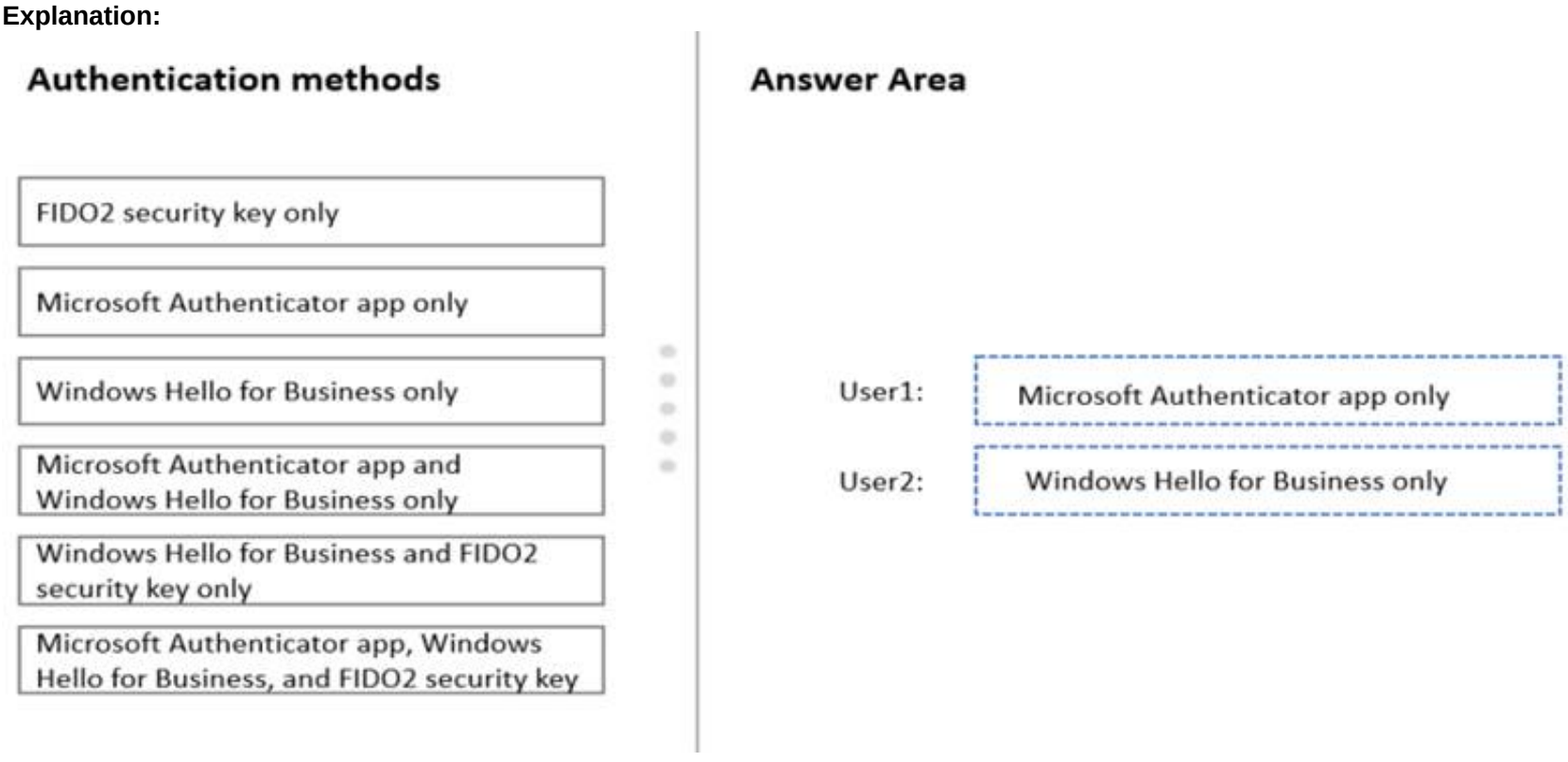
You enable passwordless authentication for the tenant.
Which authentication method can each user use for passwordless authentication? To answer, drag the appropriate authentication methods to the correct users. Each authentication method may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 327
- (Exam Topic 4)
You have an Azure key vault named KeyVault1 that contains the items shown in the following table.

Name	Type
Item1	Key
Item2	Secret
Policy1	Access policy

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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 331
- (Exam Topic 4)
You plan to use Azure Sentinel to create an analytic rule that will detect suspicious threats and automate responses.
Which components are required for the rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Detect suspicious threats:
- A Kusto query language query
- A Transact-SQL query
- An Azure PowerShell query
- An Azure Sentinel playbook

Automate responses:
- An Azure Functions app
- An Azure PowerShell script
- An Azure Sentinel playbook
- An Azure Sentinel workbook

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 333
- (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

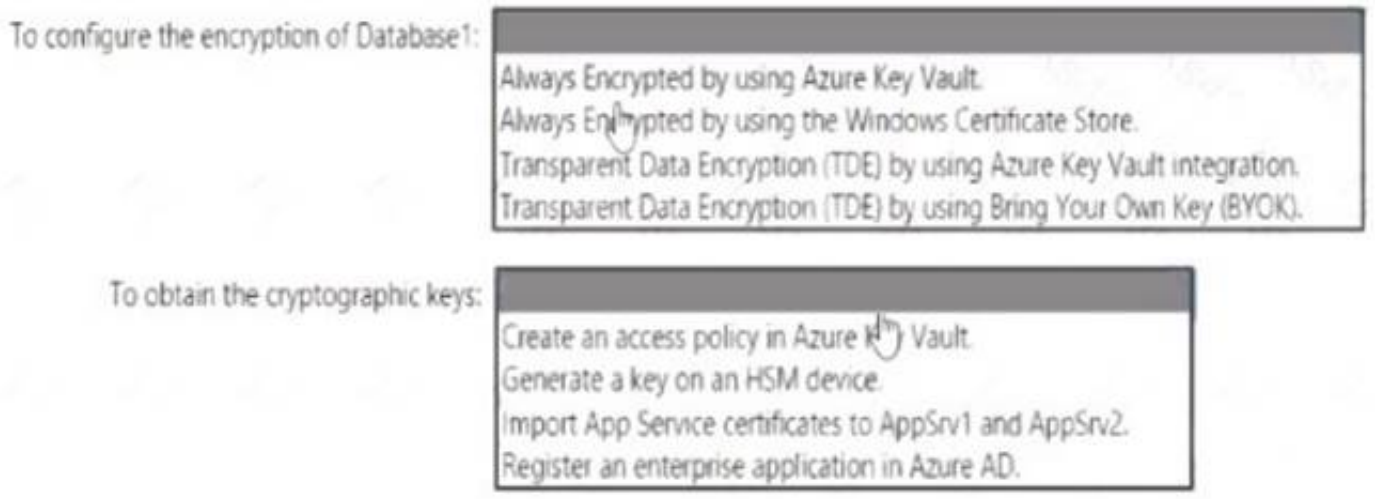
You perform the following tasks:
- Assign User1 the Network Contributor role for Subscription1.
- Assign User2 the Contributor role for RG1.

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 336
- (Exam Topic 4)
You have an Azure subscription that contains the following resources:
• An Azure key vault
• An Azure SQL database named Database1
• Two Azure App Service web apps named AppSrv1 and AppSrv2 that are configured to use system-assigned managed identities and access Database1
You need to implement an encryption solution for Database1 that meets the following requirements:
• The data in a column named Discount in Database1 must be encrypted so that only AppSrv1 can decrypt the data.
• AppSrv1 and AppSrv2 must be authorized by using managed identities to obtain cryptographic keys. How should you configure the encryption settings fa Database1 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:
Text Description automatically generated with medium confidence
Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/database/always-encrypted-azure-key-vault-configure?tabs=az

NEW QUESTION 339
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.

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

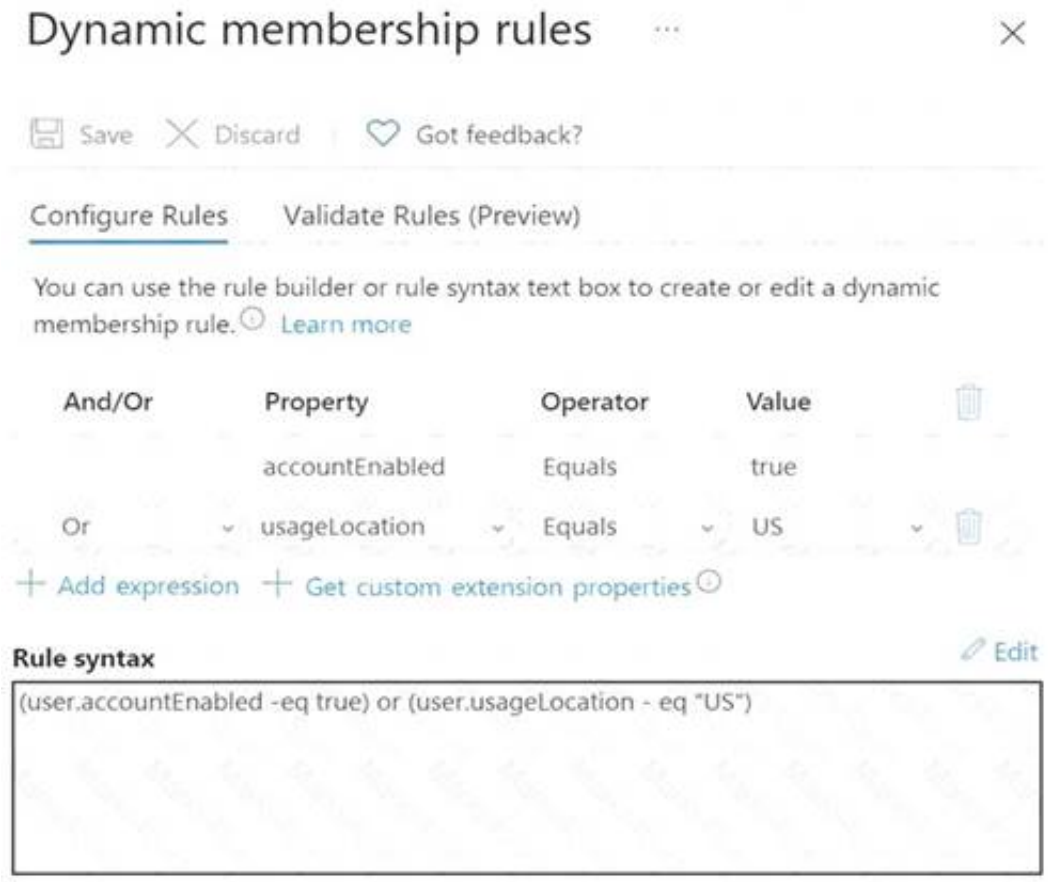
The subscription is linked to an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Usage location
User1	United States
User2	Germany

You create the groups shown in the following table.

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

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



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

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 344
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.

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

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

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

E. VM1 and storage1 only

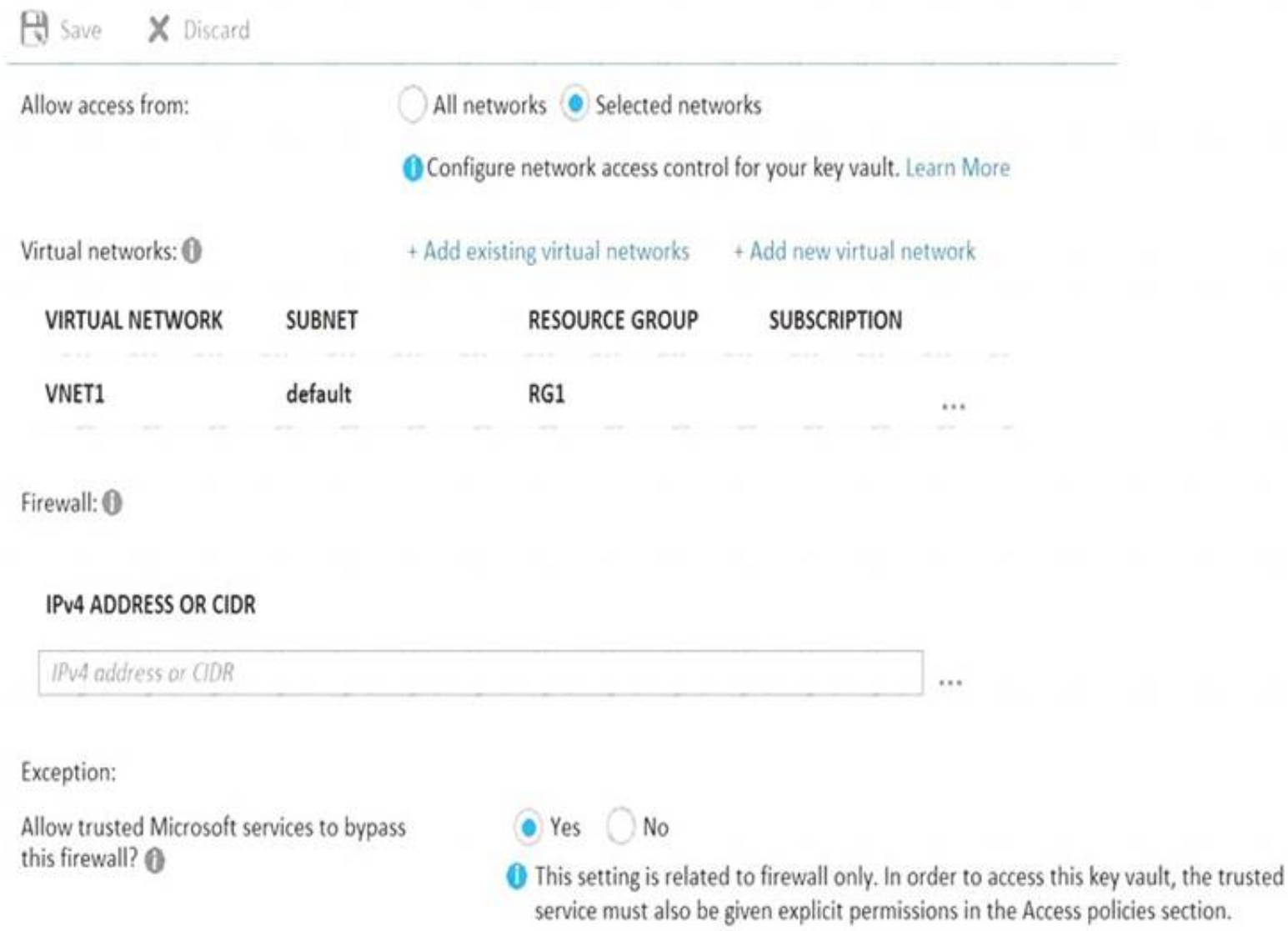
Answer: A

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

NEW QUESTION 345
- (Exam Topic 4)
You have an Azure subscription that contains an Azure key vault named KeyVault1 and the virtual machines shown in the following table.

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

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



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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 347
- (Exam Topic 4)
You have been tasked with applying conditional access policies for your company's current Azure Active Directory (Azure AD).
The process involves assessing the risk events and risk levels.
Which of the following is the risk level that should be configured for users that have leaked credentials?

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

Answer: D

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

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

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

NEW QUESTION 350
.....

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