Microsoft

Exam Questions az-500

Microsoft Azure Security Technologies

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

```
{
    "type" : "Microsoft.Compute/virtualMachines/extensions",
    "name" : "[concat(parameter('vmname'), /OMSExtension]",
    "apiVersion" : "[variables('apiVersion')]",
    "location" : "[resourceGroup().location]",
    "dependsOn" : [
        "[concat('Microsoft.Compute/virtualMachines/', parameters('vmName'))]"
    ],
    "properties" : {
        "publisher" : "Microsoft.EnterpriseCloud.Monitoring",
        "type" :  "MicrosoftMonitoringAgent",
        "typeHandlerVersion" : "1.0",
        "autoUpgradeMinorVersion" : true,
        "settings" : {
            [ ▼ ] : "[variable('var1')]"
        },
        "protectedSettings" : {
            [ ▼ ] : "[variable ('var2')]"
        }
    }
}
```

- "AzureADApplicationID"
- "WorkspaceID"
- "WorkspaceName"
- "WorkspaceURL"

- "AzureADApplicationSecret"
- "StorageAccountKey"
- "WorkspaceID"
- "WorkspaceKey"

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 2
- (Exam Topic 4)
You have an Azure subscription 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 3
- (Exam Topic 4)
You have an Azure subscription that contains four Azure SQL managed instances.
You need to evaluate the vulnerability of the managed instances to SQL injection attacks. What should you do first?

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

Answer: B

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

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

Answer: CE

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

NEW QUESTION 5
- (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:

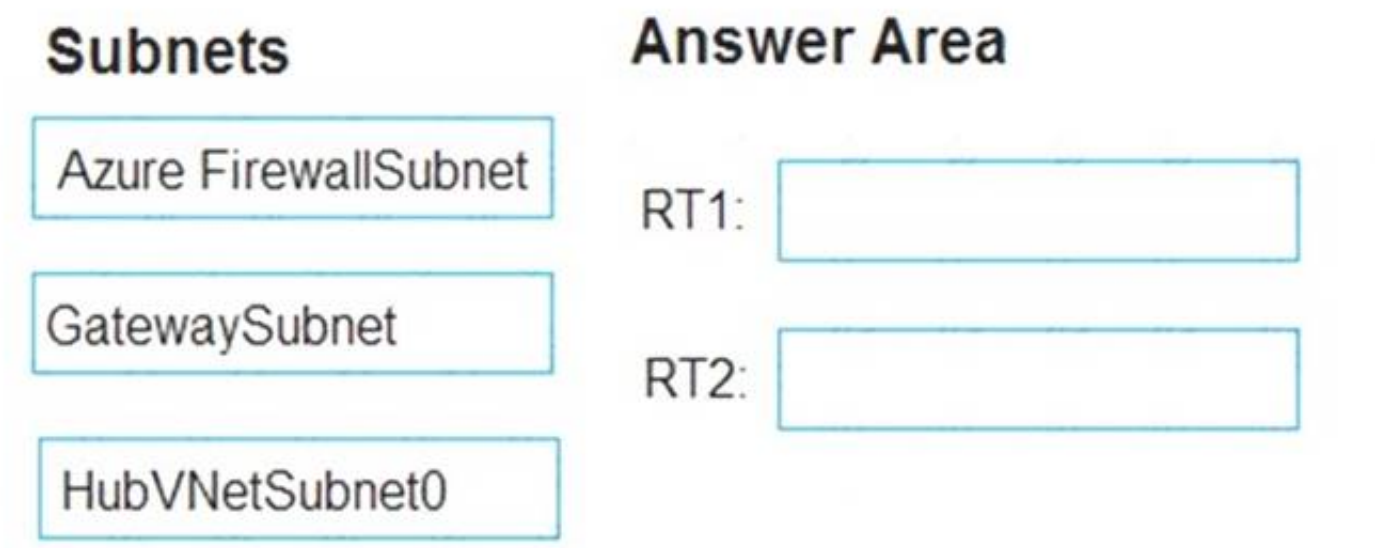
https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/auditing-configure https://docs.microsoft.com/en-us/azure/azure-sql/database/auditing-overview

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

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

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

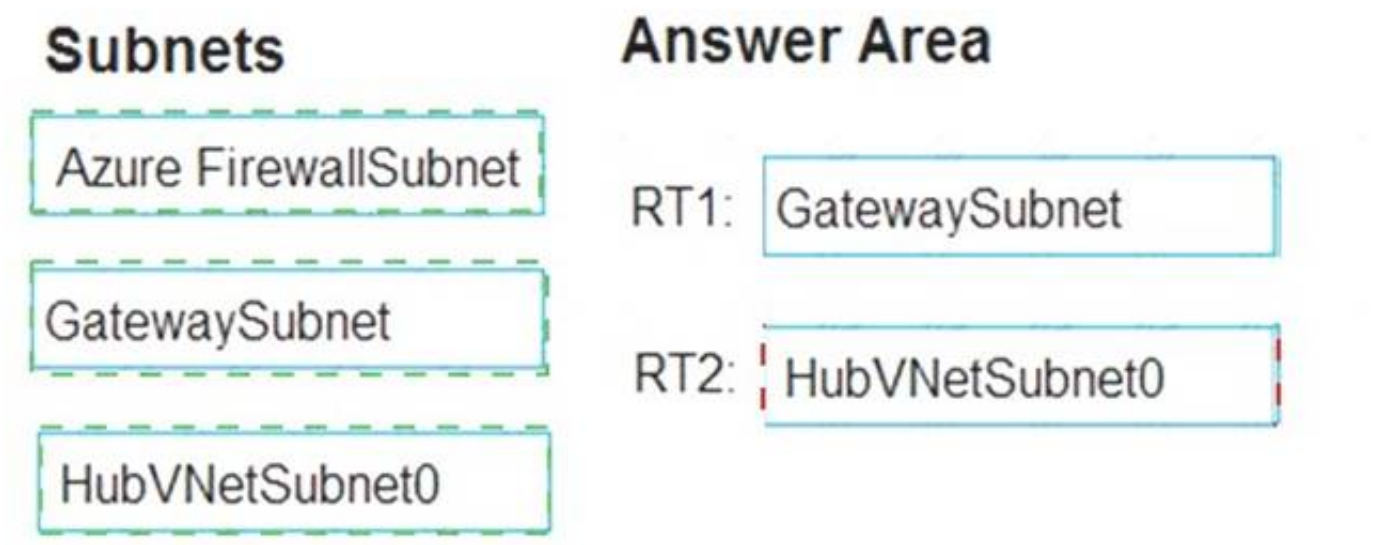
You need to ensure that traffic between SpokeVNetSubnet0 and the on-premises network flows through the Azure firewall.
To which subnet should you associate each route table? To answer, drag the appropriate subnets to the correct route tables. Each subnet may be used once, more than once, or not at all.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



A. Mastered
B. Not Mastered

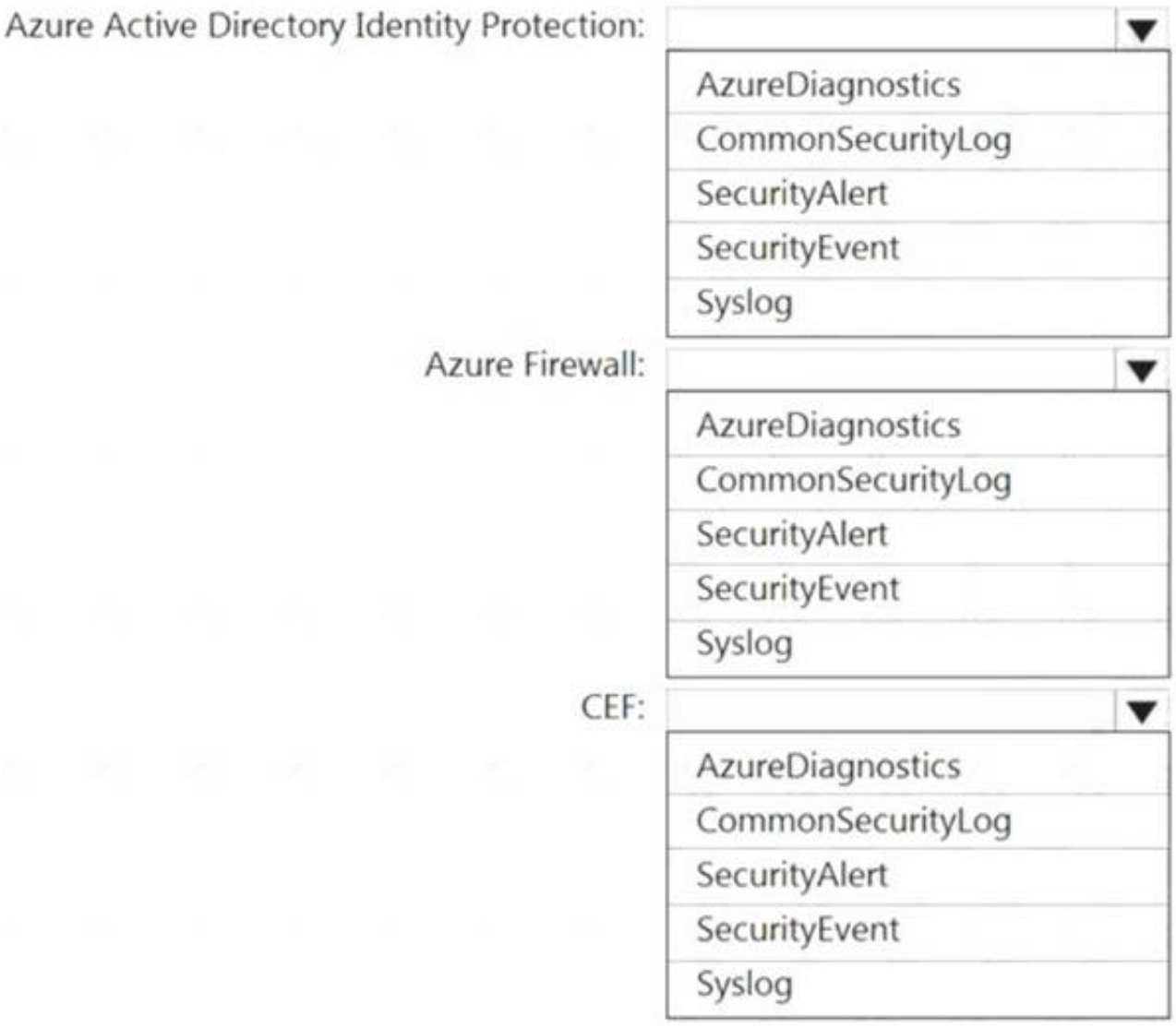
Answer: A

Explanation:



NEW QUESTION 7
- (Exam Topic 4)
You have an Azure Sentinel workspace that has the following data connectors:
- Azure Active Directory Identity Protection
- Common Event Format (CEF)
- Azure Firewall

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



A. Mastered
B. Not Mastered

Answer: A

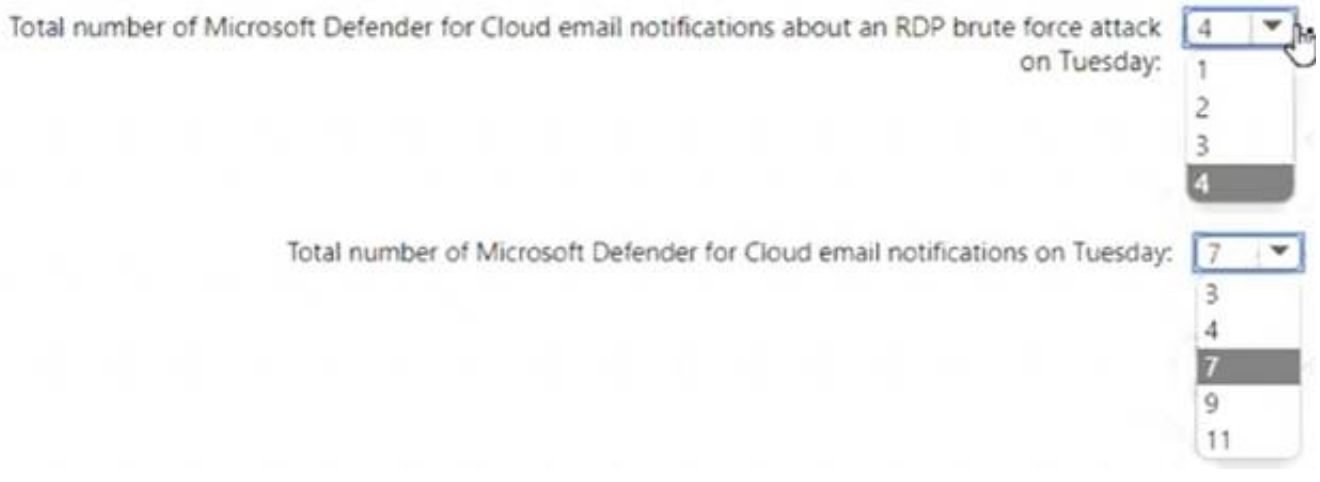
Explanation:
Graphical user interface, application, table Description automatically generated

NEW QUESTION 8
- (Exam Topic 4)
On Monday, you configure an email notification in Microsoft Defender for Cloud to notify user1 @contoso.com about alerts that have a severity level of Low, Medium, or High. On Tuesday, Microsoft Defender for Cloud generates the security alerts shown in the following table.

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

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

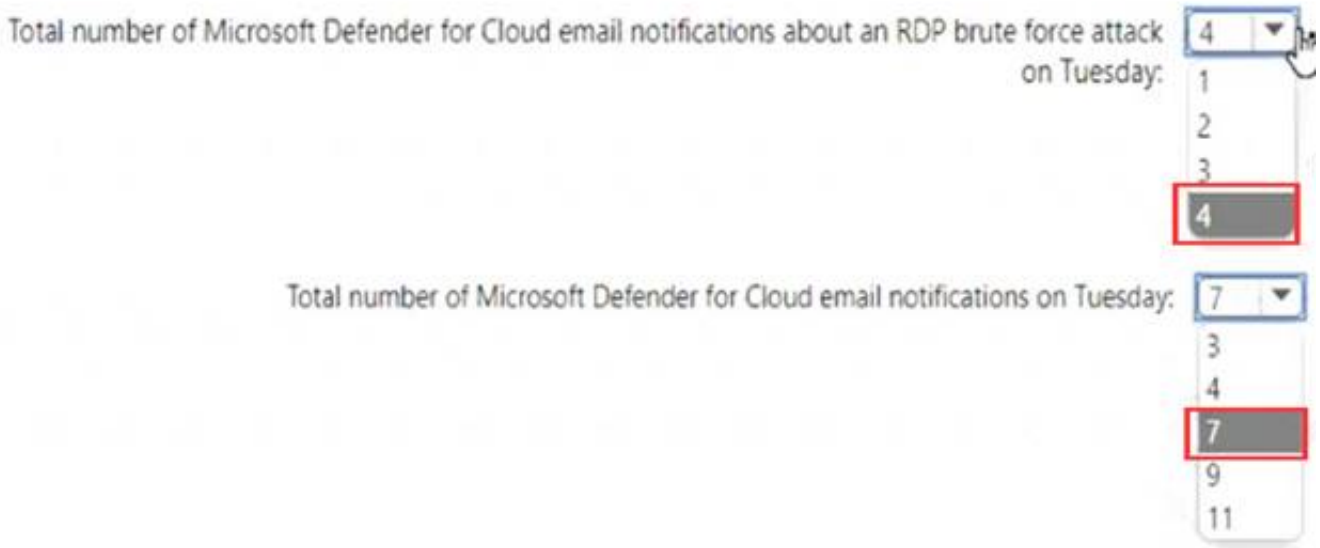
Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 9
- (Exam Topic 4)
Lab Task
use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password. place your cursor in the Enter password box and click on the password below. Azure Username: Userl -28681041@ExamUsers.com
Azure Password: GpOAe4@lDg
If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only: Lab Instance: 28681041
Task 2
You need to add the network interface of a virtual machine named VM1 to an application security group named ASG1.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
To add the network interface of a virtual machine named VM1 to an application security group named ASG1, you can follow these steps:

- In the Azure portal, search for and select the virtual machine named VM1.
- In the left pane, select Networking.
- In the Networking pane, select the network interface that you want to add to the application security group named ASG1.
- In the network interface pane, select Application security groups.
- In the Application security groups pane, select Add.
- In the Add application security group pane, select the application security group named ASG1.
- Select Save.

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

NEW QUESTION 10
- (Exam Topic 4)
Your network contains an Active Directory forest named contoso.com. You have an Azure Directory (Azure AD) tenant named contoso.com.
You plan to configure synchronization by using the Express Settings installation option in Azure AD Connect. You need to identify which roles and groups are required to perform the planned configurations. The solution

must use the principle of least privilege.
Which two roles and groups should you identify? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. the Domain Admins group in Active Directory
B. the Security administrator role in Azure AD
C. the Global administrator role in Azure AD
D. the User administrator role in Azure AD
E. the Enterprise Admins group in Active Directory

Answer: CE

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

NEW QUESTION 10
- (Exam Topic 4)
From the Azure portal, you are configuring an Azure policy.
You plan to assign policies that use the DeployIfNotExist, AuditIfNotExist, Append, and Deny effects.
Which effect requires a managed identity for the assignment?

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

Answer: C

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

NEW QUESTION 13
- (Exam Topic 4)
Lab Task
Task 6
You need to configure a Microsoft SQL server named Web3l 330471 only to accept connections from the Subnet0 subnet on the VNET01 virtual network.

A. Mastered
B. Not Mastered

Answer: A

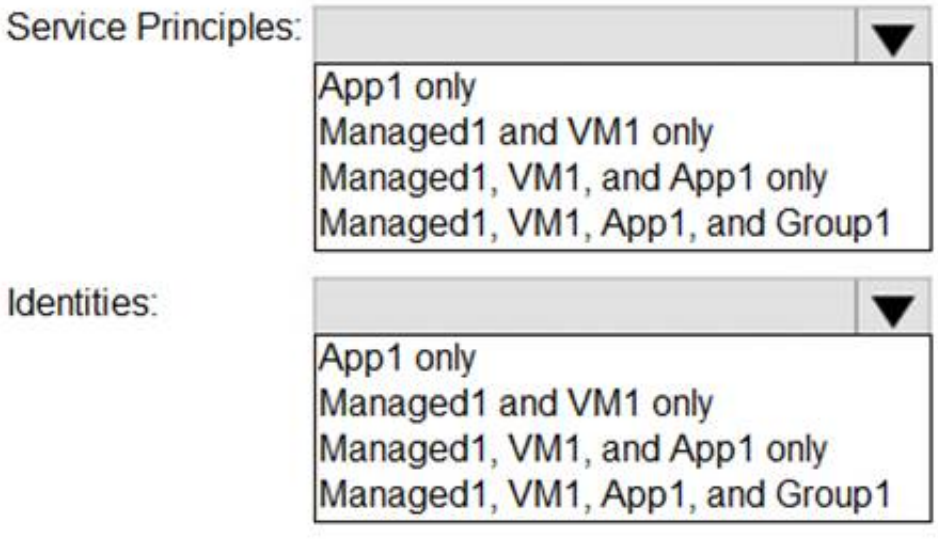
Explanation:
Configure the firewall settings for the SQL server. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to add a firewall rule that allows inbound traffic from the IP address range of the Subnet0 subnet. You also need to disable the option to allow Azure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

NEW QUESTION 14
- (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

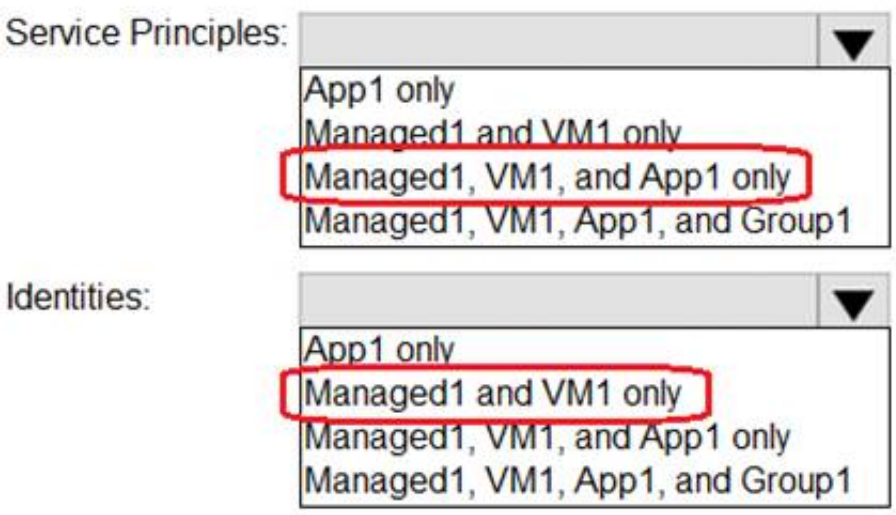


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



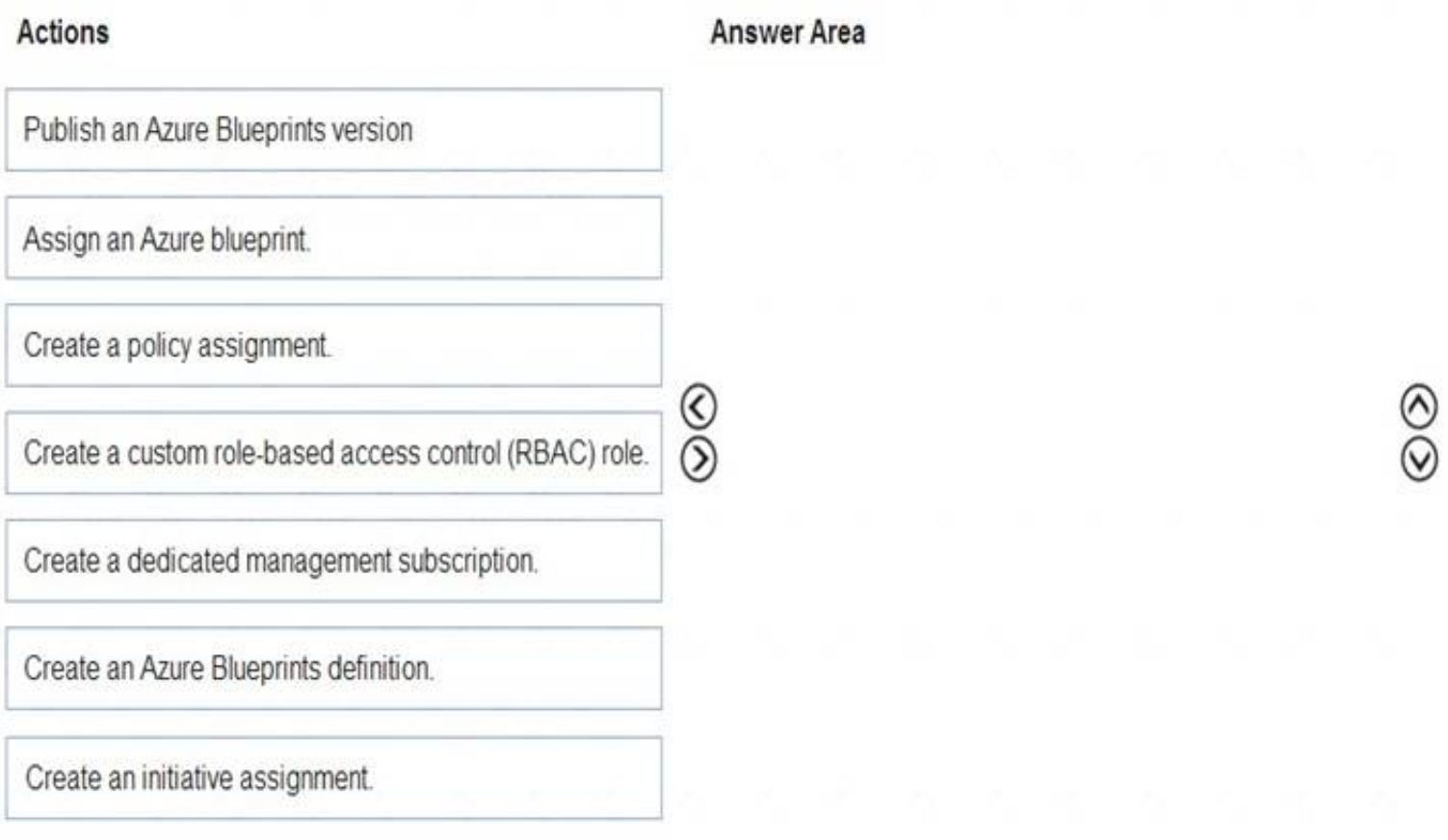
NEW QUESTION 15
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant and a root management group. You create 10 Azure subscriptions and add the subscriptions to the rout management group.
You need to create an Azure Blueprints definition that will be stored in the root management group. 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 20
- (Exam Topic 4)
You have five Azure subscriptions linked to a single Azure Active Directory (Azure AD) tenant. You create an Azure Policy initiative named SecurityPolicyInitiative1.
You identify which standard role assignments must be configured on all new resource groups.
You need to enforce SecurityPolicyInitiative1 and the role assignments when a new resource group is created. Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 21
- (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)

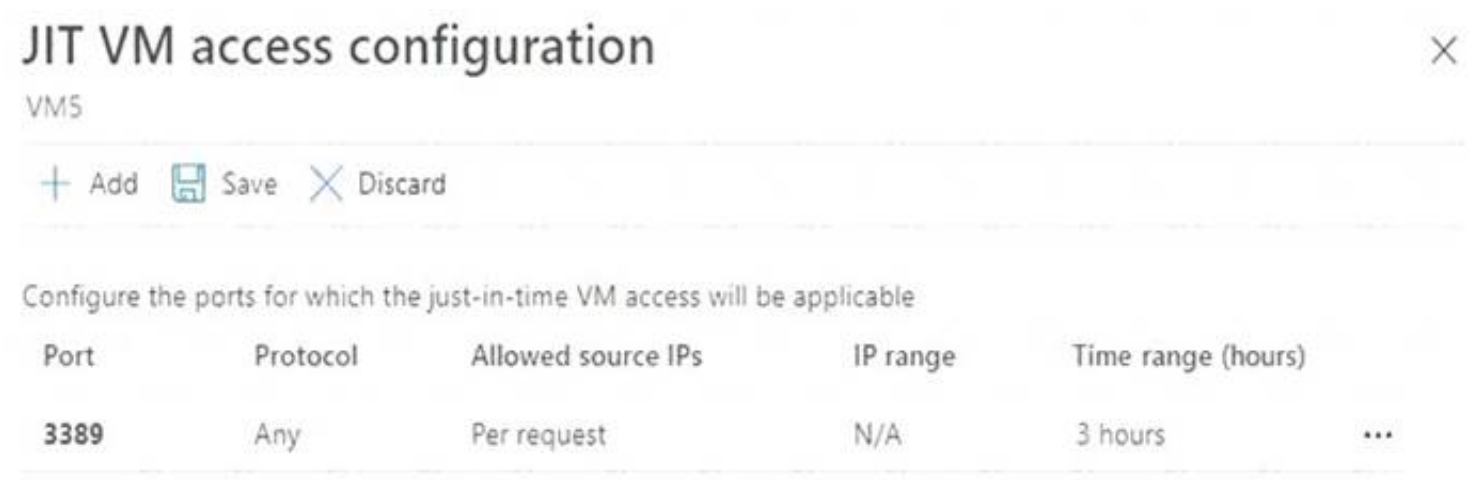
Answer: C

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 26
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Attached to	NSG
NSG1	Network security group (NSG)	VM5	*Not applicable*
NSG2	Network security group (NSG)	Subnet1	*Not applicable*
Subnet1	Subnet	*Not applicable*	*Not applicable*
VM5	Virtual machine	Subnet1	NSG1

An IP address of 10.1.0.4 is assigned to VM5. VM5 does not have a public IP address. VM5 has just in time (JIT) VM access configured as shown in the following exhibit.



You enable JIT VM access for VM5.
NSG1 has the inbound rules shown in the following exhibit.

Priority	Name	Port	Protocol	Source	Destination	Action
100	SecurityCenter-JITRule-...	3389	Any	Any	10.1.0.4	Allow
1000	SecurityCenter-JITRule_341...	3389	Any	Any	10.1.0.4	Deny
1001	RDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

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

Statements	Yes	No
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	○	○
Remote Desktop access to VM5 is blocked.	○	○
An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	○	○
Remote Desktop access to VM5 is blocked.	○	○
An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.	○	○

NEW QUESTION 27
- (Exam Topic 4)
Your on-premises network contains the servers shown in the following table.

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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 29
- (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 33
- (Exam Topic 4)
You have 15 Azure virtual machines in a resource group named RG1. All virtual machines run identical applications.
You need to prevent unauthorized applications and malware from running on the virtual machines. What should you do?

A. Apply an Azure policy to RG1.

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

Answer: B

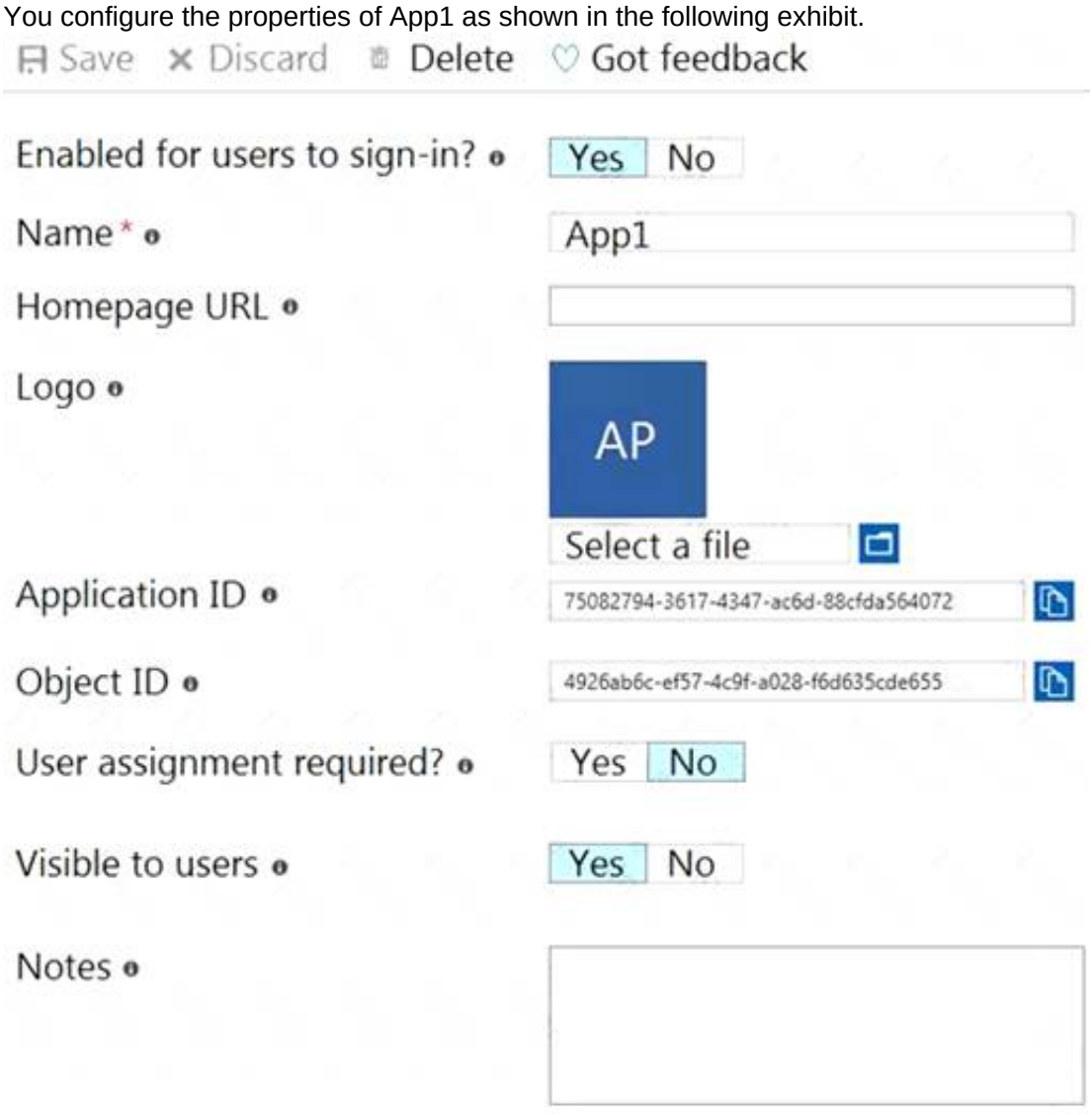
Explanation:
Adaptive application control is an intelligent, automated end-to-end application whitelisting solution from Azure Security Center. It helps you control which applications can run on your Azure and non-Azure VMs (Windows and Linux), which, among other benefits, helps harden your VMs against malware. Security Center uses machine learning to analyze the applications running on your VMs and helps you apply the specific whitelisting rules using this intelligence.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application

NEW QUESTION 34
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains three security groups named Group1, Group2, and Group3 and the users shown in the following table.

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

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

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



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

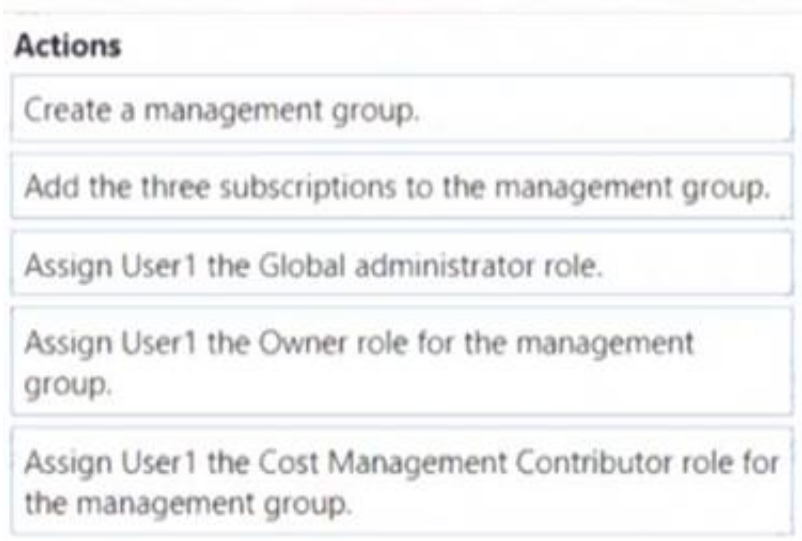
Statements	Yes	No
User1 has App1 listed on his My Apps portal.	○	○
User2 has App1 listed on her My Apps portal.	○	○
User3 has App1 listed on her My Apps portal.	○	○

A. Mastered
B. Not Mastered

Answer: A

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

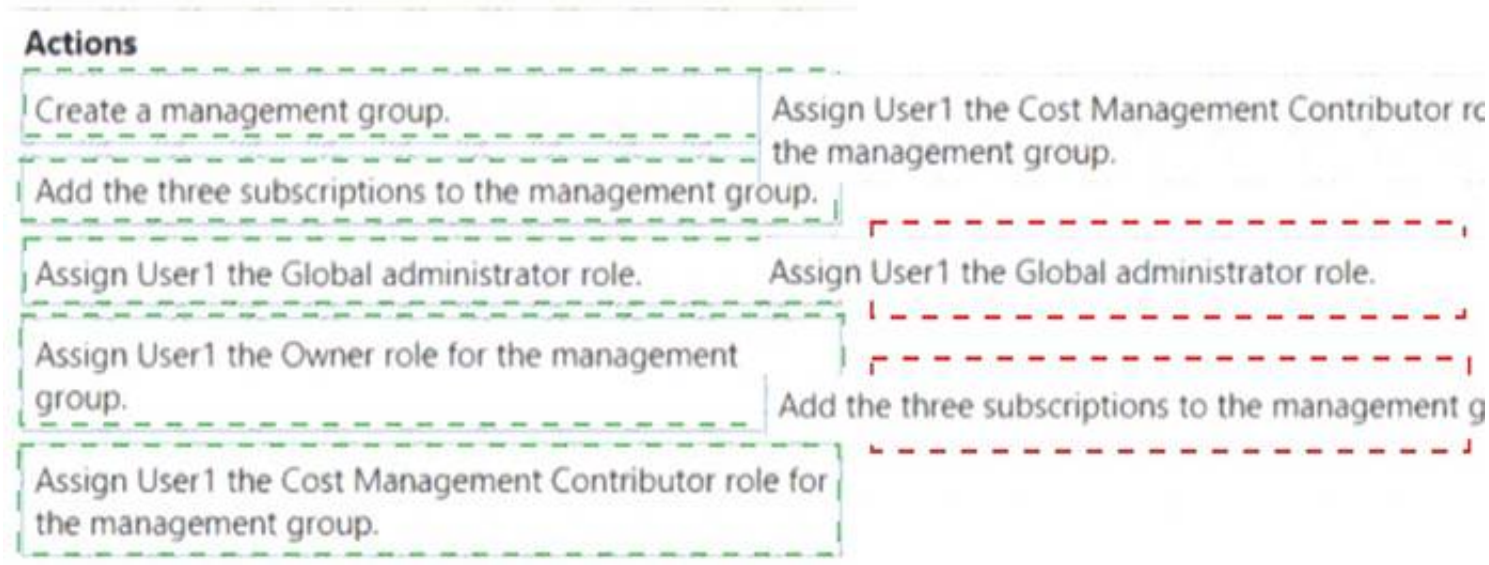
NEW QUESTION 38
- (Exam Topic 4)
You have three Azure subscriptions and a user named User1.
You need to provide User1 with the ability to manage and view costs for the resources across all three subscriptions. The solution must use the principle of least privilege.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 40
- (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 add an extension to each virtual machine.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
You can use Visual Studio to enable and configure the Microsoft Antimalware service. This entails selecting Microsoft Antimalware extension from the dropdown list under Installed Extensions and click Add to configure with default antimalware configuration.
References:
https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware

NEW QUESTION 45
- (Exam Topic 4)

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

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

The subscription contains the users shown in the following table.

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

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

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

A. Mastered
B. Not Mastered

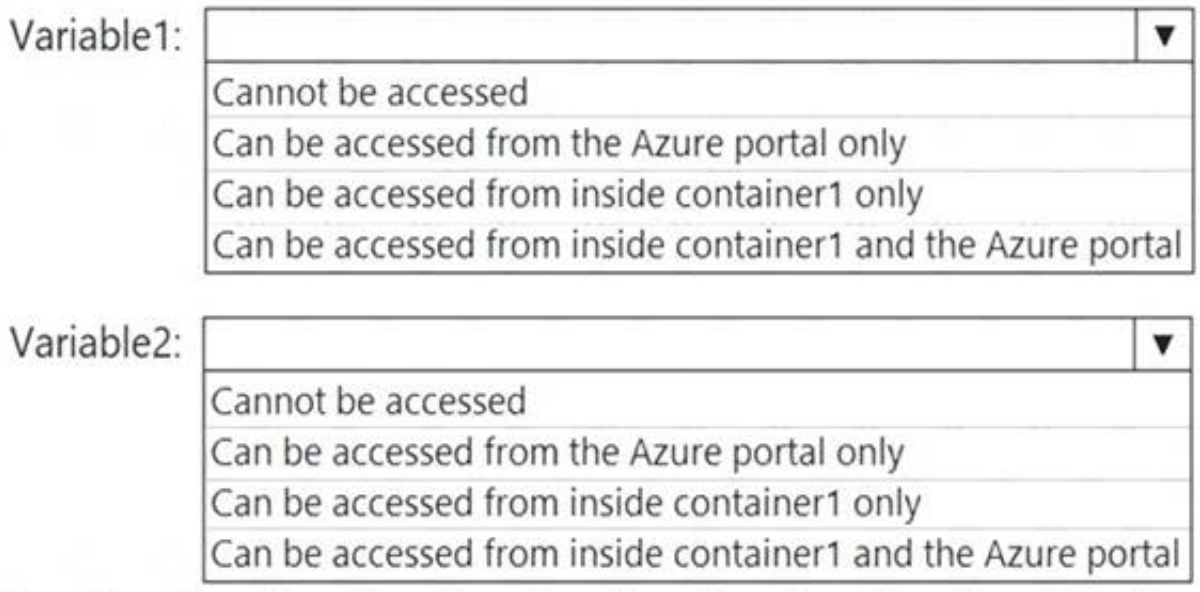
Answer: A

Explanation:
Yes
Yes No

NEW QUESTION 47
- (Exam Topic 4)
You have a file named File1.yaml that contains the following contents.

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

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



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 51
- (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 56
- (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 60
- (Exam Topic 4)
You are collecting events from Azure virtual machines to an Azure Log Analytics workspace. You plan to create alerts based on the collected events
You need to identify which Azure services can be used to create the alerts.
Which two services should you identify? Each correct answer presents a complete solution NOTE: Each correct selection is worth one point.

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

Answer: AD

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

NEW QUESTION 61
- (Exam Topic 4)
Your company has two offices in Seattle and New York. Each office connects to the Internet by using a NAT device. The offices use the IP addresses shown in the following table.

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

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

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

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

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

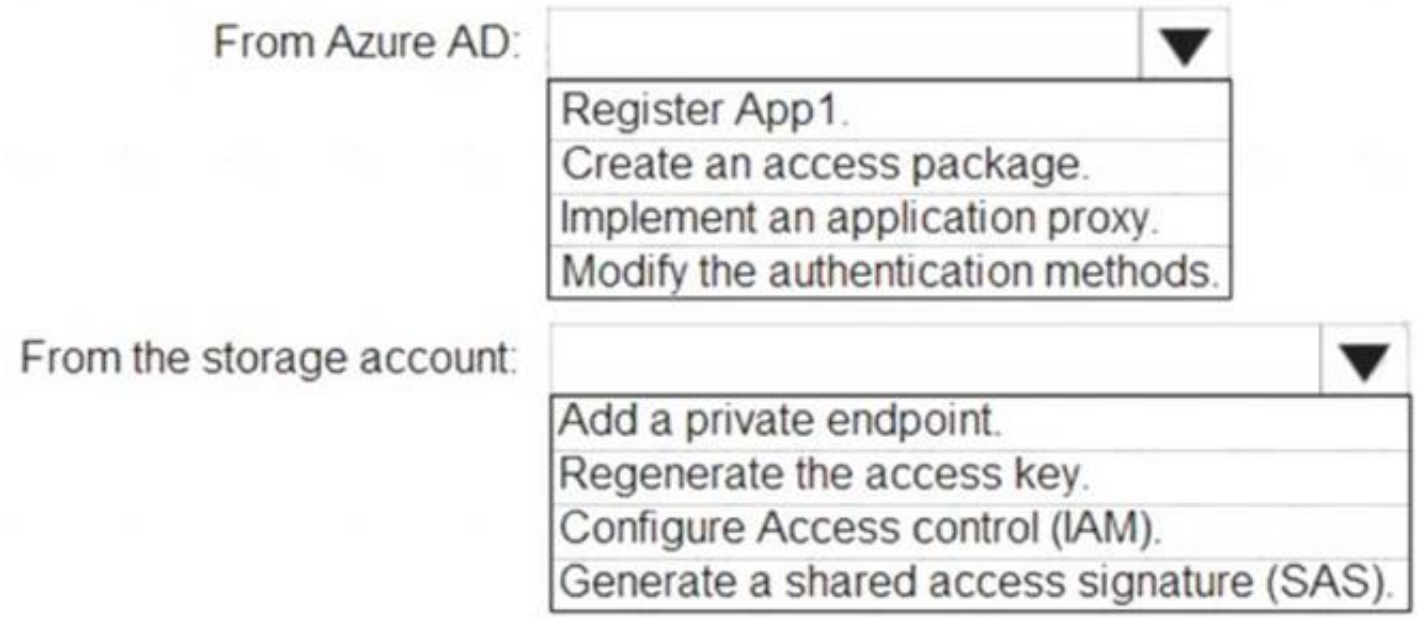
	Yes	No
If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.	○	○
If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app.	○	○
If User2 signs in to Azure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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 65
- (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 68
- (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 70
- (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]**.

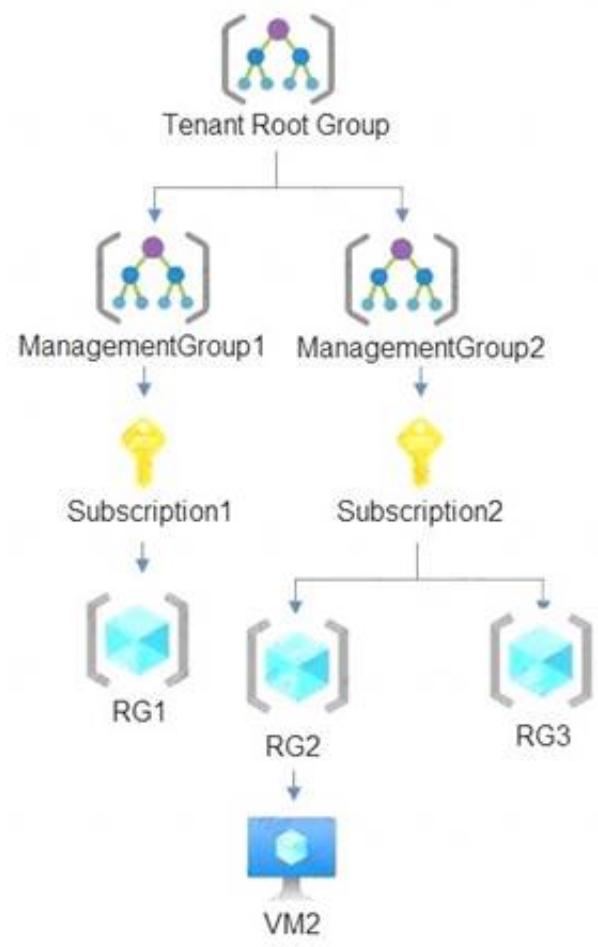
- allowed
- dropped
- forwarded

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 73
- (Exam Topic 4)
You have the hierarchy of Azure resources shown in the following exhibit.



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

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

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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 76
- (Exam Topic 4)
You are configuring just in time (JIT) VM access to a set of Azure virtual machines.
You need to grant users PowerShell access to the virtual machine by using JIT VM access. What should you configure? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

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

TCP port that must be allowed: 22 / 25 / 3389 / 5986

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 78
- (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 83
- (Exam Topic 4)
You have an Azure subscription that contains an Azure key vault named ContosoKey1. You create users and assign them roles as shown in the following table.

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

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

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

Delegate permissions for ContosoKey1: User1 only / User1 and User2 only / User1 and User3 only / User1 and User4 only / User1, User2, and User3 only / User1, User2, User3, and User4

Configure network access to ContosoKey1: User1 only / User1 and User2 only / User1 and User3 only / User1 and User4 only / User1, User2, and User3 only / User1, User2, User3, and User4

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:

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

NEW QUESTION 85
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a hybrid configuration of Azure Active Directory (AzureAD). You have an Azure HDInsight cluster on a virtual network.
You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials. You need to configure the environment to support the planned authentication.
Solution: You create a site-to-site VPN between the virtual network and the on-premises network. Does this meet the goal?

A. Yes
B. No

Answer: A

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

NEW QUESTION 90
- (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 95
- (Exam Topic 4)
You have an Azure Active directory tenant that syncs with an Active Directory Domain Services (AD DS) domain.
You plan to create an Azure file share that will contain folders and files.
Which identity store can you use to assign permissions to the Azure file share and folders within the share? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Azure files share: [▼]

Folders in the file share: [▼]

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Azure files share: AD DS only

Folders in the file share: AD DS and Azure AD

NEW QUESTION 98
- (Exam Topic 4)
You have an Azure subscription that contains a web app named App1.
Users must be able to select between a Google identity or a Microsoft identity when authenticating to App1. You need to add Google as an identity provider in Azure AD.
Which two pieces of information should you configure? Each correct answer presents part of the solution. Each correct selection is worth one point

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

Answer: DE

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

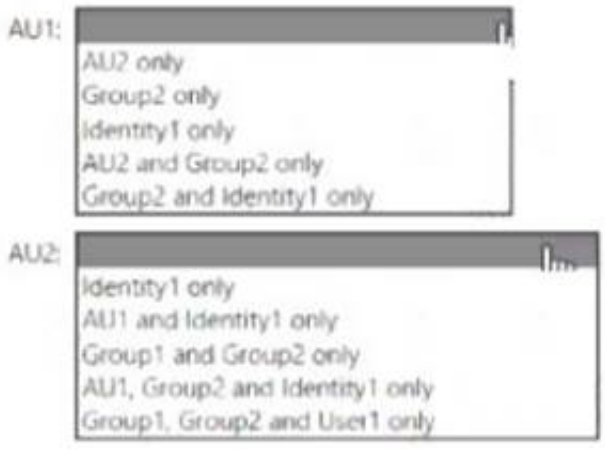
NEW QUESTION 99
- (Exam Topic 4)
You have an Azure subscription that has a managed identity named identity and is linked to an Azure Active Directory (Azure AD) tenant. The tenant contains the

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

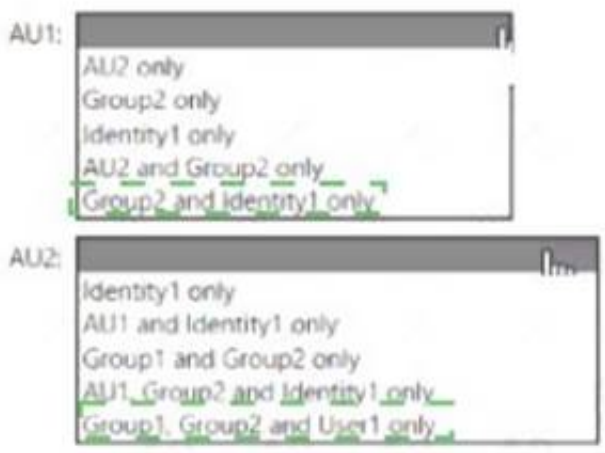


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 103
- (Exam Topic 4)
You create an alert rule that has the following settings:

- Resource: RG1
- Condition: All Administrative operations
- Actions: Action groups configured for this alert rule: ActionGroup1
- Alert rule name: Alert1

You create an action rule that has the following settings:

- Scope: VM1
- Filter criteria: Resource Type = "Virtual Machines"
- Define on this scope: Suppression
- Suppression config: From now (always)
- Name: ActionRule1

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

Statements	Yes	No
If you start VM1, an alert is triggered.	○	○
If you start VM2, an alert is triggered.	○	○
If you add a tag to RG1, an alert is triggered.	○	○

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 105
- (Exam Topic 4)
You need to create an Azure key vault. The solution must ensure that any object deleted from the key vault be retained for 90 days.
How should you complete the command? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

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

    -Location 'East US'  [ ▼ ]  [ ▼ ]
```

-EnabledForDeployment	-Confirm
-EnablePurgeProtection	-DefaultProfile
-Tag	-EnableSoftDelete
	-SKU

A. Mastered
B. Not Mastered

Answer: A

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

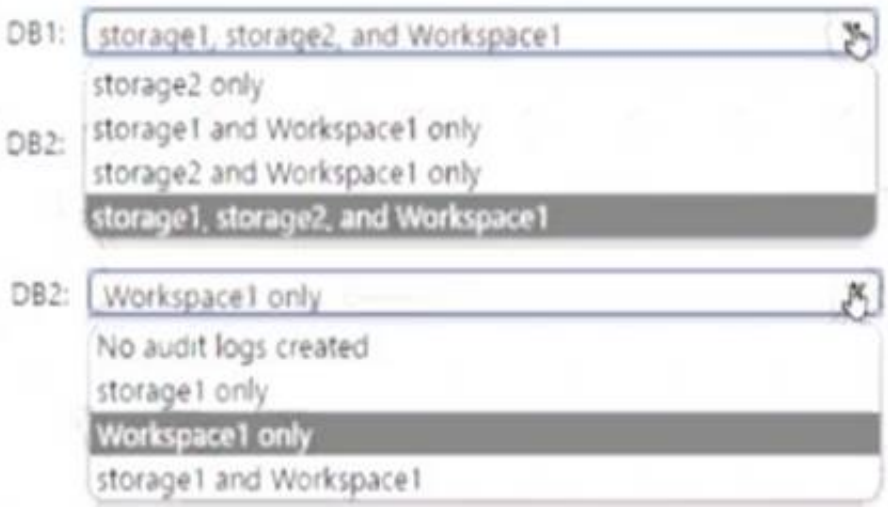
NEW QUESTION 110
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.

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

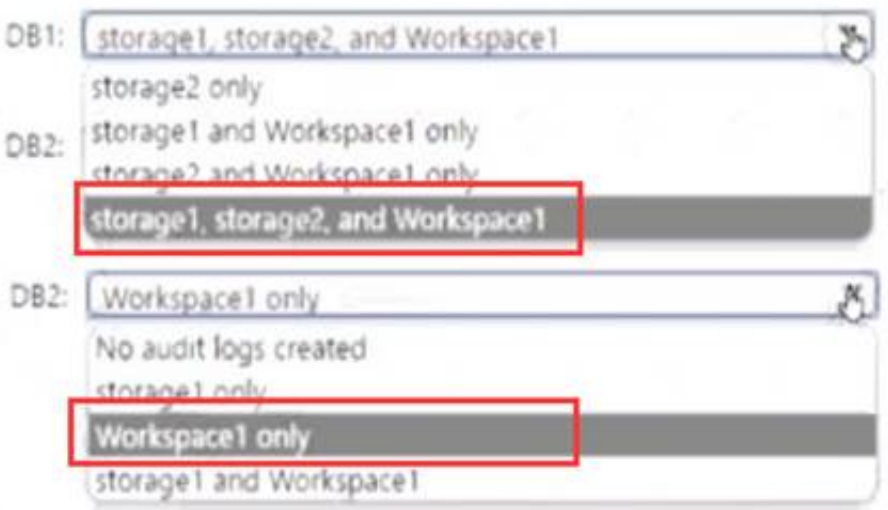


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 115
- (Exam Topic 4)
You have a web app named WebApp1.
You create a web application firewall (WAF) policy named WAF1. You need to protect WebApp1 by using WAF1.
What should you do first?

A. Deploy an Azure Front Door.
B. Add an extension to WebApp1.
C. Deploy Azure Firewall.

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/azure/frontdoor/quickstart-create-front-door

NEW QUESTION 118
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Subscription named Sub1.
You have an Azure Storage account named Sa1 in a resource group named RG1.
Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.
You discover that unauthorized users accessed both the file service and the blob service. You need to revoke all access to Sa1.
Solution: You generate new SASs. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Instead you should create a new stored access policy.

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 affects 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 123
- (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 127
- (Exam Topic 4)
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains a user named User1.
You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains an Azure Storage account named storage1. Storage1 contains an Azure file share named share1.
Currently, the domain and the tenant are not integrated.
You need to ensure that User1 can access share1 by using his domain credentials.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

- Create a private link to storage1.
- Enable Active Directory Domain Services (AD DS) authentication on storage1.
- Implement Azure AD Connect.
- Create a service endpoint to storage1.
- Assign share-level permissions for share1.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 129
- (Exam Topic 4)
You have an Azure subscription.
You plan to map an online infrastructure and perform vulnerability scanning for the following:
• ASNs
• Hostnames
• IP addresses

• SSL certificates What should you use?

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

Answer: A

NEW QUESTION 133
- (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 136
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant. You have the deleted objects shown in the following table.

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

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

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

Answer: BC

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

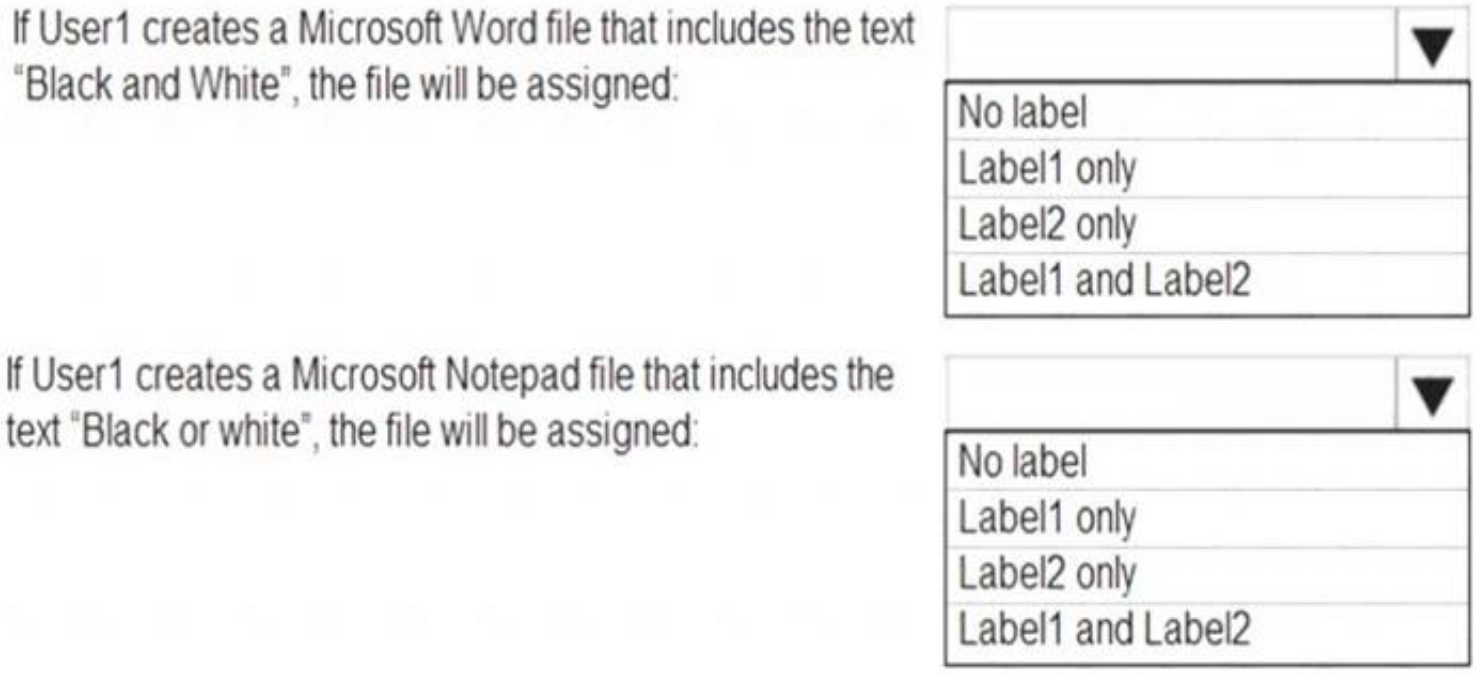
NEW QUESTION 139
- (Exam Topic 4)
You have the Azure Information Protection conditions shown in the following table.

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.



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 140
- (Exam Topic 4)
You have an Azure subscription that contains the virtual machines shown in the following table.

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

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

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

On which virtual machines is the Microsoft Monitoring agent installed?

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

Answer: D

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

NEW QUESTION 144
- (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 145
- (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 146
- (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 149
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.

Name	Type
LB1	Azure Standard Load Balancer
VM1	Virtual machine
SQL1	Azure SQL Database
VMSS1	Virtual machine scale set

You plan to deploy an Azure Private Link service named APL1. Which resource must you reference during the creation of APL1?

A. VMSS1
B. VM1
C. SQL
D. LB1

Answer: D

NEW QUESTION 154
- (Exam Topic 4)
You have a web app hosted on an on-premises server that is accessed by using a URL of https://www.contoso.com. You plan to migrate the web app to Azure.
You will continue to use https://www.contoso.com. You need to enable HTTPS for the Azure web app. What should you do first?

A. Export the public key from the on-premises server and save the key as a P7b file.
B. Export the private key from the on-premises server and save the key as a PFX file that is encrypted by using TripleDES.
C. Export the public key from the on-premises server and save the key as a CER file.
D. Export the private key from the on-premises server and save the key as a PFX file that is encrypted by using AES256.

Answer: B

Explanation:
https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate#private-certificate-requirements

NEW QUESTION 155
- (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 156
- (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 158
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result these questions will not appear in the review screen.
You use Azure Security Center for the centralized policy management of three Azure subscriptions. You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create a policy initiative and assignments that are scoped to resource groups. Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 159
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.

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

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

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

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

Name	Resource group	TDE
SQL2	RG2	Disabled
SQL3	RG1	Disabled

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

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 161
- (Exam Topic 4)
You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant. From the Azure portal, you register an enterprise application.
Which additional resource will be created in Azure AD?

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

Answer: A

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

NEW QUESTION 165
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant named contoso.com
You need to configure diagnostic settings for contoso.com. The solution must meet the following requirements:

• Retain loqs for two years.
• Query logs by using the Kusto query language
• Minimize administrative effort. Where should you store the logs?

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

Answer: A

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

NEW QUESTION 167
- (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

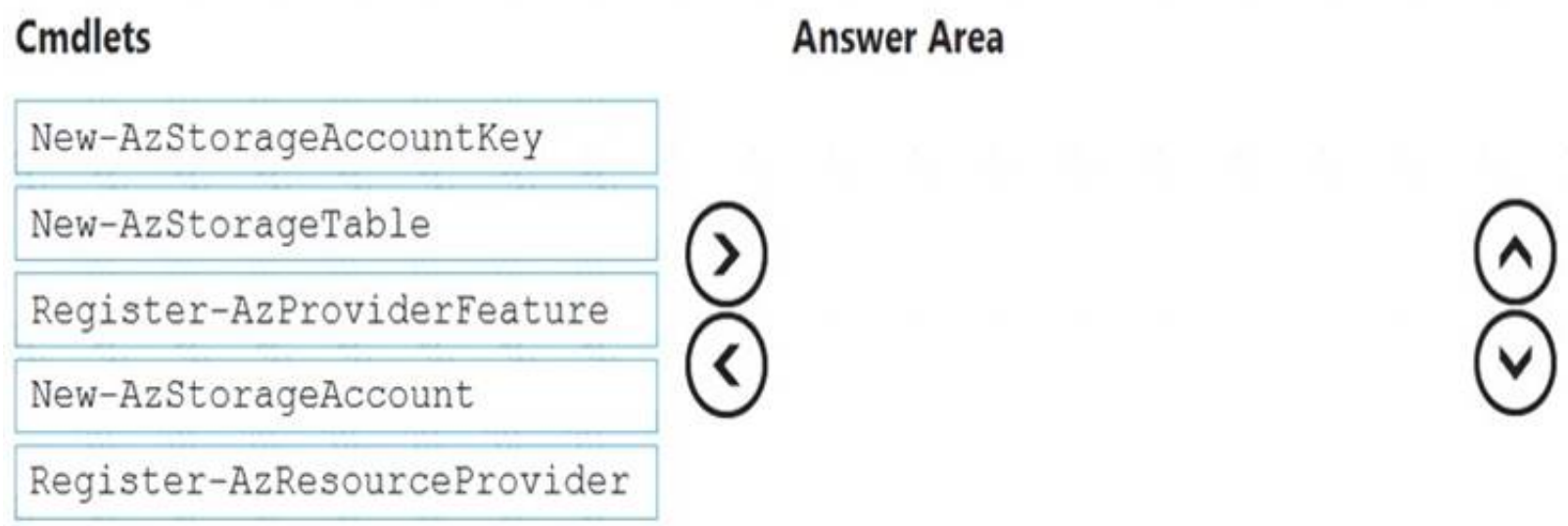
Answer: B

NEW QUESTION 170
- (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 173
- (Exam Topic 4) You have an Azure subscription. You plan to create a storage account.
You need to use customer-managed keys to encrypt the tables in the storage account.
From Azure Cloud Shell, which three cmdlets should you run in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

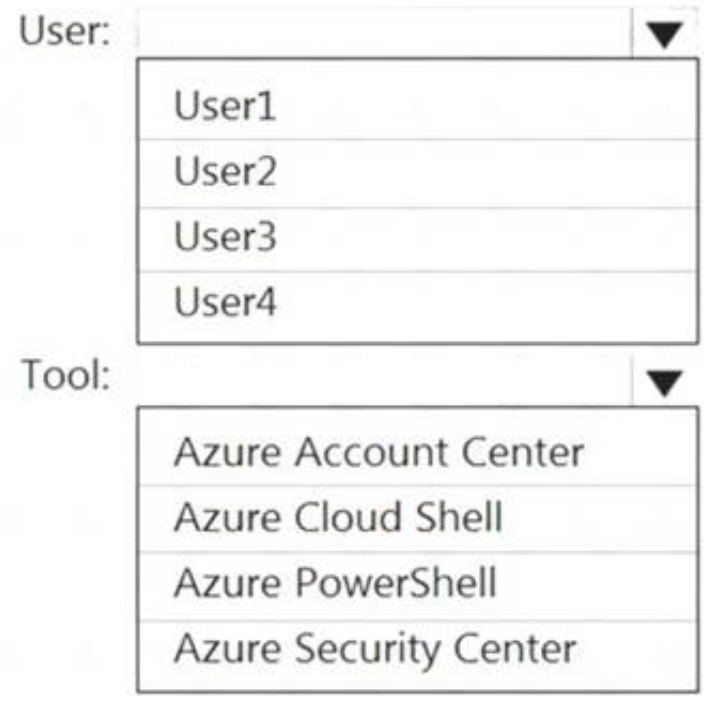
Answer: A

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

NEW QUESTION 176
- (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 179
- (Exam Topic 4)
Lab Task
use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password. place your cursor in the Enter password box and click on the password below. Azure Username: Userl -28681041@ExamUsers.com
Azure Password: GpOAe4@lDg
If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only: Lab Instance: 28681041
Task 3
The developers at your company plan to create a web app named App28681041 and to publish the app to https://www.contoso.com. You need to perform the following tasks:
• Ensure that App28681041 is registered to Azure AD.
• Generate a password for App28681041.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
To register App28681041 to Azure AD and generate a password for it, you can follow these steps:
- In the Azure portal, search for and select Azure Active Directory.
- In the left pane, select App registrations.
- Select New registration.
- In the Register an application pane, enter the following information:
- Name: App28681041
- Supported account types: Select the appropriate account types for your scenario.
- Redirect URI: Leave this field blank.
- Select Register.
- In the App registrations pane, select the newly created App28681041 application.
- In the left pane, select Certificates & secrets.
- Select New client secret.

- In the Add a client secret pane, enter the following information:
- Description: Enter a description for the client secret.
- Expires: Select an appropriate expiration date for the client secret.
- Select Add.
- In the Certificates & secrets pane, copy the value of the newly created client secret.

You can find more information on this topic in the following Microsoft documentation: Quickstart: Register an application with the Microsoft identity platform.

NEW QUESTION 184
- (Exam Topic 4)
You have a Azure subscription.
You enable Azure Active Directory (Azure AD) Privileged identify (PIM).
Your company's security policy for administrator accounts has the following conditions:
* The accounts must use multi-factor authentication (MFA).
* The account must use 20-character complex passwords.
* The passwords must be changed every 180 days.
* The account must be managed by using PIM.
You receive alerts about administrator who have not changed their password during the last 90 days. You need to minimize the number of generated alerts.
Which PIM alert should you modify?

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

Answer: D

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

NEW QUESTION 188
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains a user named Admin1. Admin1 is assigned the Application developer role.
You purchase a cloud app named App1 and register App1 in Azure AD.
Admin1 reports that the option to enable token encryption for App1 is unavailable.
You need to ensure that Admin1 can enable token encryption for App1 in the Azure portal. What should you do?

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

Answer: C

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

NEW QUESTION 189
- (Exam Topic 4)
Lab Task
use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password. place your cursor in the Enter password box and click on the password below. Azure Username: Userl -28681041@ExamUsers.com
Azure Password: GpOAe4@lDg
If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only: Lab Instance: 28681041
Task 10
You need to create a new Azure AD directory named 28681041.onmicrosoft.com. The new directory must contain a new user named user1@28681041.onmicrosoft.com.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
To create a new Azure AD directory named 28681041.onmicrosoft.com that contains a new user named user1@28681041.onmicrosoft.com, you can follow these steps:
- In the Azure portal, search for and select Azure Active Directory.
- In the left pane, select Domains.
- Select Add domain.
- In the Add a custom domain pane, enter the following information:
-

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

You can find more information on these topics in the following Microsoft documentation:
- Add a custom domain name to Azure Active Directory
- Create a new user in your organization - Azure Active Directory

NEW QUESTION 194
- (Exam Topic 4)
You have an Azure subscription that contains an Azure key vault and an Azure Storage account. The key vault contains customer-managed keys. The storage account is configured to use the customer-managed keys stored In the key vault.
You plan to store data in Azure by using the following services:
* Azure Files
* Azure Blob storage
* Azure Log Analytics
* Azure Table storage
* Azure Queue storage
Which two services data encryption by using the keys stored in the key vault? Each correct answer present a complete solution.
NOTE: Each correct selection is worth one point.

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

Answer: AC

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

NEW QUESTION 199
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant named Contoso.com and an Azure Service (AKS) cluster AKS1.
You discover that AKS1 cannot be accessed by using accounts from Contoso.com
You need to ensure AKS1 can be accessed by using accounts from Contoso.com The solution must minimize administrative effort.
What should you do first?

A. From Azure recreate AKS1,
B. From AKS1, upgrade the version of Kubermetes.
C. From Azure AD, implement Azure AD Premium P2.
D. From Azure AD, configure the User settings

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli

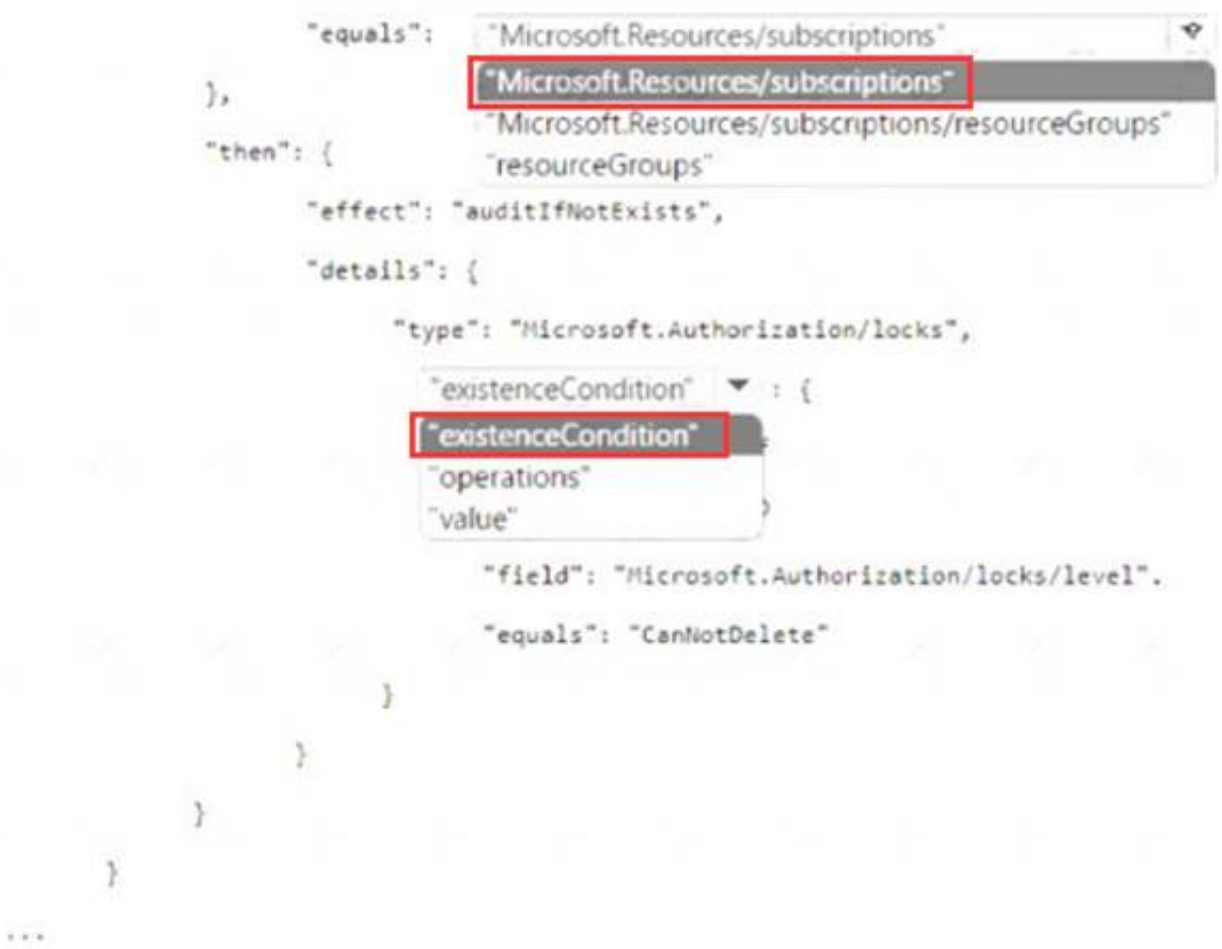
NEW QUESTION 201
- (Exam Topic 4)
You plan to deploy a custom policy initiative for Microsoft Defender for Cloud. You need to identify all the resource groups that have a Delete lock.
How should you complete the policy definition? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area



NEW QUESTION 204

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

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

Answer: B

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

NEW QUESTION 208
- (Exam Topic 4)
You have an Azure subscription that contains the virtual machines shown in the following table.

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

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

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

Answer: A

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

NEW QUESTION 210
- (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 213
- (Exam Topic 4)
You have the Azure virtual machines shown in the following table.

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

Each virtual machine has a single network interface.
You add the network interface of VM1 to an application security group named ASG1.
You need to identify the network interfaces of which virtual machines you can add to ASG1. What should you identify?

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

Answer: D

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

NEW QUESTION 218
- (Exam Topic 4)
You have an Azure subscription named Sub1.
In Azure Security Center, you have a workflow automation named WF1. WF1 is configured to send an email message to a user named User1.
You need to modify WF1 to send email messages to a distribution group named Alerts. What should you use to modify WF1?

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

Answer: C

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

NEW QUESTION 223
- (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?

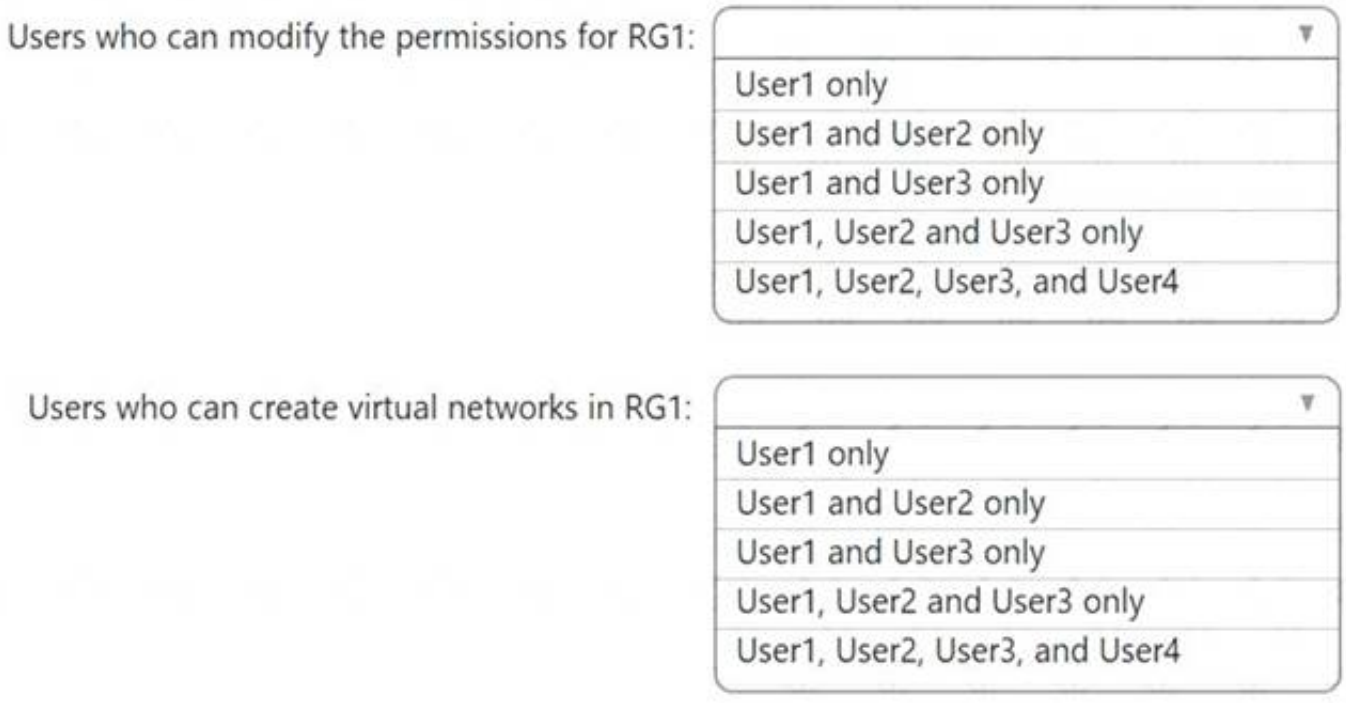
A. Attack Surface Summary
B. GDPRCompliance
C. Security Posture
D. OWASPToplO

Answer: D

NEW QUESTION 224
- (Exam Topic 4)
You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

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

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



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 229
- (Exam Topic 4)
You have an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry. You need to use automatically generated service principal for the AKS cluster to authenticate to the Azure
Container Registry.
What should you create?

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

Answer: B

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

NEW QUESTION 230
- (Exam Topic 4)
You have an Azure Storage account named storage1 that has a container named container1. You need to prevent the blobs in container1 from being modified.
What should you do?

A. From container1, change the access level.
B. From container1 add an access policy.
C. From container1, modify the Access Control (1AM) settings.
D. From storage1 , enable soft delete for blobs.

Answer: B

Explanation:

References:
https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutable-storage?tabs=azure-portal

NEW QUESTION 234
- (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 237
- (Exam Topic 4)
You have 10 virtual machines on a single subnet that has a single network security group (NSG). You need to log the network traffic to an Azure Storage account.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

Answer: D

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

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

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

NEW QUESTION 242
- (Exam Topic 4)
You have an Azure key vault named KeyVault1 that contains the items shown in the following table.

Name	Type
Item1	Key
Item2	Secret
Policy1	Access policy

In KeyVault, the following events occur in sequence:

- Item1 is deleted
- Administrator enables soft delete
- Item2 and Policy1 are deleted.

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

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

A. Mastered
B. Not Mastered

Answer: A

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

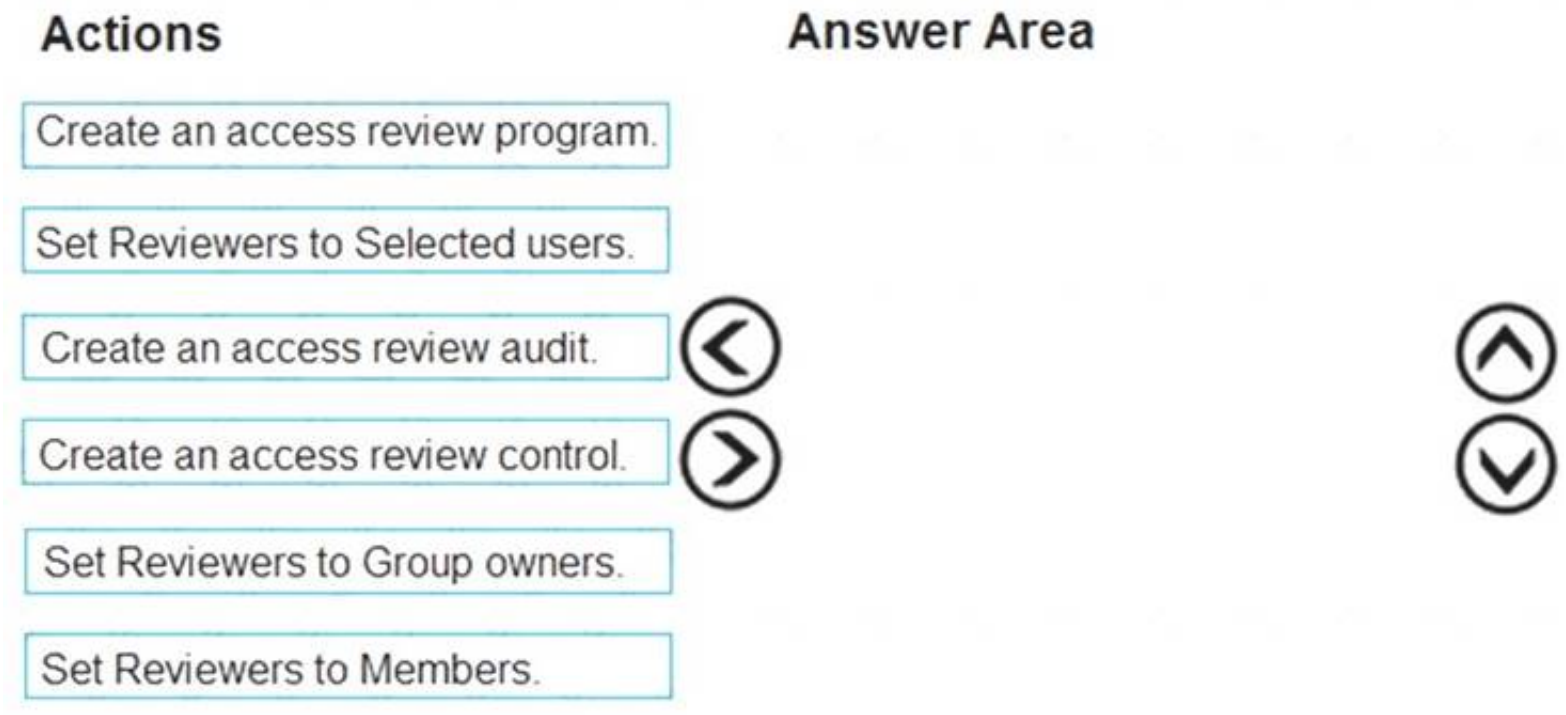
NEW QUESTION 247
- (Exam Topic 4)
From Azure Security, you create a custom alert rule.
You need to configure which users will receive an email message when the alert is triggered. What should you do?

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

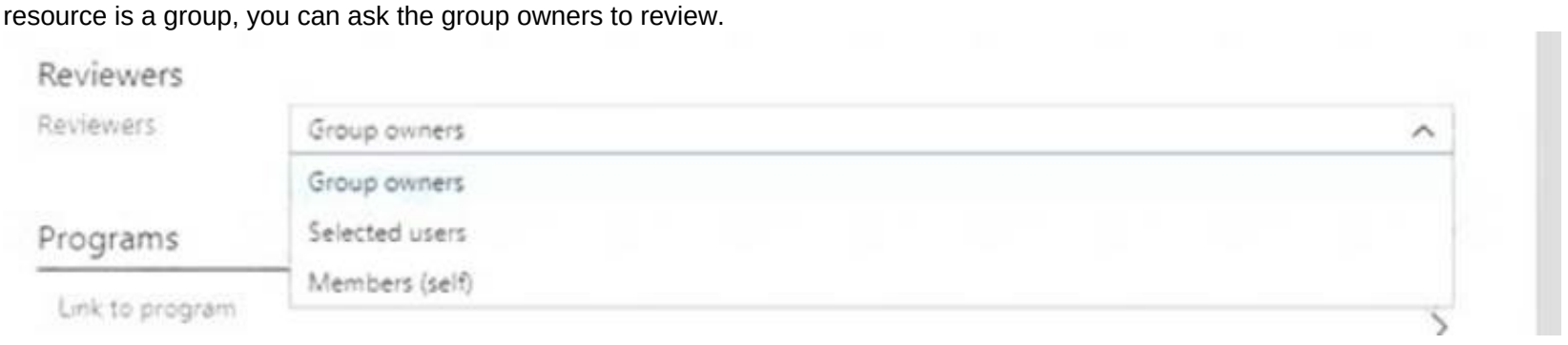
NEW QUESTION 251
- (Exam Topic 4)
You need to configure an access review. The review will be assigned to a new collection of reviews and reviewed by resource owners.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area 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.

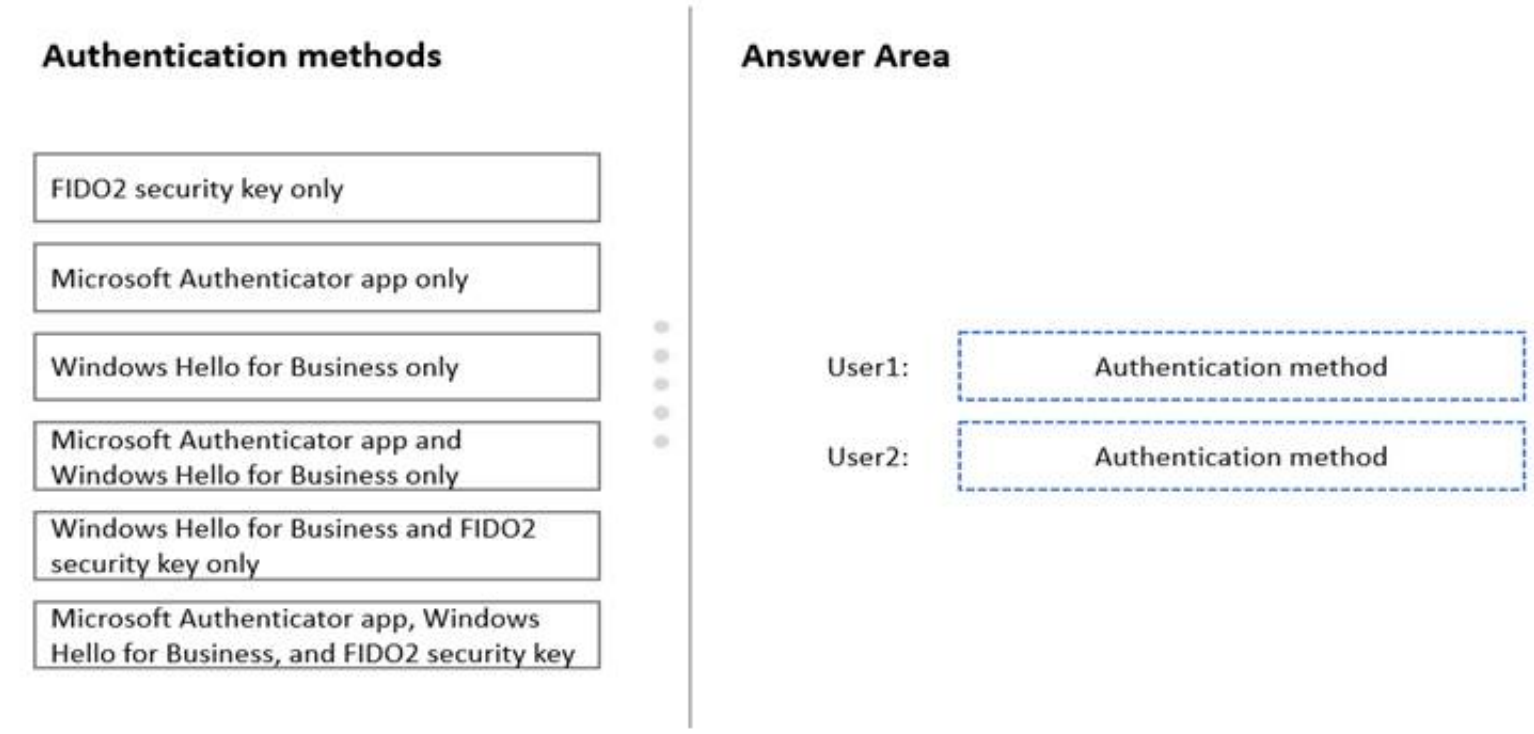


References:
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-programs-controls

NEW QUESTION 253
- (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

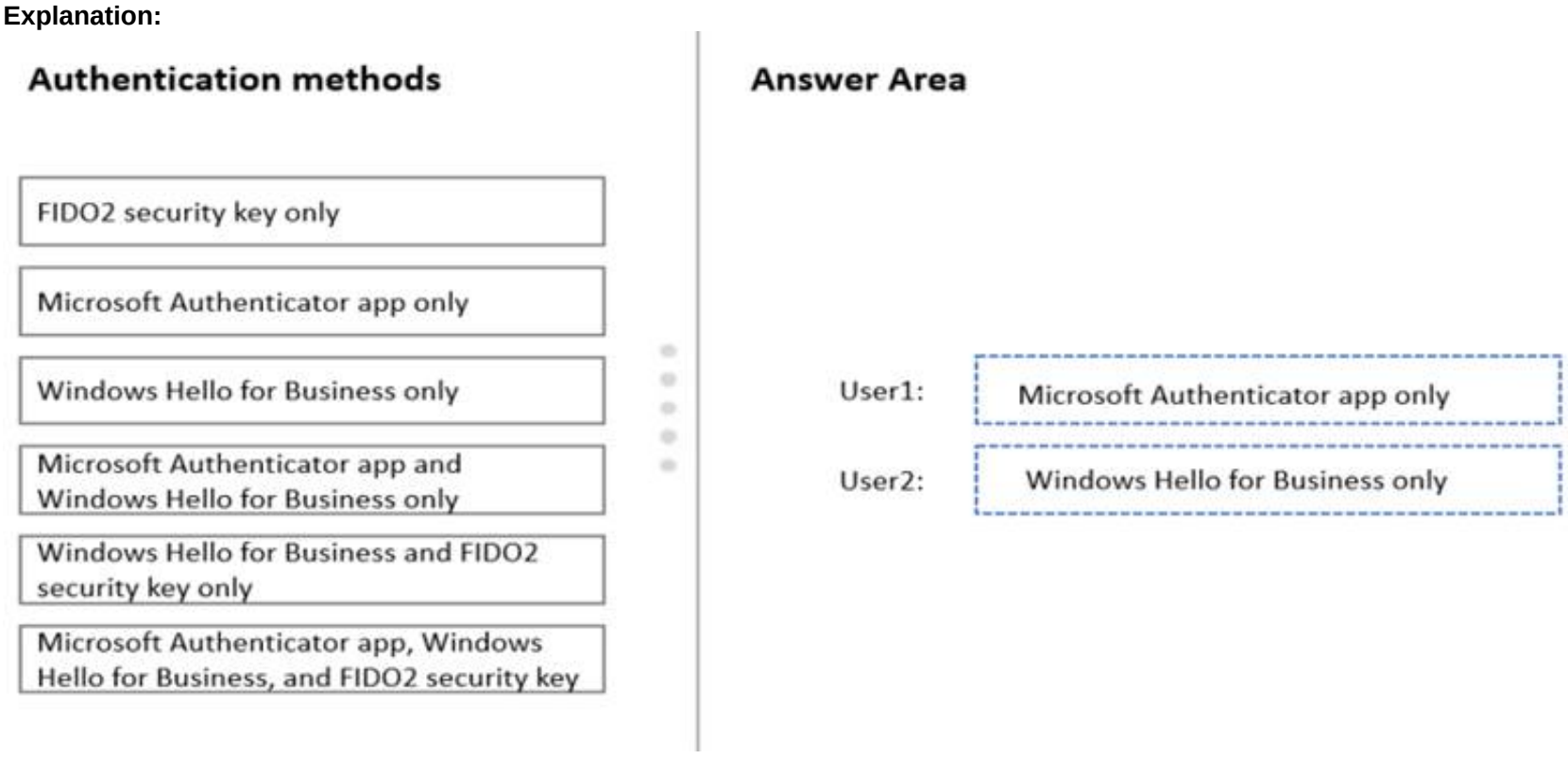
You enable passwordless authentication for the tenant.
Which authentication method can each user use for passwordless authentication? To answer, drag the appropriate authentication methods to the correct users.
Each authentication method may be used once, more than once, or not at all. You may need to 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:



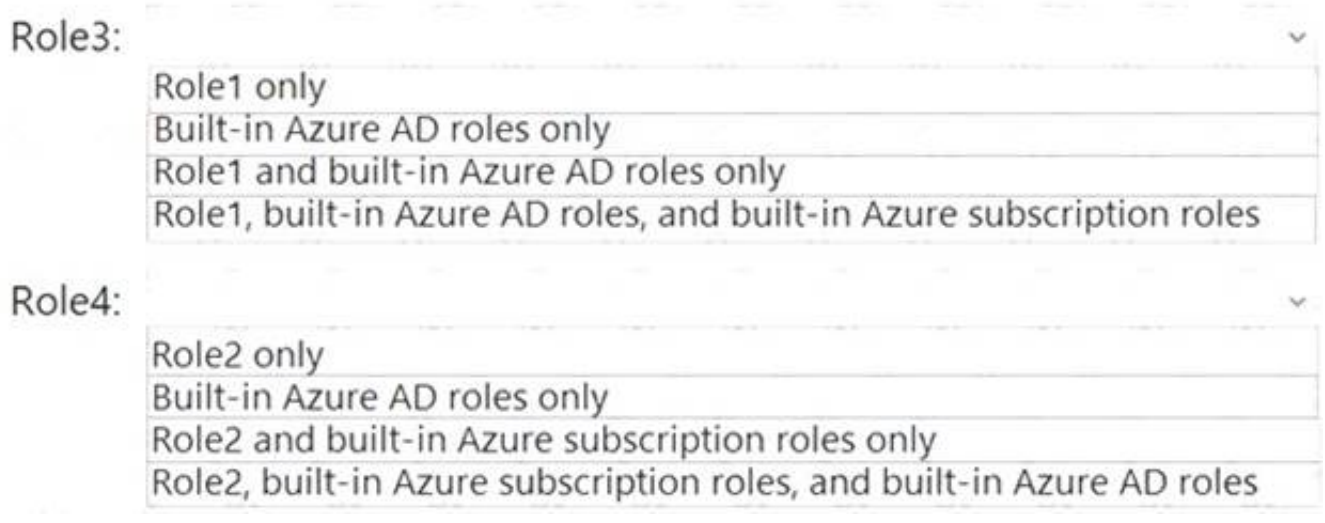
NEW QUESTION 258
- (Exam Topic 4)
You have an Azure subscription that contains the custom roles shown in the following table.

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

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

Name	Type
Role3	Azure AD
Role4	Azure subscription

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

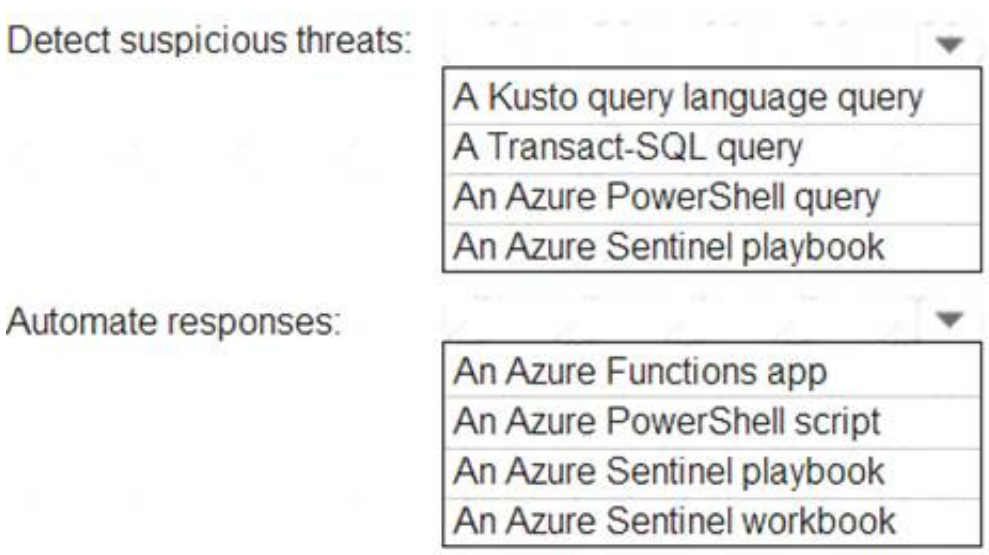


A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application, email Description automatically generated
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/custom-create https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal

NEW QUESTION 260
- (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.

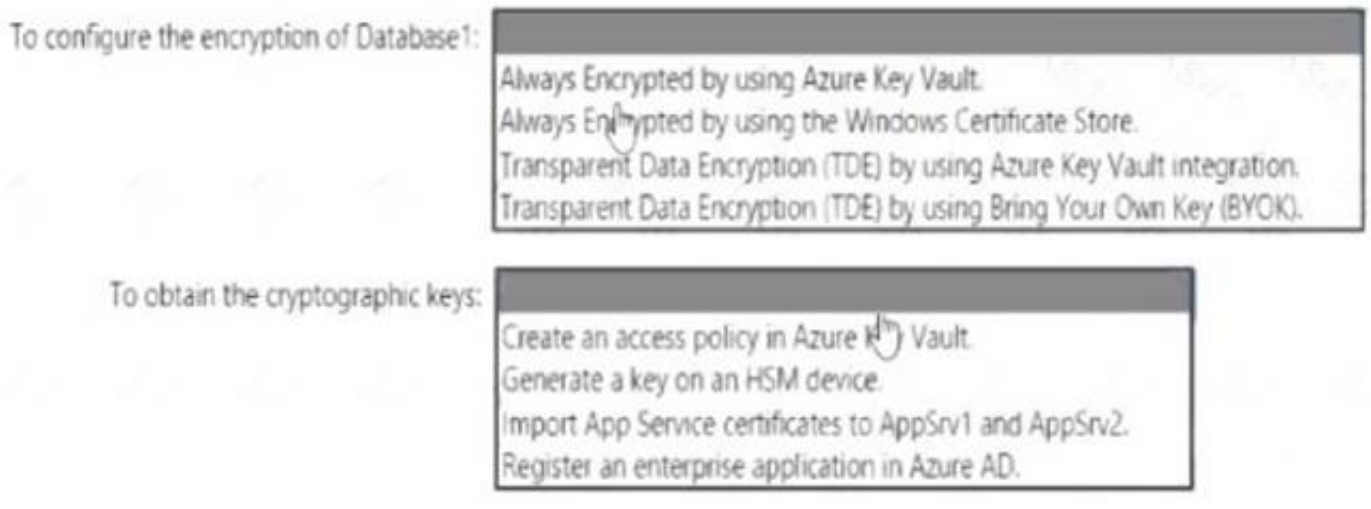


A. Mastered
B. Not Mastered

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 263
- (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 264
- (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

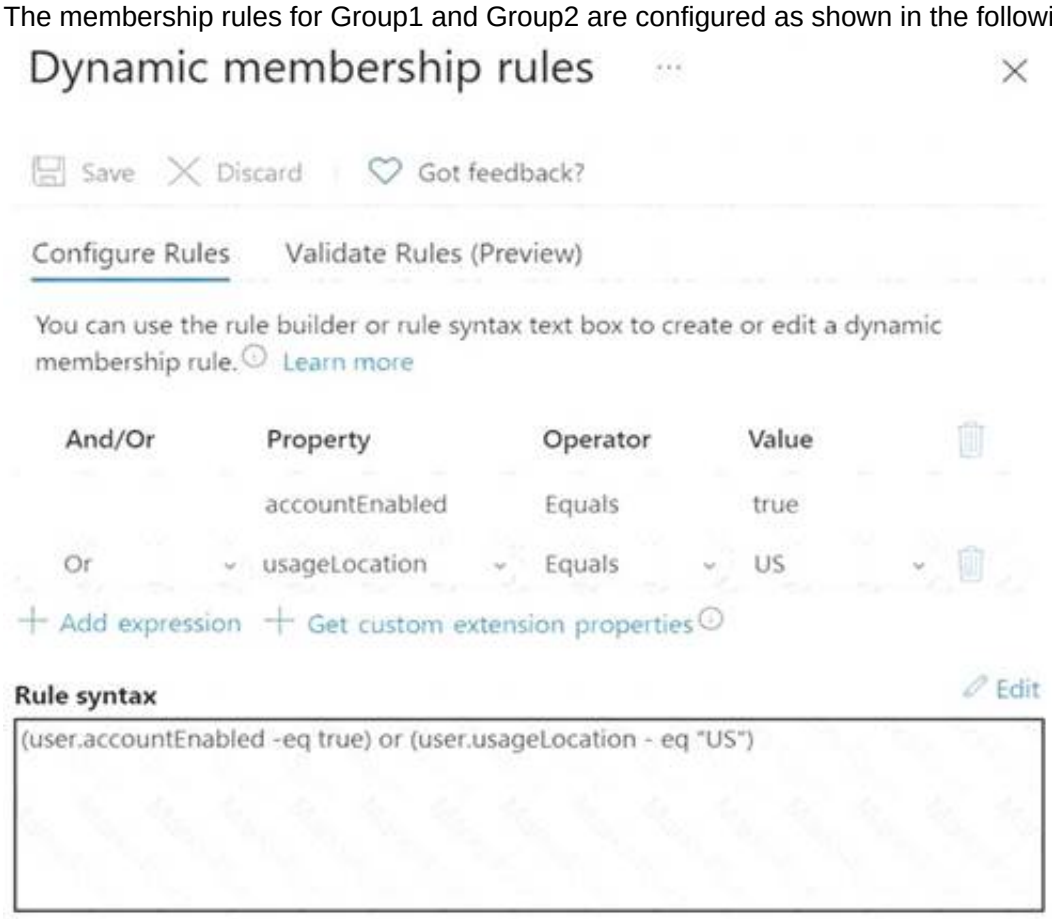
The subscription is linked to an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

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

Name	Type	Region	Resource group
SQL1	Azure SQL database	East US	RG1
Analytics1	Azure Log Analytics workspace	East US	RG1
Analytics2	Azure Log Analytics workspace	East US	RG2
Analytics3	Azure Log Analytics workspace	West Europe	RG1

You create the Azure Storage accounts shown in the following table.

Name	Region	Resource group	Storage account type	Access tier (default)
Storage1	East US	RG1	Blob	Cool
Storage2	East US	RG2	General purpose V1	*Not applicable*
Storage3	West Europe	RG1	General purpose V2	Hot

You need to configure auditing for SQL1.
Which storage accounts and Log Analytics workspaces can you use as the audit log destination? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Answer Area

Storage accounts that can be used as the audit log destination:
- Storage1 only
- Storage2 only
- Storage1 and Storage2 only
- Storage1, Storage2, and Storage3

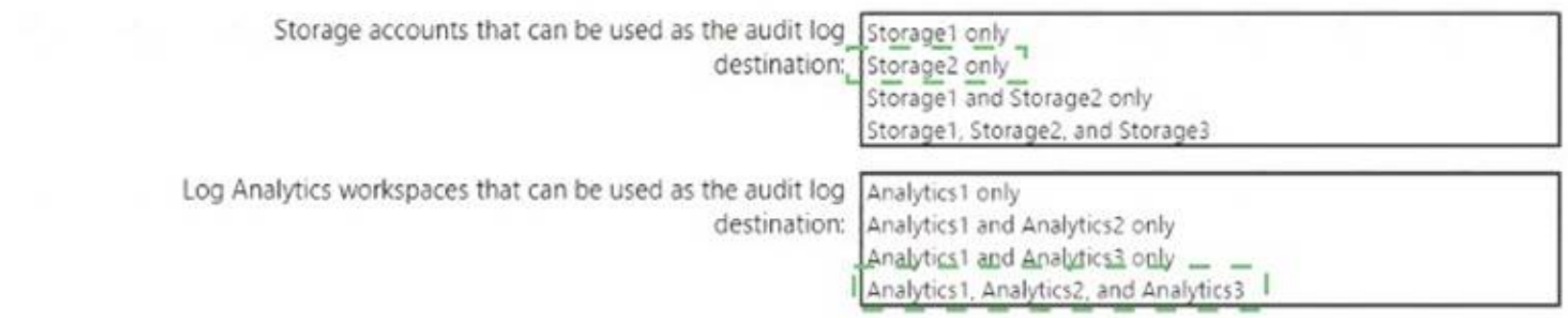
Log Analytics workspaces that can be used as the audit log destination:
- Analytics1 only
- Analytics1 and Analytics2 only
- Analytics1 and Analytics3 only
- Analytics1, Analytics2, and Analytics3

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 269
- (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

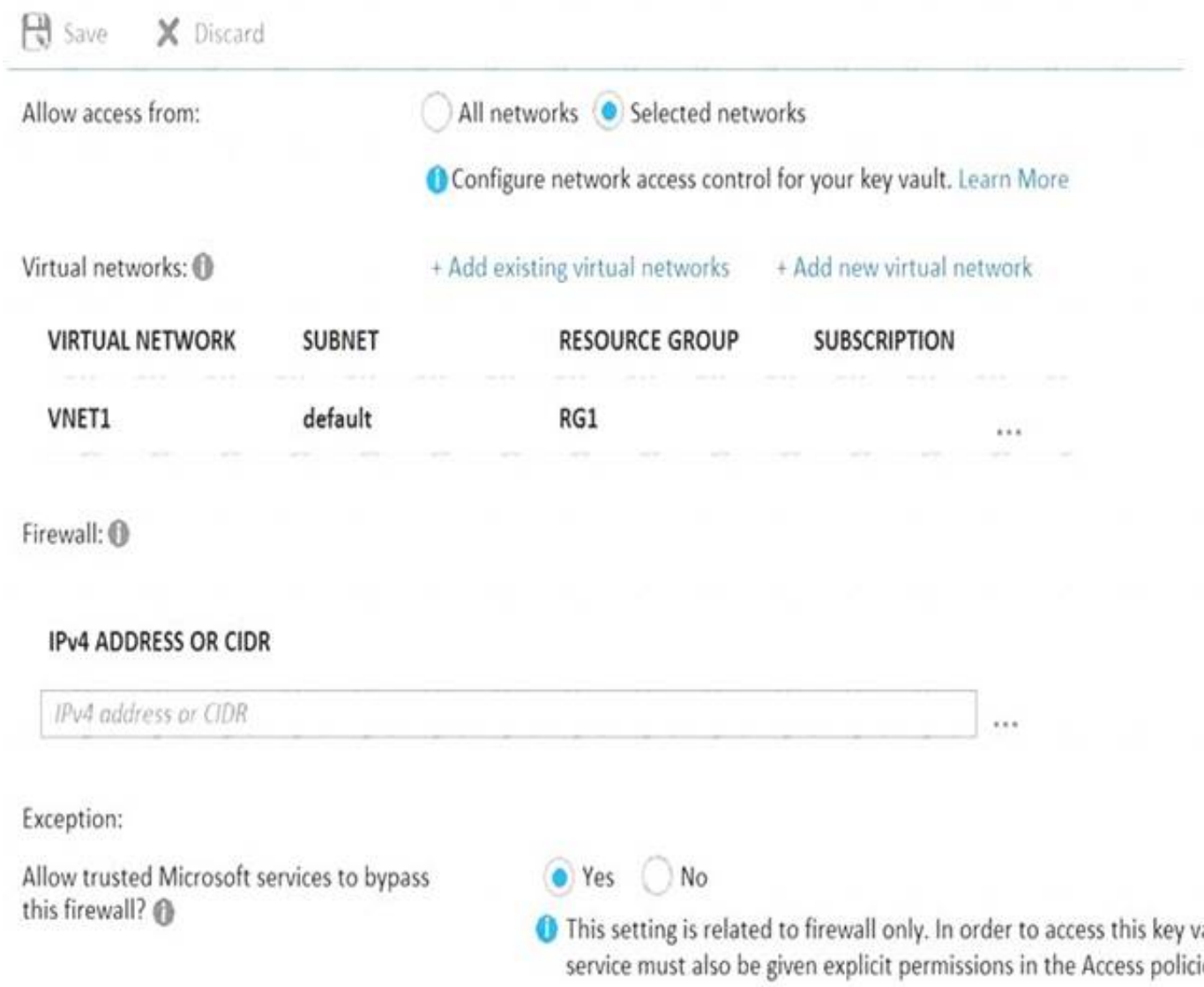
Answer: A

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

NEW QUESTION 273
- (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 278
- (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 283
- (Exam Topic 4)
On Monday, you configure an email notification in Azure Security Center to notify user user1@contoso.com. On Tuesday, Security Center generates the security alerts shown in the following table.

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

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

Total number of Security Center email notifications about an RDP brute force attack on Tuesday:
- 1
- 2
- 3
- 4

Total number of Security Center email notifications on Tuesday:
- 3
- 4
- 6
- 9
- 11

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details

NEW QUESTION 287
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant.
You need to prevent nonprivileged Azure AD users from creating service principals in Azure AD. What should you do in the Azure Active Directory admin center of the tenant?

A. From the Properties Wade, set Enable Security defaults to Yes.
B. From the Properties blade, set Access management fen Azure resources to No
C. From the User settings blade, set Users can register applications to No
D. From the User settings blade, set Restrict access to Azure AD administration portal to Yes.

Answer: C

NEW QUESTION 291
- (Exam Topic 4)
You have a Microsoft Sentinel deployment.
You need to connect a third-party security solution to the deployment. The third-party solution will send Common Event Format (CER-formatted messages.
What should you include in the solution? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Deploy: [ ]

Forward events to Microsoft Sentinel by using: [ ]

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Deploy: A Windows server and a Windows Event Forwarding subscription

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

NEW QUESTION 296
- (Exam Topic 4)
You have an Azure subscription that contains several Azure SQL databases and an Azure Sentinel workspace.
You need to create a saved query in the workspace to find events reported by Advanced Threat Protection for Azure SQL Database.
What should you do?

A. From Azure CLI run the Get-AzOperationalInsightsworkspace cmdlet.
B. From the Azure SQL Database query editor, create a Transact-SQL query.
C. From the Azure Sentinel workspace, create a Kusto Query Language query.
D. From Microsoft SQL Server Management Studio (SSMS), create a Transact-SQL query.

Answer: C

NEW QUESTION 297
- (Exam Topic 4)
Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
Your company has an Active Directory forest with a single domain, named weylandindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.
You have been tasked with integrating Active Directory and the Azure AD tenant. You intend to deploy Azure AD Connect.
Your strategy for the integration must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.
Solution: You recommend the use of federation with Active Directory Federation Services (AD FS). Does the solution meet the goal?

A. Yes
B. No

Answer: B

Explanation:
A federated authentication system relies on an external trusted system to authenticate users. Some companies want to reuse their existing federated system investment with their Azure AD hybrid identity solution. The maintenance and management of the federated system falls outside the control of Azure AD. It's up to the organization by using the federated system to make sure it's deployed securely and can handle the authentication load.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

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

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

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

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

Answer: C

NEW QUESTION 305
- (Exam Topic 4)
You have an Azure subscription named Sub1 that contains the Azure key vaults shown in the following table:

Name	Region	Resource group
Vault1	West Europe	RG1
Vault2	East US	RG1
Vault3	West Europe	RG2
Vault4	East US	RG2

In Sub1, you create a virtual machine that has the following configurations:
- Name: VM1
- Size: DS2v2
- Resource group: RG1
- Region: West Europe
- Operating system: Windows Server 2016

You plan to enable Azure Disk Encryption on VM1.
In which key vaults can you store the encryption key for VM1?

A. Vault1 or Vault3 only
B. Vault1, Vault2, Vault3, or Vault4
C. Vault1 only
D. Vault1 or Vault2 only

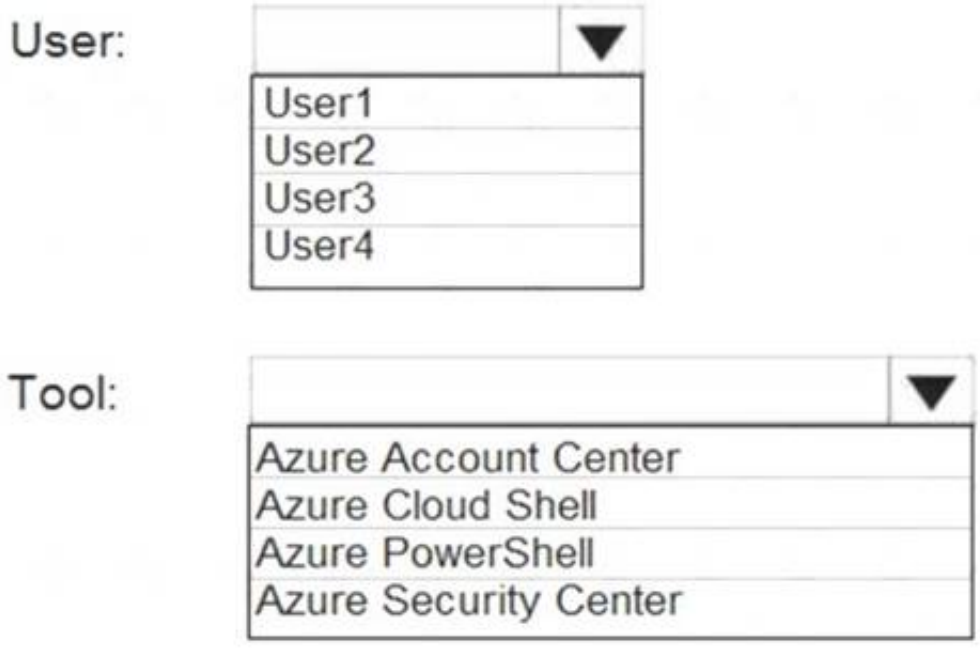
Answer: A

Explanation:
In order to make sure the encryption secrets don't cross regional boundaries, Azure Disk Encryption needs the Key Vault and the VMs to be co-located in the same region. Create and use a Key Vault that is in the same region as the VM to be encrypted.
Reference:
https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-prerequisites

NEW QUESTION 309
- (Exam Topic 4)
HOTSPOT
Your company has an Azure subscription named Subscription1 that contains the users shown in the following table.

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

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



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 312
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
RG1	Resource group	Used to store virtual machines
RG2	Resource group	Used to store virtual networks
ServerAdmins	Security group	Used to manage virtual machines

You need to ensure that ServerAdmins can perform the following tasks:
- Create virtual machines in RG1 only.
- Connect the virtual machines to the existing virtual networks in RG2 only.

The solution must use the principle of least privilege.
Which two role-based access control (RBAC) roles should you assign to ServerAdmins? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. a custom RBAC role for RG2
B. the Network Contributor role for RG2
C. the Contributor role for the subscription
D. a custom RBAC role for the subscription
E. the Network Contributor role for RG1
F. the Virtual Machine Contributor role for RG1

Answer: AF

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

NEW QUESTION 314
- (Exam Topic 4)
Your company recently created an Azure subscription.
You have been tasked with making sure that a specified user is able to implement Azure AD Privileged Identity Management (PIM).
Which of the following is the role you should assign to the user?

A. The Global administrator role.
B. The Security administrator role.
C. The Password administrator role.
D. The Compliance administrator role.

Answer: A

Explanation:
To start using PIM in your directory, you must first enable PIM.

* 1. Sign in to the Azure portal as a Global Administrator of your directory.
You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com), to enable PIM for a directory.
Scenario: Technical requirements include: Enable Azure AD Privileged Identity Management (PIM) for contoso.com
Reference:
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-started

NEW QUESTION 319
- (Exam Topic 4)
You have an Azure subscription.
You create a new virtual network named VNet1.
You plan to deploy an Azure web app named App1 that will use VNet1 and will be reachable by using private IP addresses. The solution must support inbound and outbound network traffic.
What should you do?

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

Answer: D

NEW QUESTION 324
- (Exam Topic 4)
Your company plans to create separate subscriptions for each department. Each subscription will be associated to the same Azure Active Directory (Azure AD) tenant.
You need to configure each subscription to have the same role assignments. What should you use?

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

Answer: D

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

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

NEW QUESTION 329
- (Exam Topic 4)
You have an Azure subscription that contains the resources show in the following table.

Name	Type
DB1	Azure Cosmos DB account
VM1	Virtual machine
VM2	Virtual machine
VNET1	Virtual network
NSG1	Network security group (NSG)

Both VM1 and VM2 connect to VNET1 and are configured to use NSG1. You need to ensure that only VM1 and VM2 can access DB1.
What should you do?

A. Add the IP address range of VNET1 to the Firewall setting of DB1.
B. For NSG1, configure a rule that has a service tag.
C. Create an application security group.
D. Configure DB1 to allow access from only VNET1.

Answer: B

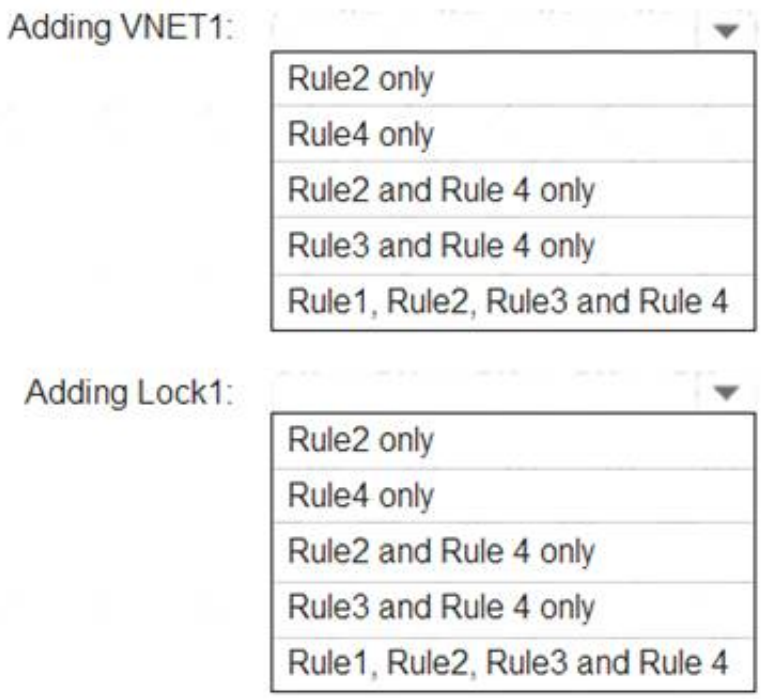
NEW QUESTION 331
- (Exam Topic 4)
You have an Azure subscription that contains a user named Admin1 and a resource group named RG1. In Azure Monitor, you create the alert rules shown in the following table.

Name	Resource	Condition
Rule1	RG1	All security operations
Rule2	RG1	All administrative operations
Rule3	Azure subscription	All security operations by Admin1
Rule4	Azure subscription	All administrative operations by Admin1

Admin1 performs the following actions on RG1:

- Adds a virtual network named VNET1
- Adds a Delete lock named Lock1

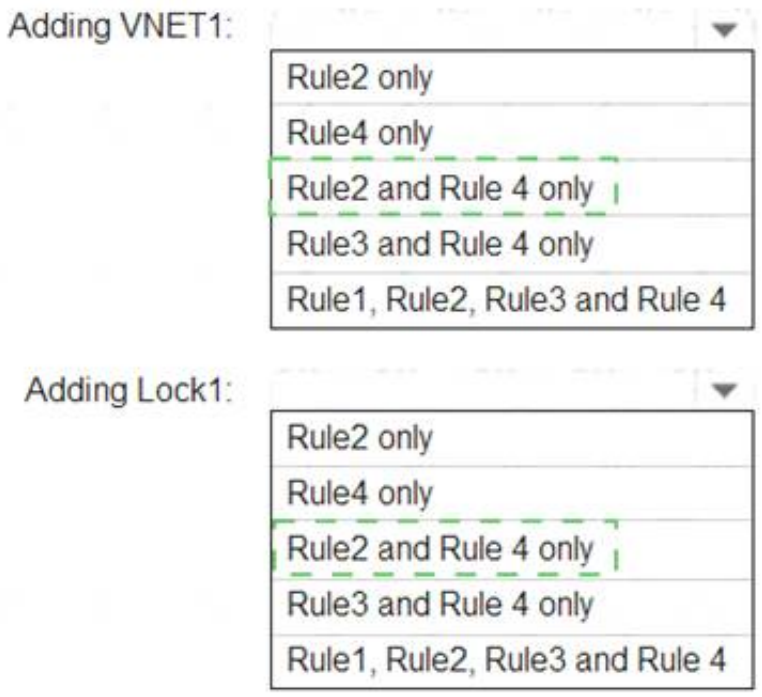
Which rules will trigger an alert as a result of the actions of Admin1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 334
- (Exam Topic 4)
You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Azure region	Connected to	Associated network security group (NSG)
VM1	West US	VNET1/Subnet1	*None*
VM2	West US	VNET1/Subnet2	NSG2
VM3	Central US	VNET2/Subnet1	NSG3
VM4	West US	VNET3/Subnet1	NSG4

VNET1, VNET2, and VNET3 are peered with each other. You perform the following actions:
* Create two application security groups named ASG1 and ASG2 in the West US region.
* Add the network interface of VM1 to ASG1.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 337
- (Exam Topic 4)
You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016.
You need to implement a policy to ensure that each virtual machine has a custom antimalware virtual machine extension installed.
How should you complete 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:
Box 1: DeployIfNotExists
DeployIfNotExists executes a template deployment when the condition is met. Box 2: Template
The details property of the DeployIfNotExists effects has all the subproperties that define the related resources to match and the template deployment to execute.
Deployment [required]
This property should include the full template deployment as it would be passed to the Microsoft.Resources/deployment
References:
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

NEW QUESTION 339

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

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

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

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

Answer: D

NEW QUESTION 344
- (Exam Topic 4)
You have an Azure Subscription that is linked to an Azure Active Directory (Azure AD). The tenant contains the users shown in the following table.

Name	Role	Member of
User1	Security administrator	Group1
User2	Network Contributor	Group2
User3	Key Vault Contributor	Group1, Group2

You have an Azure key vault named Vault1 that has Purge protection set to Disabled. Vault1 contains the access policies shown in the following table.

Name	Key permission	Secret permission	Certificate permission
Group1	Purge	Purge	Purge
Group2	Select all	Select all	Select all

You create role assignments for Vault1 as shown in the following table.

Name	Role
User1	None
User2	Key Vault Reader
User3	User Access Administrator

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

Answer Area

Statements	Yes	No
User1 can set Purge protection to Enable for Vault1.	○	○
User2 can configure firewalls and virtual networks for Vault1.	○	○
User3 can add access policies to Vault1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can set Purge protection to Enable for Vault1.	○	○
User2 can configure firewalls and virtual networks for Vault1.	○	○
User3 can add access policies to Vault1.	○	○

NEW QUESTION 349
- (Exam Topic 4)

You have an Azure AD tenant that contains 500 users and an administrative unit named AU1.
From the Azure Active Directory admin center, you plan to add the users to AU1 by using Bulk add members. You need to create and upload a file for the bulk add.
What should you include in the file?

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

Answer: E

NEW QUESTION 351
- (Exam Topic 3)
You plan to configure Azure Disk Encryption for VM4. Which key vault can you use to store the encryption key?

A. KeyVault1
B. KeyVault3
C. KeyVault2

Answer: A

Explanation:
The key vault needs to be in the same subscription and same region as the VM. VM4 is in West US. KeyVault1 is the only key vault in the same region as the VM.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault

NEW QUESTION 356
- (Exam Topic 3)
You need to meet the technical requirements for the finance department users. Which CAPolicy1 settings should you modify?

A. Cloud apps or actions
B. Conditions
C. Grant
D. Session

Answer: D

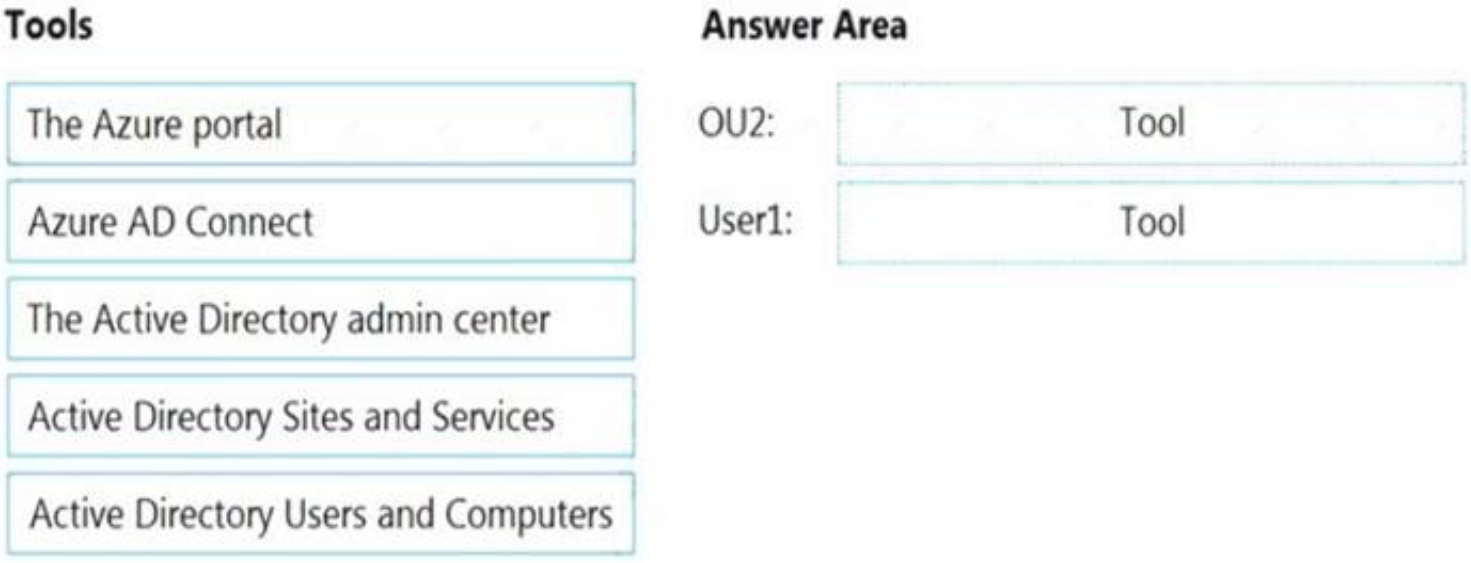
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-life

NEW QUESTION 359
- (Exam Topic 3)
You plan to implement JIT VM access. Which virtual machines will be supported?

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

Answer: A

NEW QUESTION 360
- (Exam Topic 3)
You need to perform the planned changes for OU2 and User1.
Which tools should you use? To answer, drag the appropriate tools to the correct resources. Each tool 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.



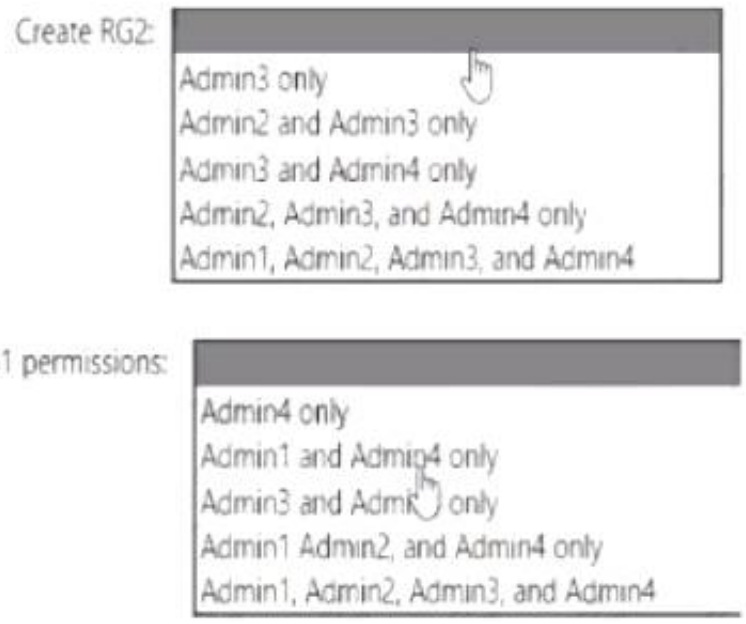
A. Mastered

B. Not Mastered

Answer: A

Explanation:
Table Description automatically generated

NEW QUESTION 363
- (Exam Topic 3)
You need to delegate the creation of RG2 and the management of permissions for RG1. Which users can perform each task? To answer select the appropriate options in the answer area. NOTE: Each correct selection is worth one point



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application, chat or text message Description automatically generated
Box 1: Admin3 only
The Contributor role has the necessary write permissions to create the resource group. Box 2: Admin4 only
You need Owner level access to be able to manage permissions. The Contributor role can do most things but cannot modify permissions on existing objects.

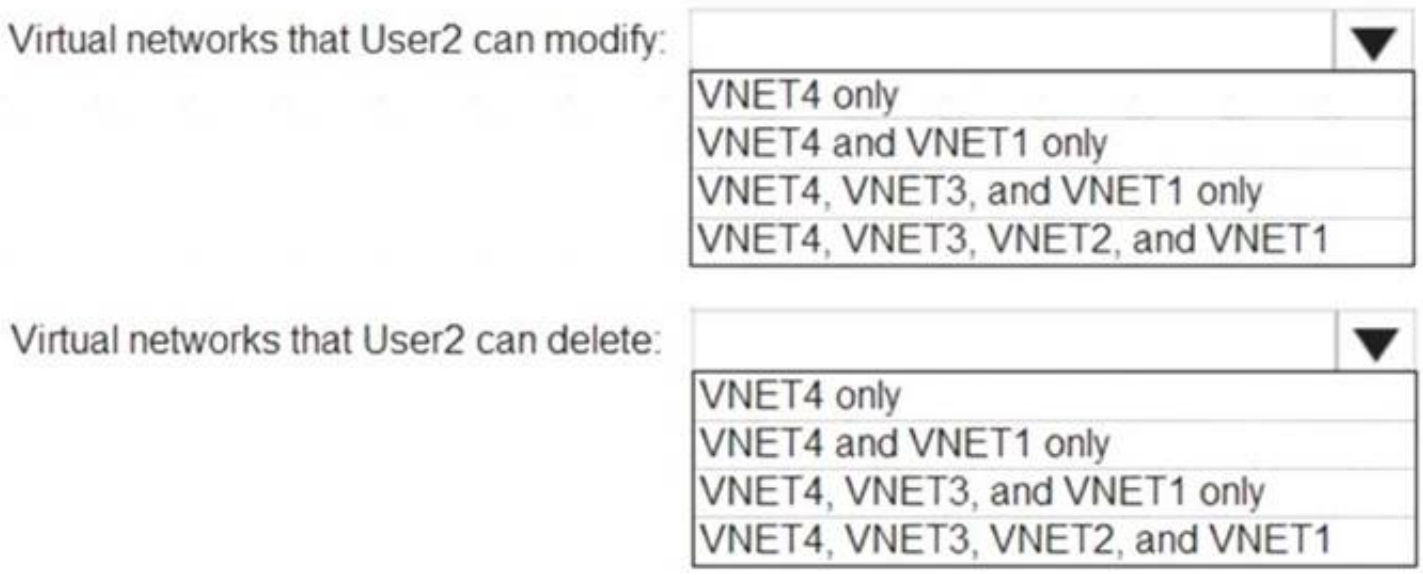
NEW QUESTION 364
- (Exam Topic 3)
You need to configure support for Azure Sentinel notebooks to meet the technical requirements. What is the minimum number of Azure container registries and Azure Machine Learning workspaces
required?

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Table Description automatically generated with medium confidence
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

NEW QUESTION 365
- (Exam Topic 2)
HOTSPOT
Which virtual networks in Sub1 can User2 modify and delete in their current state? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: VNET4 and VNET1 only
RG1 has only Delete lock, while there are no locks on RG4. RG2 and RG3 both have Read-only locks.
Box 2: VNET4 only
There are no locks on RG4, while the other resource groups have either Delete or Read-only locks.
Note: As an administrator, you may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. You can set the lock level to CanNotDelete or ReadOnly. In the portal, the locks are called Delete and Read-only respectively.
- CanNotDelete means authorized users can still read and modify a resource, but they can't delete the resource.
- ReadOnly means authorized users can read a resource, but they can't delete or update the resource.

Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.
Scenario:
User2 is a Security administrator.
Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6. User2 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

Name	Set on	Lock type
Lock1	RG1	Delete
Lock2	RG2	Read-only
Lock3	RG3	Delete
Lock4	RG3	Read-only

References:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources

NEW QUESTION 366
- (Exam Topic 2)
You need to meet the technical requirements for VNetwork1. What should you do first?

A. Create a new subnet on VNetwork1.
B. Remove the NSGs from Subnet11 and Subnet13.
C. Associate an NSG to Subnet12.
D. Configure DDoS protection for VNetwork1.

Answer: A

Explanation:
From scenario: Deploy Azure Firewall to VNetwork1 in Sub2.
Azure firewall needs a dedicated subnet named AzureFirewallSubnet. References:
https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal

NEW QUESTION 370
- (Exam Topic 1)

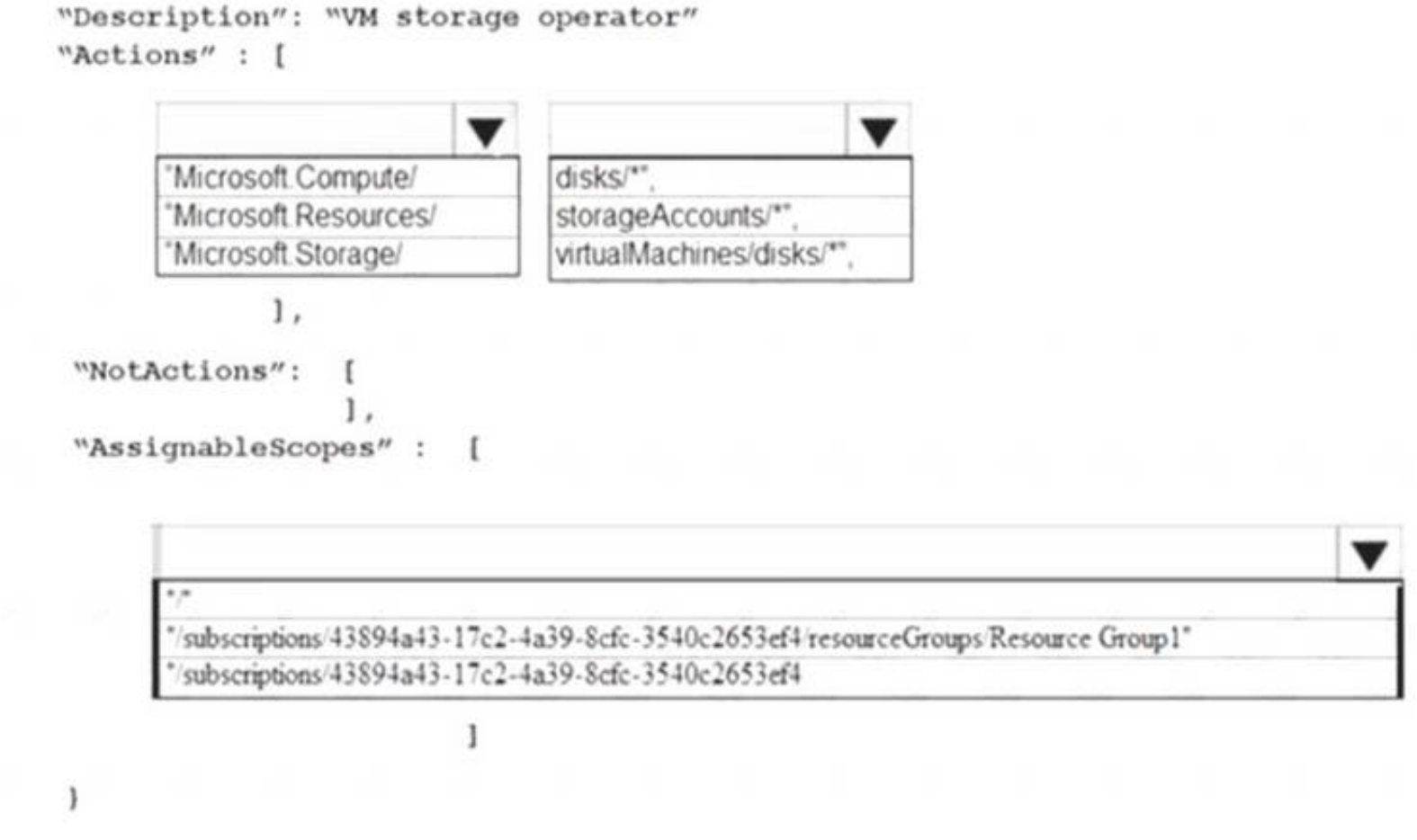
You need to ensure that you can meet the security operations requirements. What should you do first?

A. Turn on Auto Provisioning in Security Center.
B. Integrate Security Center and Microsoft Cloud App Security.
C. Upgrade the pricing tier of Security Center to Standard.
D. Modify the Security Center workspace configuration.

Answer: C

Explanation:
The Standard tier extends the capabilities of the Free tier to workloads running in private and other public clouds, providing unified security management and threat protection across your hybrid cloud workloads. The Standard tier also adds advanced threat detection capabilities, which uses built-in behavioral analytics and machine learning to identify attacks and zero-day exploits, access and application controls to reduce exposure to network attacks and malware, and more.
Scenario: Security Operations Requirements
Litware must be able to customize the operating system security configurations in Azure Security Center. References:
https://docs.microsoft.com/en-us/azure/security-center/security-center-pricing

NEW QUESTION 374
- (Exam Topic 1)
You need to create Role1 to meet the platform protection requirements.
How should you complete the role definition of Role1? 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:
1) Microsoft.Compute/
2) disks
3) /subscrption/{subscriptionId}/resourceGroups/{Resource Group Id}
A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.

NEW QUESTION 379
.....

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