Microsoft

Exam Questions az-500

Microsoft Azure Security Technologies

NEW QUESTION 1
- (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 2
- (Exam Topic 4)
You plan to deploy Azure container instances.
You have a containerized application that validates credit cards. The application is comprised of two containers: an application container and a validation container.
The application container is monitored by the validation container. The validation container performs security checks by making requests to the application container and waiting for responses after every transaction.
You need to ensure that the application container and the validation container are scheduled to be deployedtogether. The containers must communicate to each other only on ports that are not externally exposed.
What should you include in the deployment?

A. application security groups
B. network security groups (NSGs)
C. management groups
D. container groups

Answer: D

Explanation:
Azure Container Instances supports the deployment of multiple containers onto a single host using a container group. A container group is useful when building an application sidecar for logging, monitoring, or any other configuration where a service needs a second attached process.
Reference:
https://docs.microsoft.com/en-us/azure/container-instances/container-instances-container-groups

NEW QUESTION 3
- (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 4
- (Exam Topic 4)
You need to configure a weekly backup of an Azure SQL database named Homepage. The backup must be retained for eight weeks.
To complete this task, sign in to the Azure portal.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
You need to configure the backup policy for the Azure SQL database.

- In the Azure portal, type Azure SQL Database in the search box, select Azure SQL Database from the search results then select Homepage. Alternatively, browse to Azure SQL Database in the left navigation pane.
- Select the server hosting the Homepage database and click on Manage backups.
- Click on Configure policies.
- Ensure that the Weekly Backups option is ticked.
- Configure the How long would you like weekly backups to be retained option to 8 weeks.
- Click Apply to save the changes.

NEW QUESTION 5
- (Exam Topic 4)
Your company has an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
The company develops an application named App1. App1 is registered in Azure AD.
You need to ensure that App1 can access secrets in Azure Key Vault on behalf of the application users. What should you configure?

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

Answer: B

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

NEW QUESTION 6
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

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

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

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

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

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

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

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 7
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription named Sub1.
You have an Azure Storage account named Sa1 in a resource group named RG1.
Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.
You discover that unauthorized users accessed both the file service and the blob service. You need to revoke all access to Sa1.
Solution: You create a lock on Sa1. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately 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 8
- (Exam Topic 4)
Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD). Azure AD Connect is installed on a domain member server named Server1.
You need to ensure that a domain administrator for the adatum.com domain can modify the synchronization options. The solution must use the principle of least privilege.
Which Azure AD role should you assign to the domain administrator?

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

Answer: B

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

NEW QUESTION 9
- (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 10
- (Exam Topic 4)
You have an Azure resource group that contains 100 virtual machines.
You have an initiative named Initiative1 that contains multiple policy definitions. Initiative1 is assigned to the resource group.
You need to identify which resources do NOT match the policy definitions.
What should you do?

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

Answer: A

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

NEW QUESTION 10
- (Exam Topic 4)
You have an Azure subscription.
You plan to create a workflow automation in Azure Security Center that will automatically remediate a security vulnerability.
What should you create first?

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

Answer: E

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

NEW QUESTION 13
- (Exam Topic 4)
You onboard Azure Sentinel. You connect Azure Sentinel to Azure Security Center.
You need to automate the mitigation of incidents in Azure Sentinel. The solution must minimize administrative effort.
What should you create?

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

Answer: B

NEW QUESTION 16
- (Exam Topic 4)
You have an Azure subscription named Sub1. Sub1 contains a virtual network named VNet1 that contains one subnet named Subnet1.
You create a service endpoint for Subnet1.
Subnet1 contains an Azure virtual machine named VM1 that runs Ubuntu Server 18.04.
You need to deploy Docker containers to VM1. The containers must be able to access Azure Storage resources and Azure SQL databases by using the service endpoint.

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

Answer: C

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

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

NEW QUESTION 18
- (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 21
- (Exam Topic 4)
You are troubleshooting a security issue for an Azure Storage account.
You enable the diagnostic logs for the storage account. What should you use to retrieve the diagnostics logs?

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

Answer: D

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

NEW QUESTION 23
- (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 28
- (Exam Topic 4)
You are troubleshooting a security issue for an Azure Storage account. You enable the diagnostic logs for the storage account.
What should you use to retrieve the diagnostics logs?

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

Answer: A

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

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

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

NEW QUESTION 32
- (Exam Topic 4)
You have an Azure environment.
You need to identify any Azure configurations and workloads that are non-compliant with ISO 27001:2013 standards.
What should you use?

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

Answer: B

NEW QUESTION 34
- (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 35
- (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 regenerate the Azure storage account access keys. Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
Generating new storage account keys will invalidate all SAS's that were based on the previous keys.

NEW QUESTION 38
- (Exam Topic 4)
You have an Azure web app named webapp1.
You need to configure continuous deployment for webapp1 by using an Azure Repo. What should you create first?

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

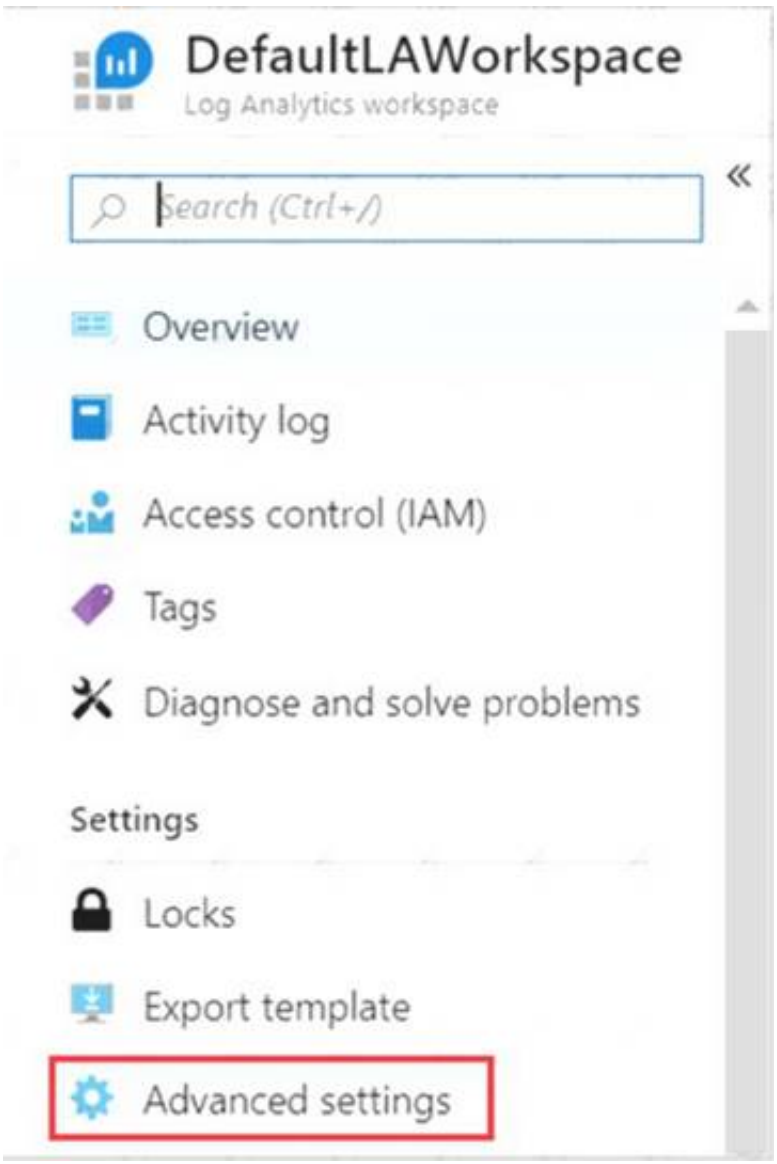
Answer: B

NEW QUESTION 41
- (Exam Topic 4)
You plan to connect several Windows servers to the WS11641655 Azure Log Analytics workspace.
You need to ensure that the events in the System event logs are collected automatically to the workspace after you connect the Windows servers.
To complete this task, sign in to the Azure portal and modify the Azure resources.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Azure Monitor can collect events from the Windows event logs or Linux Syslog and performance counters that you specify for longer term analysis and reporting, and take action when a particular condition is detected. Follow these steps to configure collection of events from the Windows system log and Linux Syslog, and several common performance counters to start with.
Data collection from Windows VM
* 1. In the Azure portal, locate the WS11641655 Azure Log Analytics workspace then select Advanced settings.



* 2. Select Data, and then select Windows Event Logs.
* 3. You add an event log by typing in the name of the log. Type System and then select the plus sign +.
* 4. In the table, check the severities Error and Warning. (for this question, select all severities to ensure that ALL logs are collected).
* 5. Select Save at the top of the page to save the configuration. Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-azurevm

NEW QUESTION 44
- (Exam Topic 4)
You have an Azure subscription that contains an Azure SQL database named DB1 in the East US Azure region. You create the storage accounts shown in the following table.

Name	Location	Performance	Premium account type
storage1	East US	Standard	*Not applicable*
storage2	East US	Premium	Block blobs
storage3	East US	Premium	File shares
storage4	East US 2	Standard	*Not applicable*

You plan to enable auditing for DB1.
Which storage accounts can you use as the auditing destination for DB1?

A. storage1 only
B. storage1 and storage4 only
C. Storage2 and storage3 only
D. storage1, storage2 and storage3 only

Answer: C

NEW QUESTION 46
- (Exam Topic 4)
You have an Azure subscription that uses Microsoft Sentinel.
You need to create a Microsoft Sentinel notebook that will use the Guided Investigation - Anomaly Lookup template.
What should you create first?

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

Answer: A

NEW QUESTION 49
- (Exam Topic 4)
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.

After syncing all on-premises identities to Azure AD, you are informed that users with a givenName attribute starting with LAB should not be allowed to sync to Azure AD.
Which of the following actions should you take?

A. You should make use of the Synchronization Rules Editor to create an attribute-based filtering rule.
B. You should configure a DNAT rule on the Firewall.
C. You should configure a network traffic filtering rule on the Firewall.
D. You should make use of Active Directory Users and Computers to create an attribute-based filtering rule.

Answer: A

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

NEW QUESTION 51
- (Exam Topic 4)
You have an Azure subscription that contains the storage accounts shown in the following, table.

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

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

Answer Area

Monitored storage5 services: [ ]
Protected storage accounts: [ ]

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Monitored storage5 services: File services and table services only
Protected storage accounts: storage1, storage4, and storage5 only

NEW QUESTION 56
- (Exam Topic 4)
You have an Azure web app named webapp1.
You need to configure continuous deployment for webapp1 by using an Azure Repo. What should you create first?

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

Answer: B

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

NEW QUESTION 58
- (Exam Topic 4)
From Azure Security Center, you enable Azure Container Registry vulnerability scanning of the images in Registry1.
You perform the following actions:
- Push a Windows image named Image1 to Registry1.
- Push a Linux image named Image2 to Registry1.
- Push a Windows image named Image3 to Registry1.
- Modify Image1 and push the new image as Image4 to Registry1.
- Modify Image2 and push the new image as Image5 to Registry1.

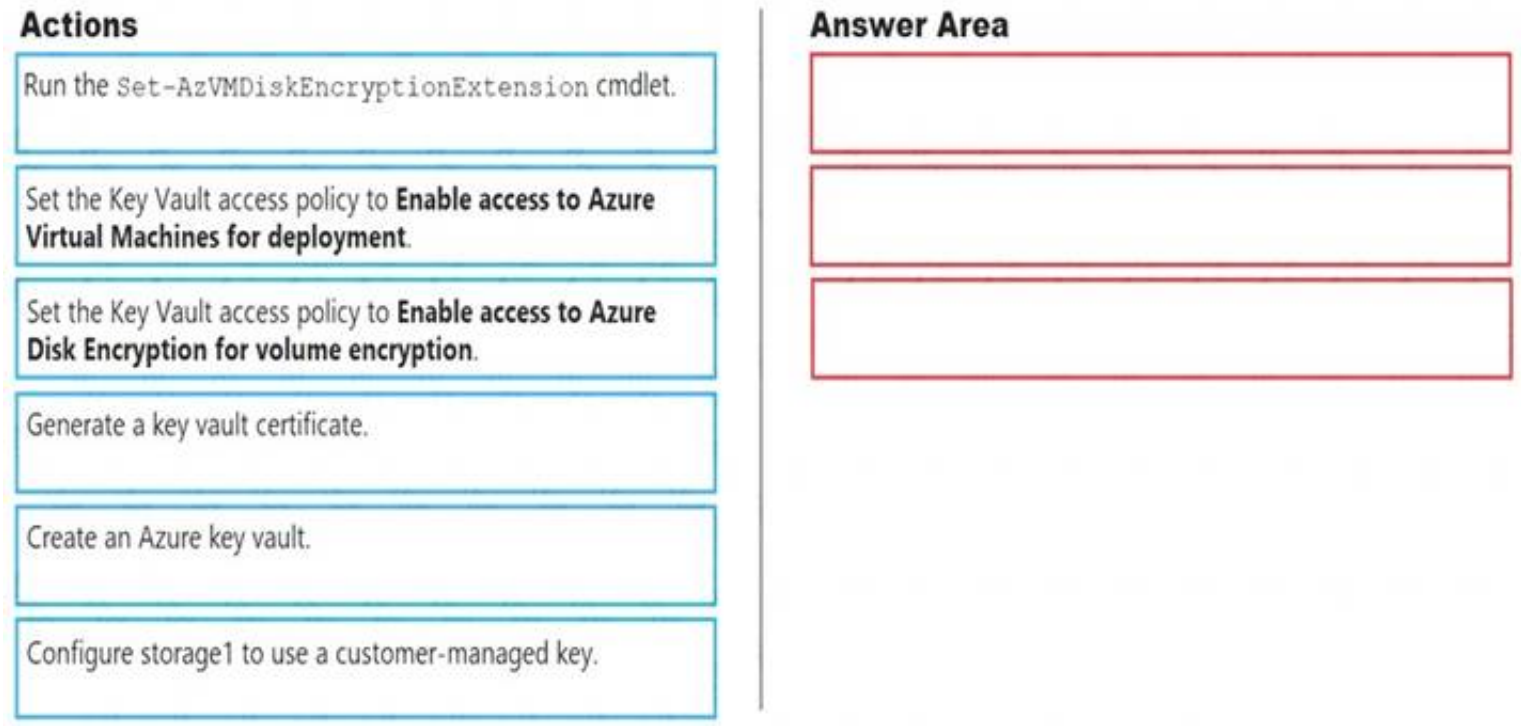
Which two images will be scanned for vulnerabilities? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Image4

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

Answer: BC

NEW QUESTION 62
- (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.

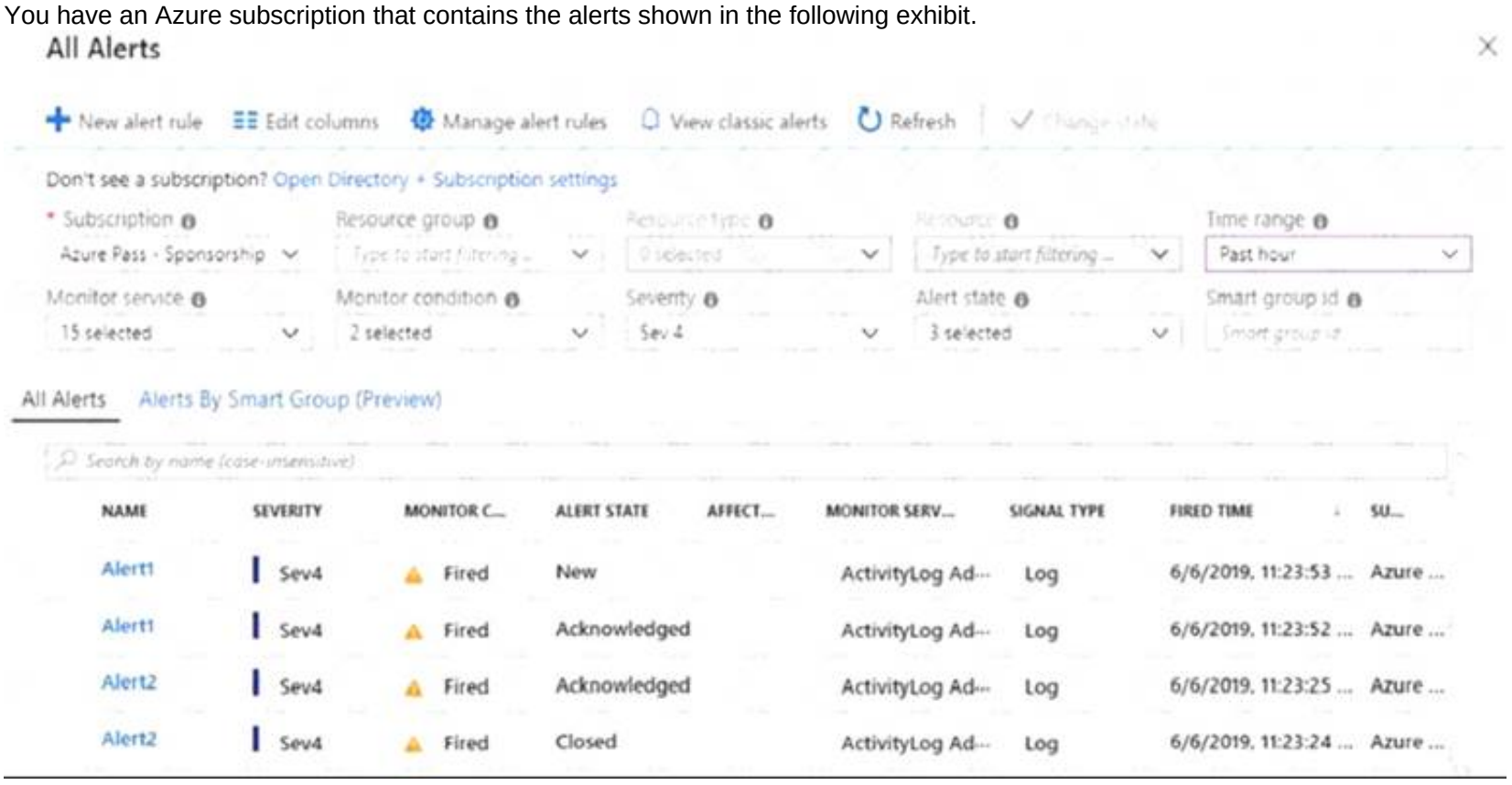


A. Mastered
B. Not Mastered

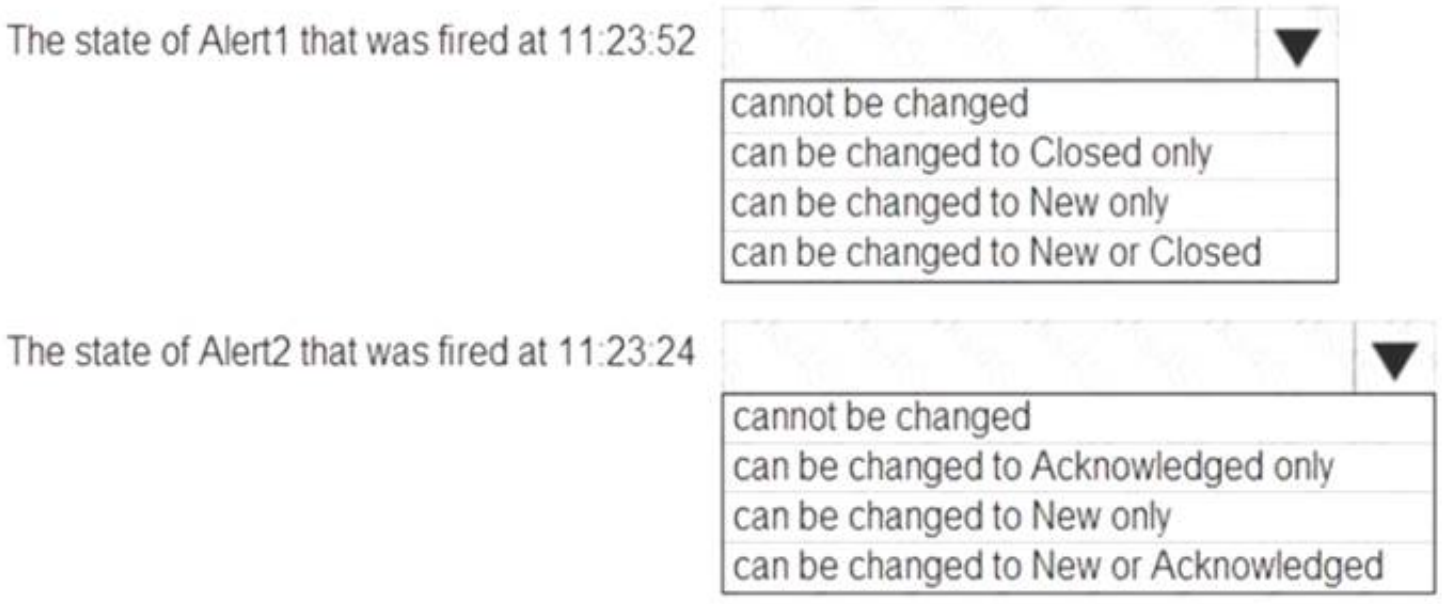
Answer: A

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 66
- (Exam Topic 4)
You have an Azure subscription that contains the alerts shown in the following exhibit.



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.



A. Mastered
B. Not Mastered

Answer: A

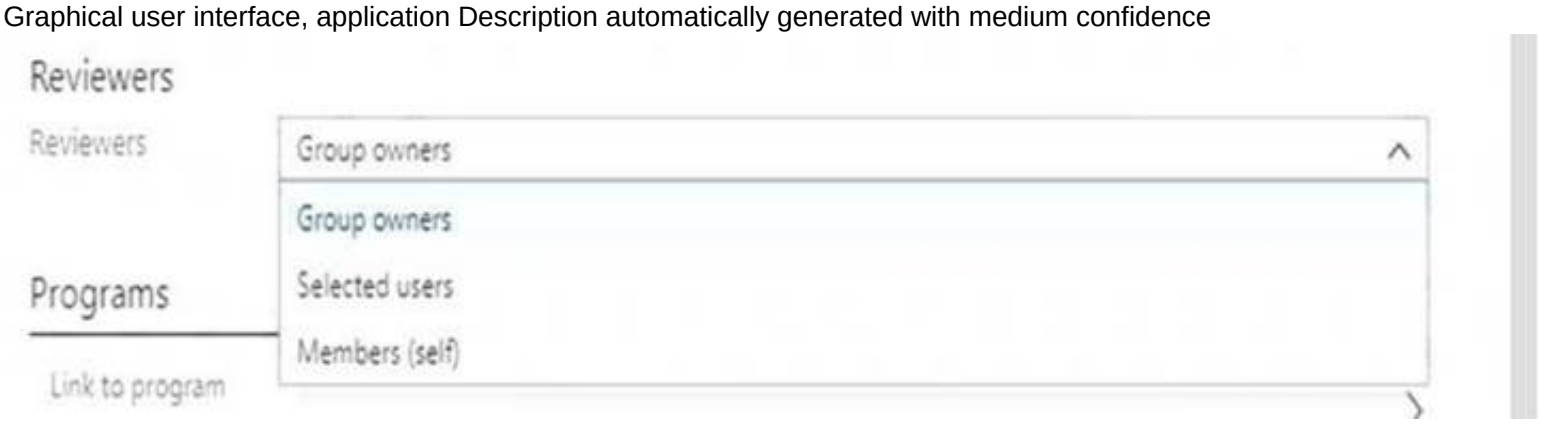
Explanation:
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-overview

NEW QUESTION 70
- (Exam Topic 4)
You have been tasked with configuring an access review, which you plan to assigned to a new collection of reviews. You also have to make sure that the reviews can be reviewed by resource owners.
You start by creating an access review program and an access review control. You now need to configure the Reviewers.
Which of the following should you set Reviewers to?

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

Answer: C

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



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

NEW QUESTION 75
- (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 76
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains a group named Group1 You need to ensure that the members of Group1 sign in by using passwordless authentication What should you do?

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

Answer: A

NEW QUESTION 80
- (Exam Topic 4)
You need to deploy an Azure firewall to a virtual network named VNET3.
To complete this task, sign in to the Azure portal and modify the Azure resources.
This task might take several minutes to complete. You can perform other tasks while the task completes.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
To add an Azure firewall to a VNET, the VNET must first be configured with a subnet named AzureFirewallSubnet (if it doesn't already exist).
Configure VNET3.

- In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET3. Alternatively, browse to Virtual Networks in the left navigation pane.
- In the Overview section, note the Location (region) and Resource Group of the virtual network. We'll need these when we add the firewall.
- Click on Subnets.
- Click on + Subnet to add a new subnet.
- Enter AzureFirewallSubnet in the Name box. The subnet must be named AzureFirewallSubnet.
- Enter an appropriate IP range for the subnet in the Address range box.
- Click the OK button to create the subnet. Add the Azure Firewall.
- In the settings of VNET3 click on Firewall.
- Click the Click here to add a new firewall link.
- The Resource group will default to the VNET3 resource group. Leave this default.
- Enter a name for the firewall in the Name box.
- In the Region box, select the same region as VNET3.
- In the Public IP address box, select an available public IP address if one exists, or click Add new to add a new public IP address.
- Click the Review + create button.
- Review the settings and click the Create button to create the firewall. Reference:

https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal

NEW QUESTION 84
- (Exam Topic 4)
Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
Your company has an Active Directory forest with a single domain, named weylandindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.
You have been tasked with integrating Active Directory and the Azure AD tenant. You intend to deploy Azure AD Connect.
Your strategy for the integration must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.
Solution: You recommend the use of password hash synchronization and seamless SSO. Does the solution meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 86
- (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 90
- (Exam Topic 4)
You need to ensure that when administrators deploy resources by using an Azure Resource Manager template, the deployment can access secrets in an Azure key vault named KV11597200.
To complete this task, sign in to the Azure portal.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
You need to configure an option in the Advanced Access Policy of the key vault.
- In the Azure portal, type Azure Key Vault in the search box, select Azure Key Vault from the search results then select the key vault named KV11597200. Alternatively, browse to Azure Key Vault in the left navigation pane.
- In the properties of the key vault, click on Advanced Access Policies.
- Tick the checkbox labelled Enable access to Azure Resource Manager for template deployment.
- Click Save to save the changes.

NEW QUESTION 92
- (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 93
- (Exam Topic 4)
You have the hierarchy of Azure resources shown in the following exhibit.

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

Name	Published at
Blueprint1	Tenant Root Group
Blueprint2	Subscription1

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

Blueprint1:

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

Blueprint2:

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

A. Mastered
B. Not Mastered

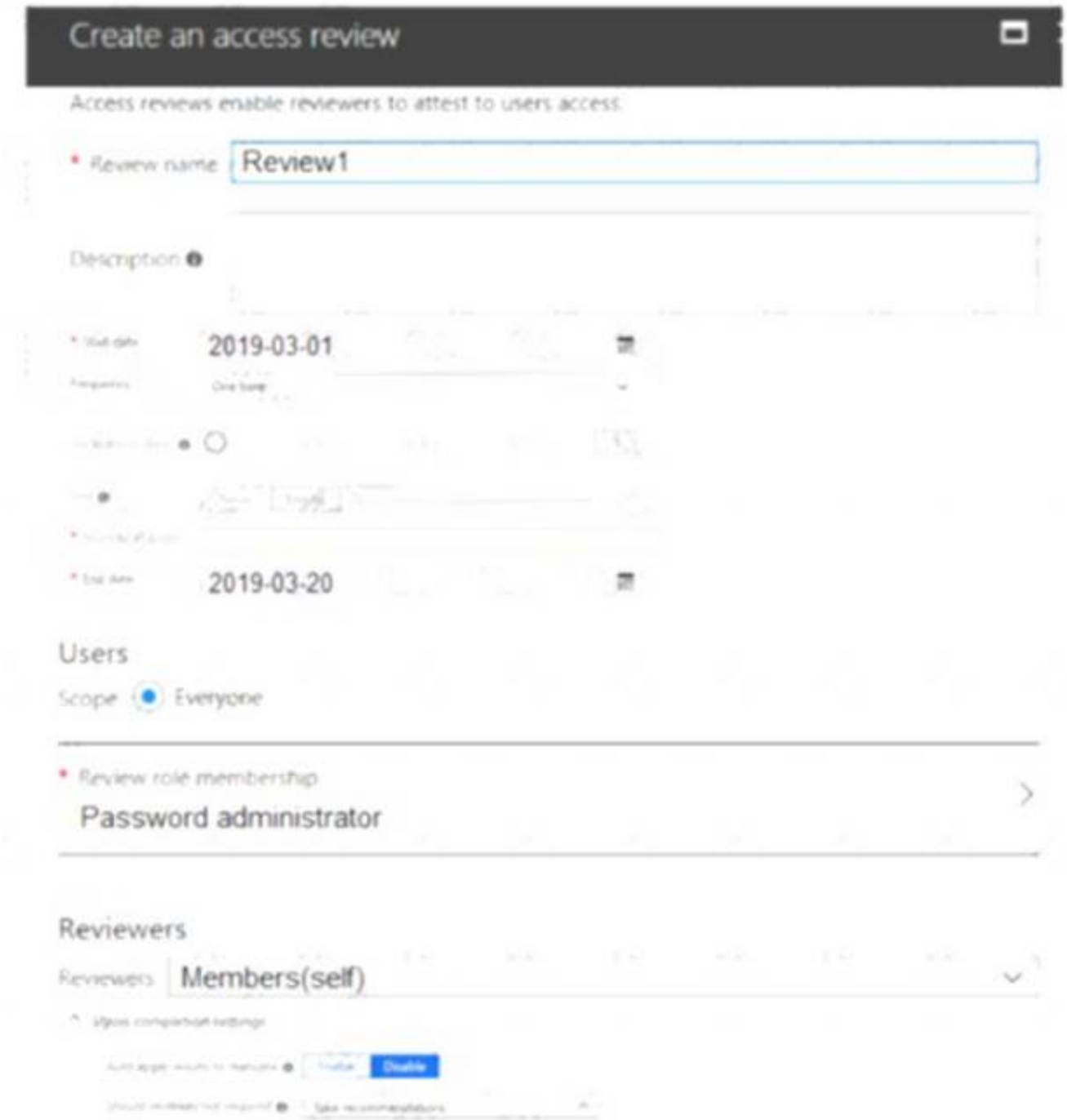
Answer: A

Explanation:
Blueprints can only be assigned to subscriptions.

NEW QUESTION 96
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role	Sign in frequency
User1	Password administrator	Sign in every work day
User2	Password administrator	Sign in bi-weekly
User3	Global administrator, Password administrator	Signs in every month

You configure an access review named Review1 as shown in the following exhibit.



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.

User3 can perform Review1 for
- User3 only
- User1 and User2 only
- User1, User2, and User3

If User2 fails to complete Review1 by March 20, 2019
- The Password administrator role will be revoked from User2
- User2 will retain the Password administrator role
- User3 will receive a confirmation request

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: User3 only
Use the Members (self) option to have the users review their own role assignments. Box 2: User3 will receive a confirmation request
Use the Should reviewer not respond list to specify what happens for users that are not reviewed by the reviewer within the review period. This setting does not impact users who have been reviewed by the reviewers manually. If the final reviewer's decision is Deny, then the user's access will be removed.
No change - Leave user's access unchanged Remove access - Remove user's access Approve access - Approve user's access
Take recommendations - Take the system's recommendation on denying or approving the user's continued access
References:
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-start-s

NEW QUESTION 97
- (Exam Topic 4)
You have an Azure subscription that contains a storage account named storage1 and several virtual machines. The storage account and virtual machines are in the same Azure region. The network configurations of the virtual machines are shown in the following table.

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

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

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

You configure the following Firewall and virtual networks settings for storage1:

- Allow access from: Selected networks
- Virtual networks: VNET3\Subnet3
- Firewall – Address range: 52.233.129.0/24

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

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

A. Mastered
B. Not Mastered

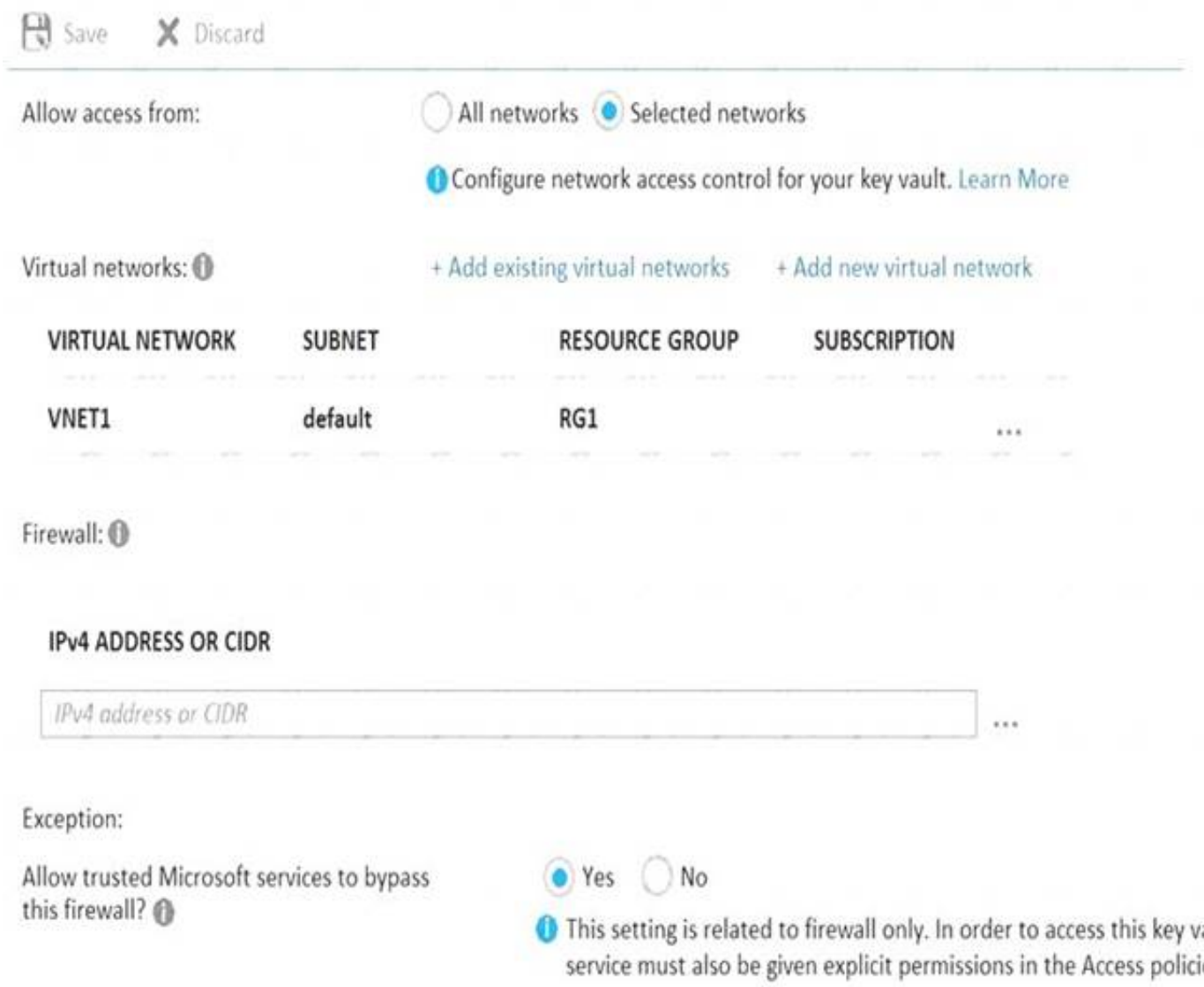
Answer: A

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

NEW QUESTION 98
- (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 103
- (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 108
- (Exam Topic 4)
You network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant. The tenant contains the users shown in the following table.

Name	Source
User1	Azure AD
User2	Azure AD
User3	On-premises Active Directory

The tenant contains the groups shown in the following table.

Name	Members
Group1	User1, User2, User3
Group2	User2

You configure a multi-factor authentication (MFA) registration policy that and the following settings:
- Assignments:
- Include: Group1
- Exclude Group2

Controls: Require Azure MFA registration Enforce Policy: On
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Azure AD authentication.	○	○
User2 must configure MFA during the user's next Azure AD authentication.	○	○
User3 will be prompted to configure MFA registration during the user's next Azure AD authentication.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Azure AD authentication.	○	○
User2 must configure MFA during the user's next Azure AD authentication.	○	○
User3 will be prompted to configure MFA registration during the user's next Azure AD authentication.	○	○

NEW QUESTION 110
- (Exam Topic 4)
You have a hybrid configuration of Azure Active Directory (Azure AD). You have an Azure SQL Database instance that is configured to support Azure AD authentication.
Database developers must connect to the database instance and authenticate by using their on-premises Active Directory account.
You need to ensure that developers can connect to the instance by using Microsoft SQL Server Management Studio. The solution must minimize authentication prompts.
Which authentication method should you recommend?

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

Answer: D

Explanation:

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

NEW QUESTION 112
- (Exam Topic 4)
You plan to use Azure Resource Manager templates to perform multiple deployments of identically configured Azure virtual machines. The password for the administrator account of each deployment is stored as a secret in different Azure key vaults.
You need to identify a method to dynamically construct a resource ID that will designate the key vault containing the appropriate secret during each deployment.
The name of the key vault and the name of the secret will be provided as inline parameters.
What should you use to construct the resource ID?

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

Answer: C

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

NEW QUESTION 116
- (Exam Topic 4)
You have an Azure subscription that contains a resource group named RG1 and a security group serverless RG1 contains 10 virtual machine, a virtual network VNET1, and a network security group (NSG) named NSG1. ServerAdmins can access the virtual machines by using RDP.
You need to ensure that NSG1 only RDP connections to the virtual for a maximum of 60 minutes when a member of ServerAdmins requests access.
What should you configure?

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

Answer: B

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

NEW QUESTION 118
- (Exam Topic 4)
You have an Azure subscription named Sub1.
In Azure Security Center, you have a security playbook named Play1. Play1 is configured to send an email message to a user named User1.
You need to modify Play1 to send email messages to a distribution group named Alerts. What should you use to modify Play1?

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

Answer: D

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

NEW QUESTION 119
- (Exam Topic 4)
You have an Azure subscription name Sub1 that contains an Azure Policy definition named Policy1. Policy1 has the following settings:
- Definition location: Tenant Root Group
- Category: Monitoring

You need to ensure that resources that are noncompliant with Policy1 are listed in the Azure Security Center dashboard.
What should you do first?

A. Change the Category of Policy1 to Security Center.
B. Add Policy1 to a custom initiative.
C. Change the Definition location of Policy1 to Sub1.
D. Assign Policy1 to Sub1.

Answer: D

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

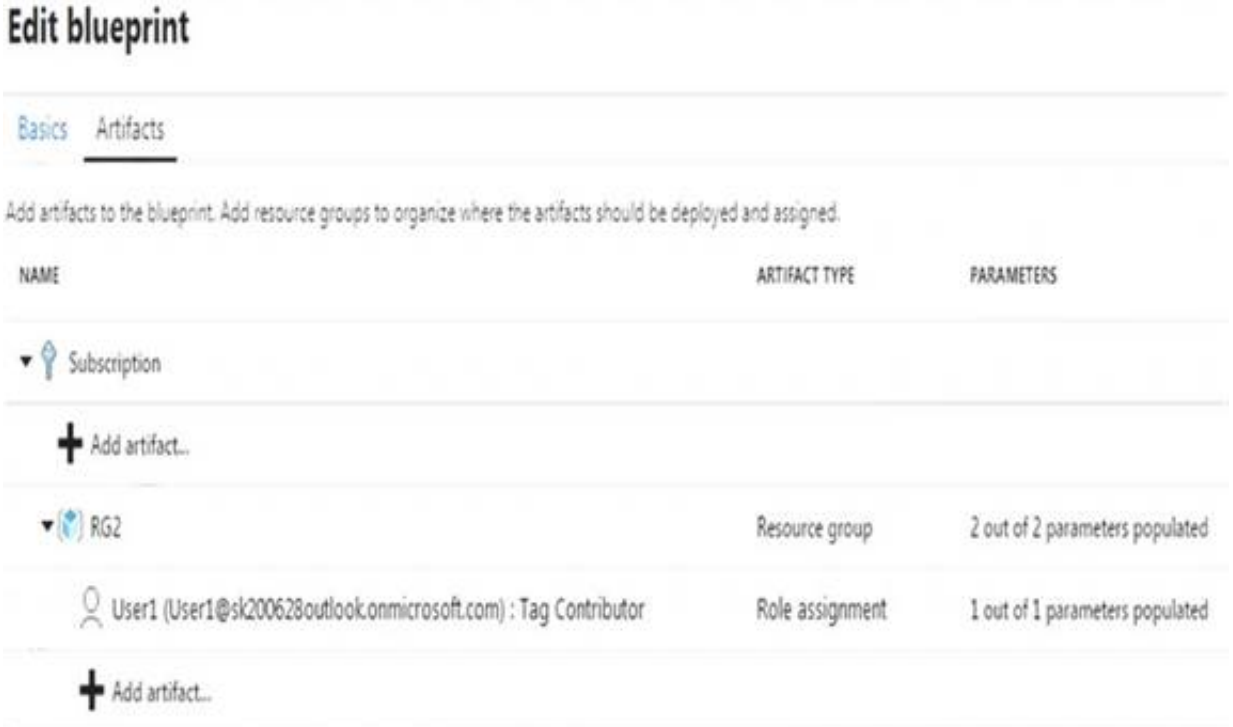
NEW QUESTION 121
- (Exam Topic 4)
You have an Azure Sentinel deployment.
You need to create a scheduled query rule named Rule1. What should you use to define the query rule logic for Rule1?

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

Answer: D

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

NEW QUESTION 125
- (Exam Topic 4)
You have an Azure subscription named Subscription1 that contains a resource group named RG1 and a user named User1. User1 is assigned the Owner role for RG1.
You create an Azure Blueprints definition named Blueprint1 that includes a resource group named RG2 as shown in the following exhibit.



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

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

NOTE: Each correct selection is worth one point.

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 126
- (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.	○	○

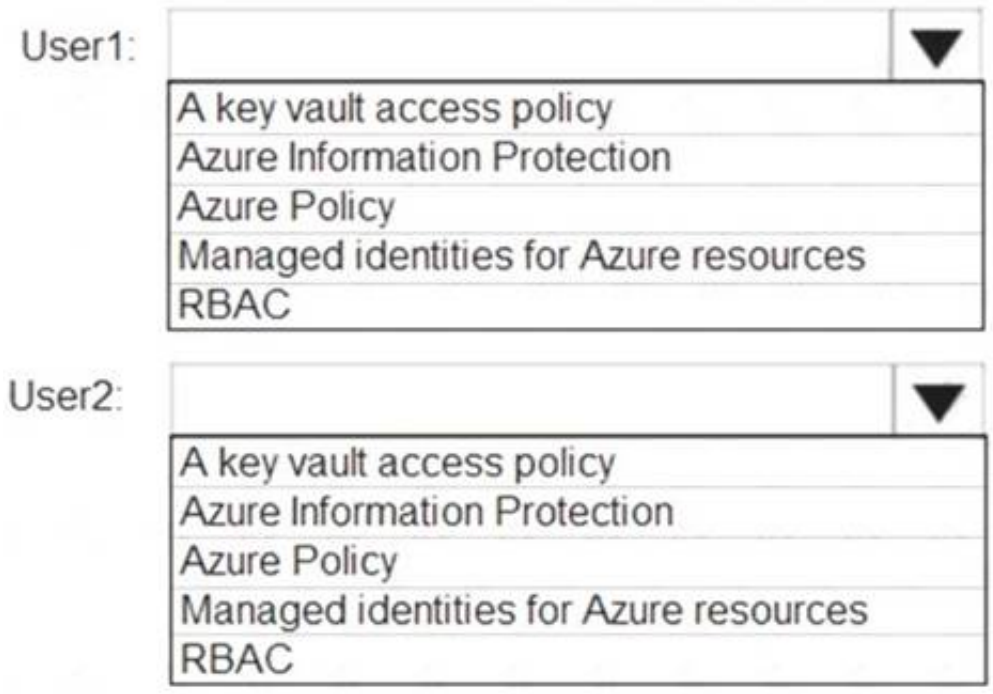
A. Mastered
B. Not Mastered

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 129
- (Exam Topic 4)
You have an Azure key vault.
You need to delegate administrative access to the key vault to meet the following requirements:
- Provide a user named User1 with the ability to set advanced access policies for the key vault.
- Provide a user named User2 with the ability to add and delete certificates in the key vault.
- Use the principle of least privilege.

What should you use to assign access to each user? 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:
User1: RBAC
RBAC is used as the Key Vault access control mechanism for the management plane. It would allow a user with the proper identity to:

- set Key Vault access policies
- create, read, update, and delete key vaults
- set Key Vault tags

Note: Role-based access control (RBAC) is a system that provides fine-grained access management of Azure resources. Using RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs.
User2: A key vault access policy
A key vault access policy is the access control mechanism to get access to the key vault data plane. Key Vault access policies grant permissions separately to keys, secrets, and certificates.
References:
https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

NEW QUESTION 130
- (Exam Topic 4)
You have an Azure subscription that contains an Azure key vault. The role assignments for the key vault are shown in the following exhibit.

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

Answer Area

[Answer choice] can create keys in the key vault.

[Answer choice] can create secrets in the key vault.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

[Answer choice] can create keys in the key vault. Only User1 and User4

[Answer choice] can create secrets in the key vault. Only User1 and User3

NEW QUESTION 132
- (Exam Topic 4)
You have an Azure subscription that contains virtual machines. You enable just in time (JIT) VM access to all the virtual machines.
You need to connect to a virtual machine by using Remote Desktop. What should you do first?

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

Answer: C

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

NEW QUESTION 137
- (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.

Tools

- The Azure portal
- Azure AD Connect
- The Active Directory admin center
- Active Directory Sites and Services
- Active Directory Users and Computers

Answer Area

OU2: Tool

User1: Tool

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Table Description automatically generated

NEW QUESTION 139
- (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

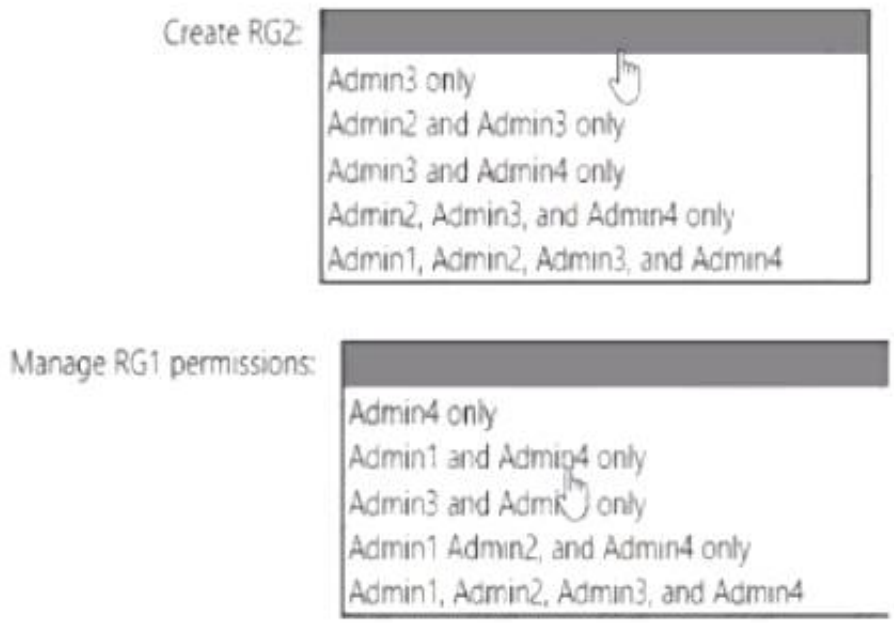
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-life

NEW QUESTION 143
- (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 144
- (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 147
- (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 151
- (Exam Topic 2)

You need to ensure that User2 can implement PIM. What should you do first?

A. Assign User2 the Global administrator role.
B. Configure authentication methods for contoso.com.
C. Configure the identity secure score for contoso.com.
D. Enable multi-factor authentication (MFA) for User2.

Answer: D

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
References:
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-started

NEW QUESTION 156
- (Exam Topic 2)
You are evaluating the security of the network communication between the virtual machines in Sub2. For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
No, Yes,
Yes

NEW QUESTION 158
- (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.

Virtual networks that User2 can modify:
- VNET4 only
- VNET4 and VNET1 only
- VNET4, VNET3, and VNET1 only
- VNET4, VNET3, VNET2, and VNET1

Virtual networks that User2 can delete:
- VNET4 only
- VNET4 and VNET1 only
- VNET4, VNET3, and VNET1 only
- VNET4, VNET3, VNET2, and VNET1

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 161
- (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

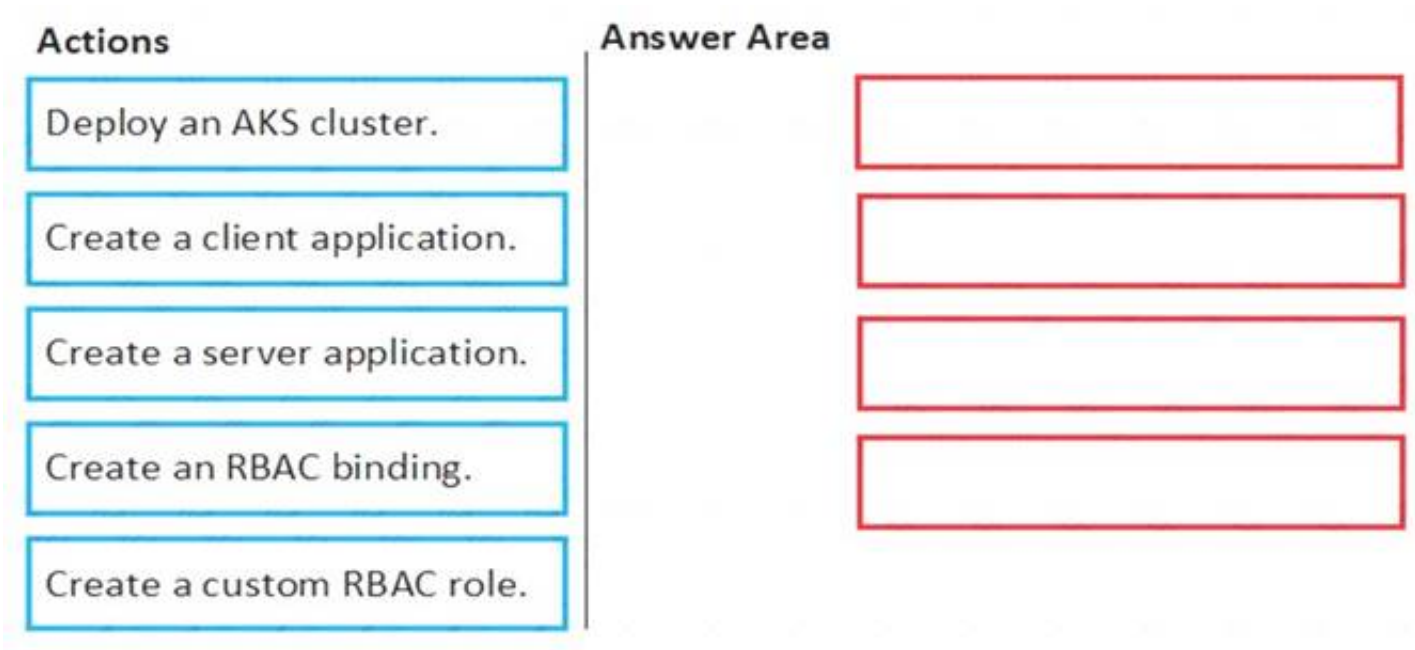
NEW QUESTION 163
- (Exam Topic 1)
You need to ensure that users can access VM0. The solution must meet the platform protection requirements.
What should you do?

A. Move VM0 to Subnet1.
B. On Firewall, configure a network traffic filtering rule.
C. Assign RT1 to AzureFirewallSubnet.
D. On Firewall, configure a DNAT rule.

Answer: D

Explanation:
https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-dnat

NEW QUESTION 166
- (Exam Topic 1)
You need to deploy AKS1 to meet the platform protection requirements.
Which four 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.

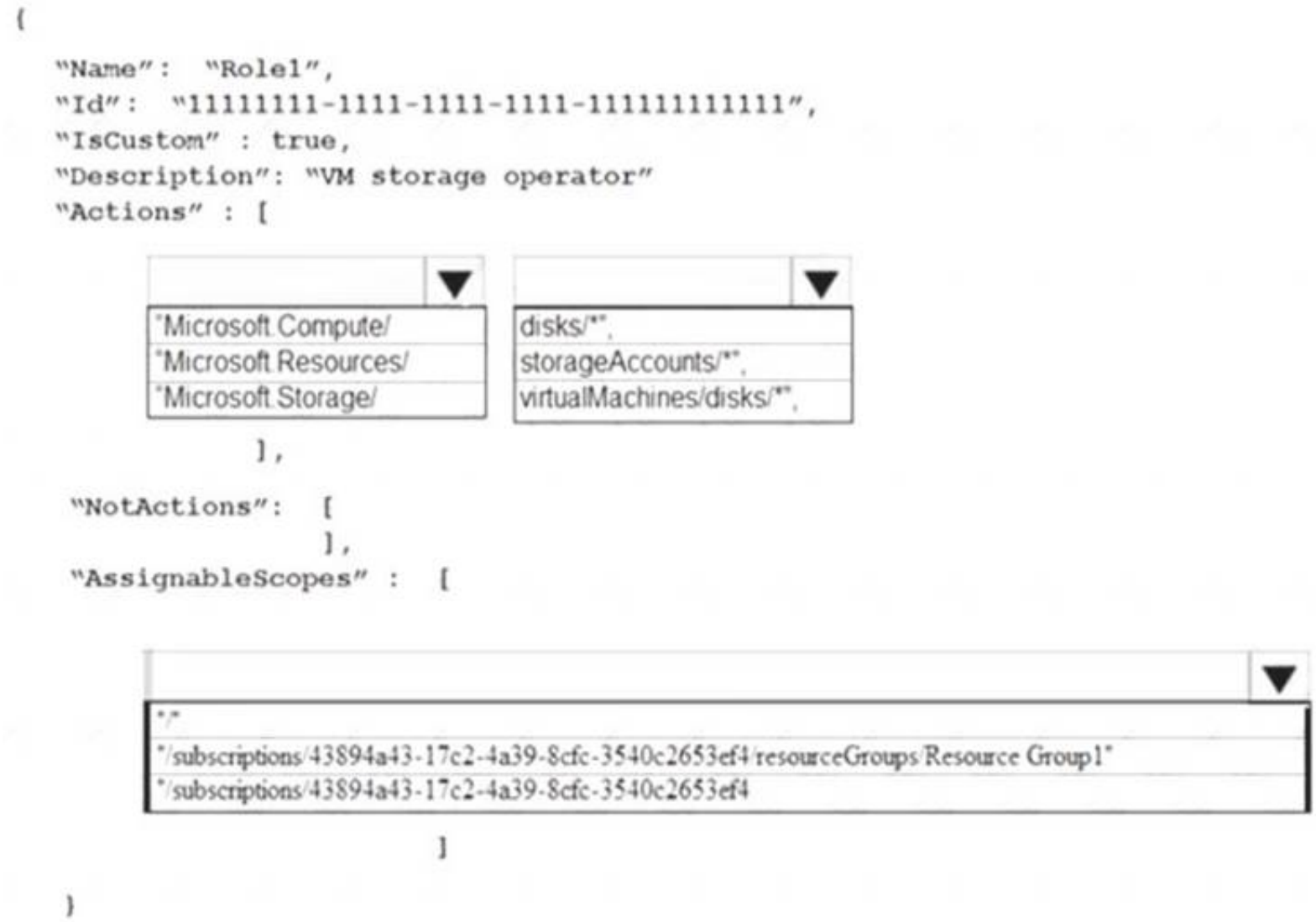


A. Mastered
B. Not Mastered

Answer: A

Explanation:
Scenario: Azure AD users must be to authenticate to AKS1 by using their Azure AD credentials. Litewire plans to deploy AKS1, which is a managed AKS (Azure Kubernetes Services) cluster. Step 1: Create a server application
To provide Azure AD authentication for an AKS cluster, two Azure AD applications are created. The first
application is a server component that provides user authentication. Step 2: Create a client application
The second application is a client component that's used when you're prompted by the CLI for authentication. This client application uses the server application for the actual authentication of the credentials provided by the client.
Step 3: Deploy an AKS cluster.
Use the az group create command to create a resource group for the AKS cluster. Use the az aks create command to deploy the AKS cluster.
Step 4: Create an RBAC binding.
Before you use an Azure Active Directory account with an AKS cluster, you must create role-binding or cluster role-binding. Roles define the permissions to grant, and bindings apply them to desired users. These assignments can be applied to a given namespace, or across the entire cluster.
Reference:
https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration

NEW QUESTION 170
- (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 171
- (Exam Topic 4)
You need to configure a Microsoft SQL server named Web11597200 only to accept connections from the Subnet0 subnet on the VNET01 virtual network.
To complete this task, sign in to the Azure portal.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
You need to allow access to Azure services and configure a virtual network rule for the SQL Server.

- In the Azure portal, type SQL Server in the search box, select SQL Server from the search results then select the server named web11597200. Alternatively, browse to SQL Server in the left navigation pane.
- In the properties of the SQL Server, click Firewalls and virtual networks.
- In the Virtual networks section, click on Add existing. This will open the Create/Update virtual network rule window.
- Give the rule a name such as Allow_VNET01-Subnet0 (it doesn't matter what name you enter for the exam).
- In the Virtual network box, select VNET01.
- In the Subnet name box, select Subnet0.
- Click the OK button to save the rule.
- Back in the Firewall / Virtual Networks window, set the Allow access to Azure services option to On.

NEW QUESTION 173
- (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 174
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Security Center for the centralized policy management of three Azure subscriptions. You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create a policy initiative and assignments that are scoped to resource groups. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Instead use a management group.
Management groups in Microsoft Azure solve the problem of needing to impose governance policy on more than one Azure subscription simultaneously.
Reference:
https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-managementgroups

NEW QUESTION 175
- (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 176

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

What should you do?

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

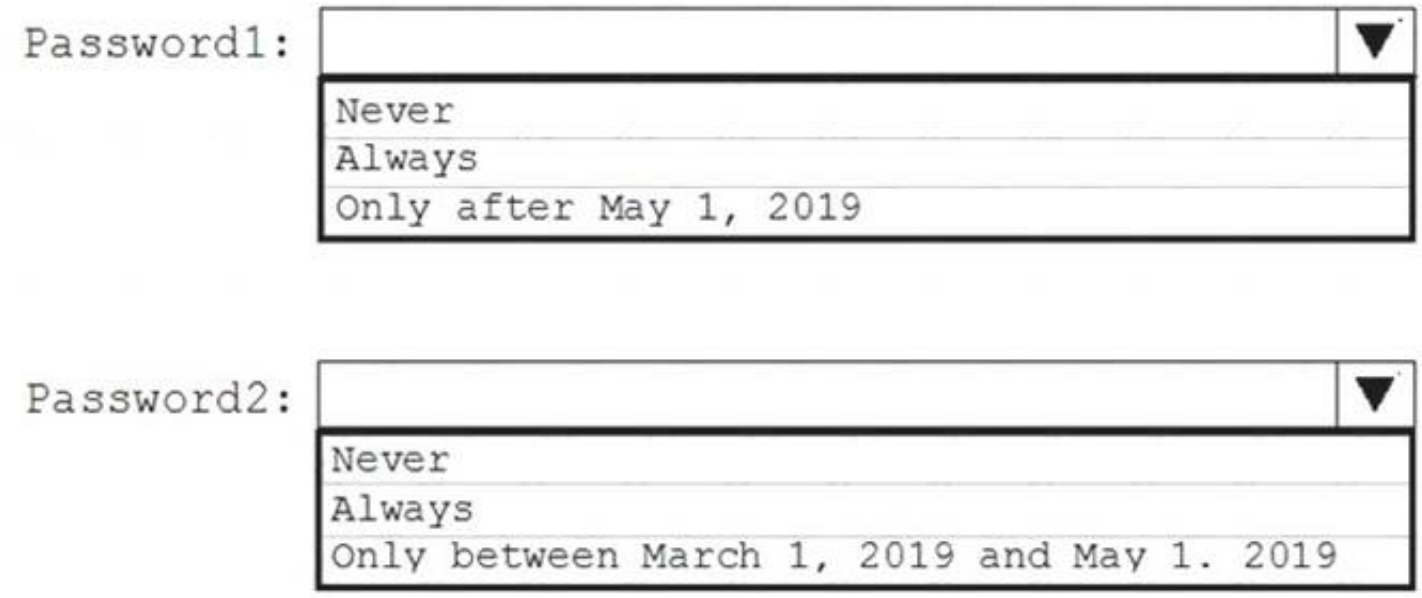
Answer: B

NEW QUESTION 178
- (Exam Topic 4)
You have an Azure subscription that contains an Azure key vault named Vault1. On January 1, 2019, Vault1 stores the following secrets.

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

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

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



A. Mastered
B. Not Mastered

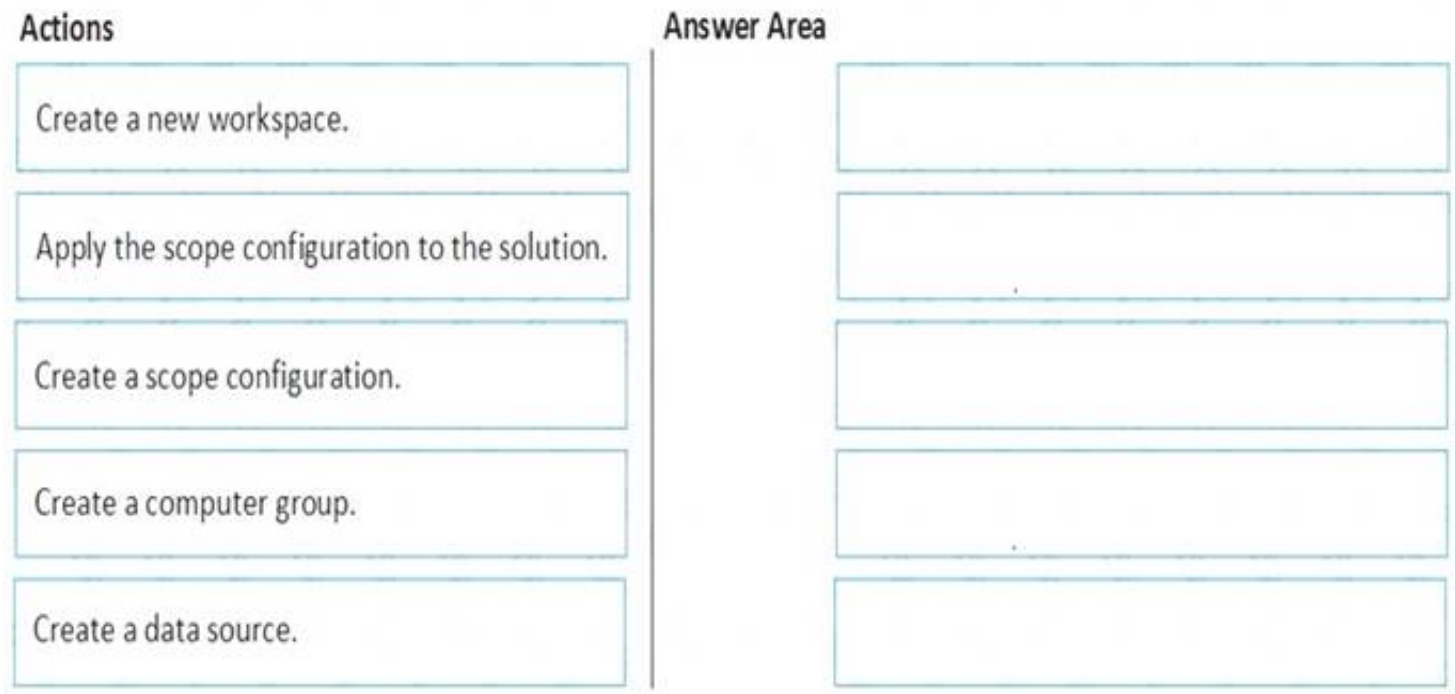
Answer: A

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

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

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

NEW QUESTION 180
- (Exam Topic 4)
You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1. You have 500 Azure virtual machines that run Windows Server 2016 and are enrolled in LAW1.
You plan to add the System Update Assessment solution to LAW1.
You need to ensure that System Update Assessment-related logs are uploaded to LAW1 from 100 of the virtual machines only.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/insights/solution-targeting

NEW QUESTION 182
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

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

Azure AD Privileged Identity Management (PIM) is enabled for the tenant. In PIM, the Password Administrator role has the following settings:
- Maximum activation duration (hours): 2
- Send email notifying admins of activation: Disable
- Require incident/request ticket number during activation: Disable
- Require Azure Multi-Factor Authentication for activation: Enable
- Require approval to activate this role: Enable
- Selected approver: Group1

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

Name	Assignment type
User1	Active
User2	Eligible
user3	Eligible

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

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

A. Mastered
B. Not Mastered

Answer: A

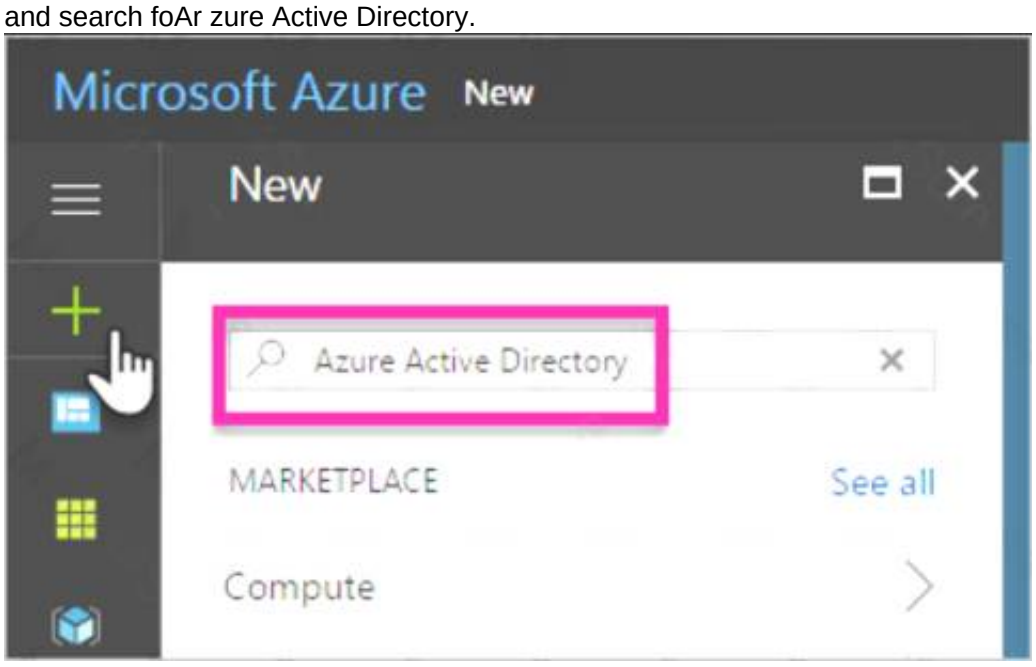
Explanation:
YES (Already active)
YES (The user will be prompted for MFA regardless the MFA Status of the user) NO (Even the user is included in the group, a user can't approve itself)
https://docs.microsoft.com/es-es/azure/active-directory/privileged-identity-management/pim-deployment-plan (Require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

NEW QUESTION 187
- (Exam Topic 4)
You need to create a new Azure Active Directory (Azure AD) directory named 10317806.onmicrosoft.com. The new directory must contain a user named user10317806 who is configured to sign in by using Azure Multi-Factor Authentication (MFA).

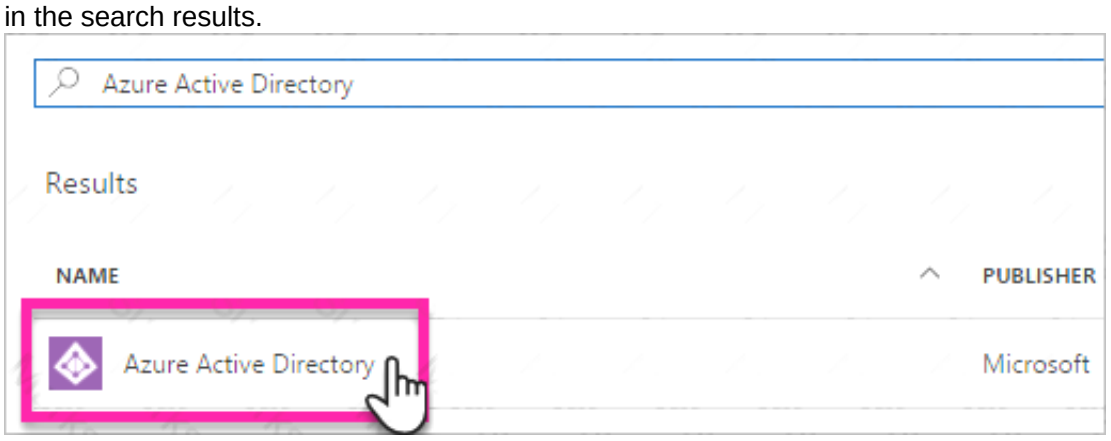
A. Mastered
B. Not Mastered

Answer: A

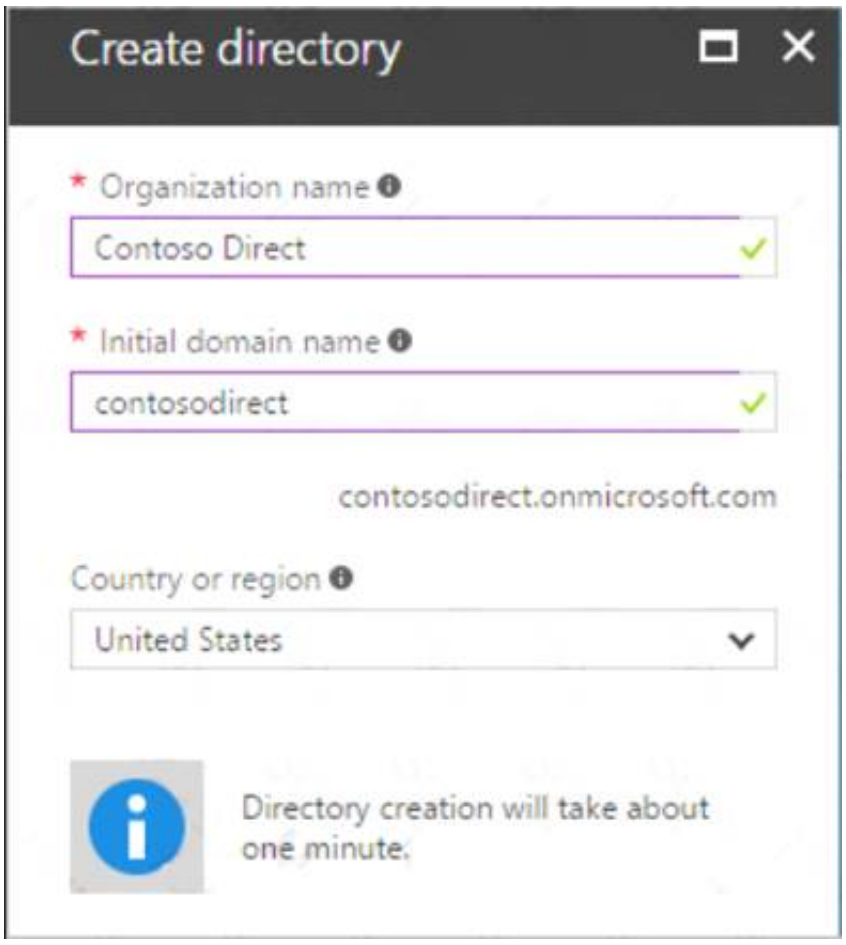
Explanation:
To create a new Azure AD tenant:
* 1. Browse to the Azure portal and sign in with an account that has an Azure subscription.
* 2. Select the plus icon (+)
and search foAr zure Active Directory.



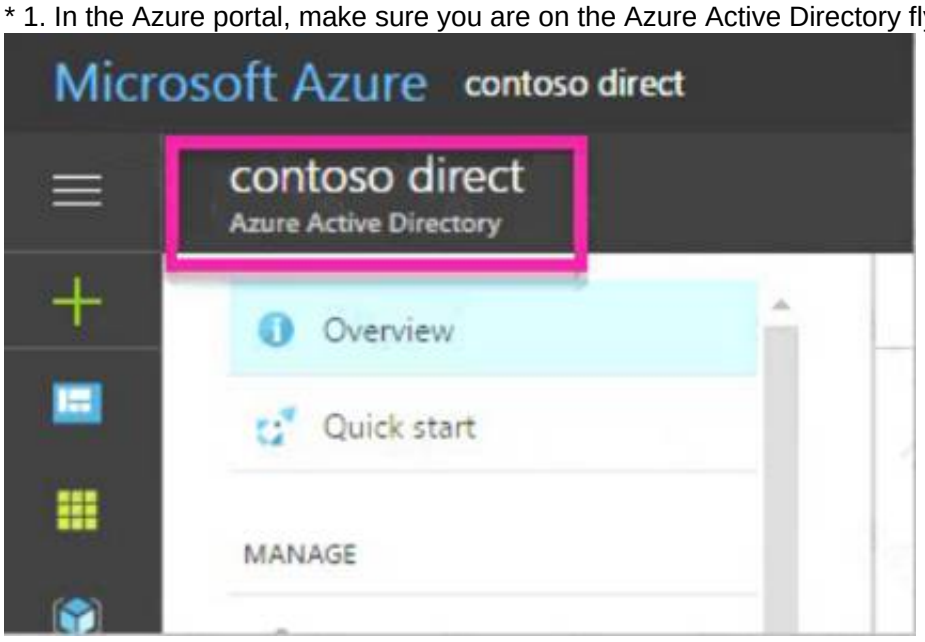
* 3. Select Azure Active Directory
in the search results.



* 4. Select Create.
* 5. Provide an Organization name
This will create the directory named 10317806.onmicrosoft.com.
(10317806) and anInitial domain name (10317806). Then select Create.

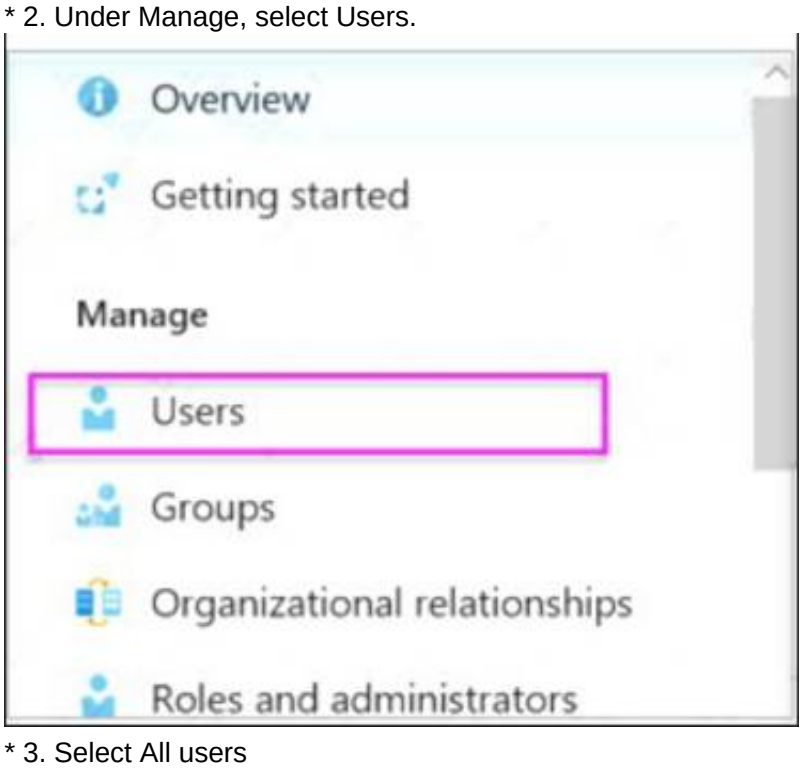


* 6. After directory creation is complete, select the information box to manage your new directory. To create the user:
* 1. In the Azure portal, make sure you are on the Azure Active Directory fly out.



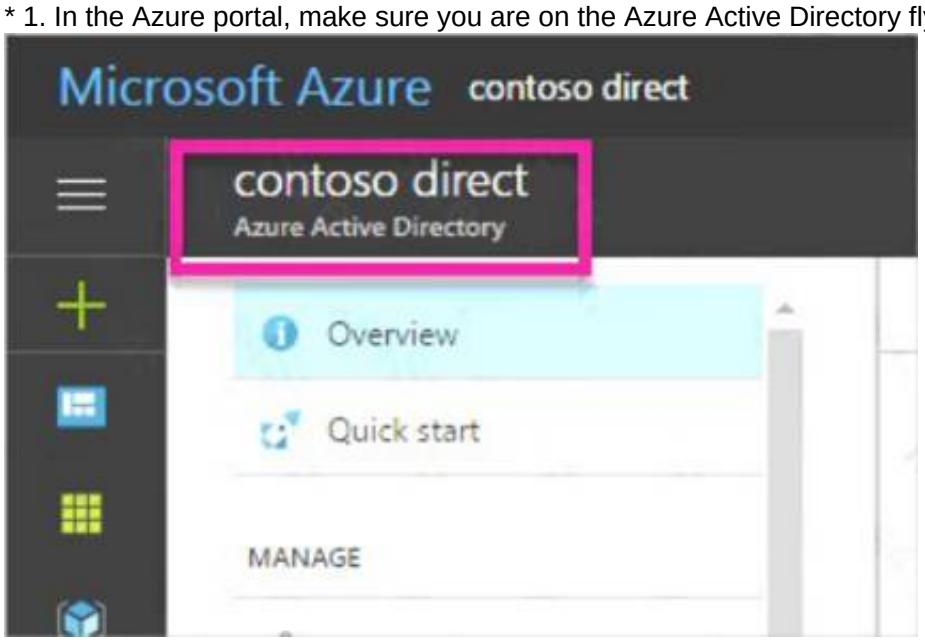
If not, select the Azure Active Directory icon from the left services navigation.

* 2. Under Manage, select Users.



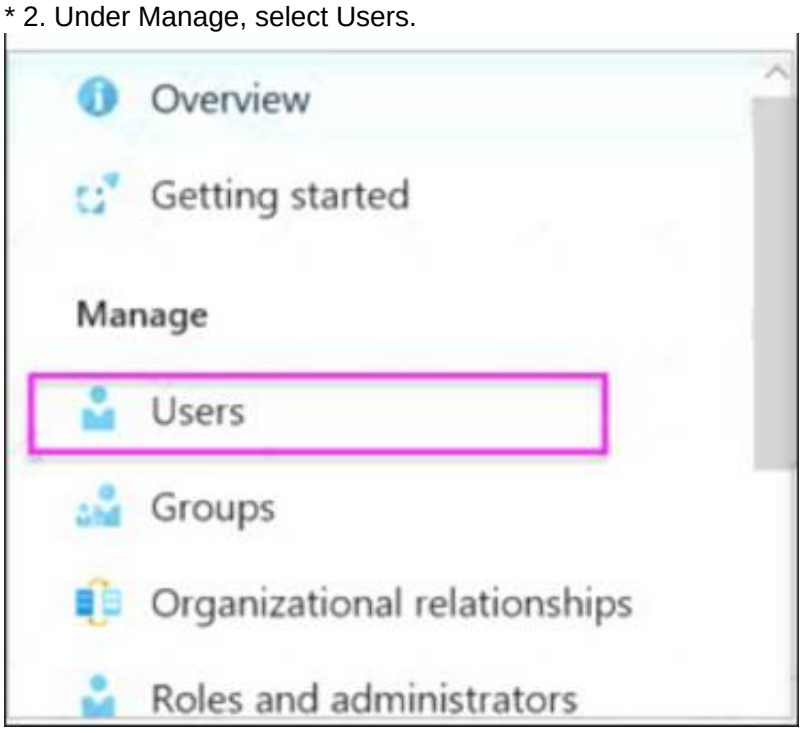
* 3. Select All users

and then selec+t New user.
* 4. Provide a Name
andUser name
(user10317806) for the user. When you're done, selecCt reate.
To enable MFA:
* 1. In the Azure portal, make sure you are on the Azure Active Directory fly out.



If not, select the Azure Active Directory icon from the left services navigation.

* 2. Under Manage, select Users.



* 3. Click on the Multi-Factor Authentication link.
* 4. Tick the checkbox next to the user's name and click the Enable link.
Reference:
https://docs.microsoft.com/en-us/power-bi/developer/create-an-azure-active-directory-tenant

NEW QUESTION 190
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a hybrid configuration of Azure Active Directory (Azure AD). You have an Azure HDInsight cluster on a virtual network.
You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials. You need to configure the environment to support the planned authentication.
Solution: You deploy Azure Active Directory Domain Services (Azure AD DS) to the Azure subscription.
Does this meet the goal?

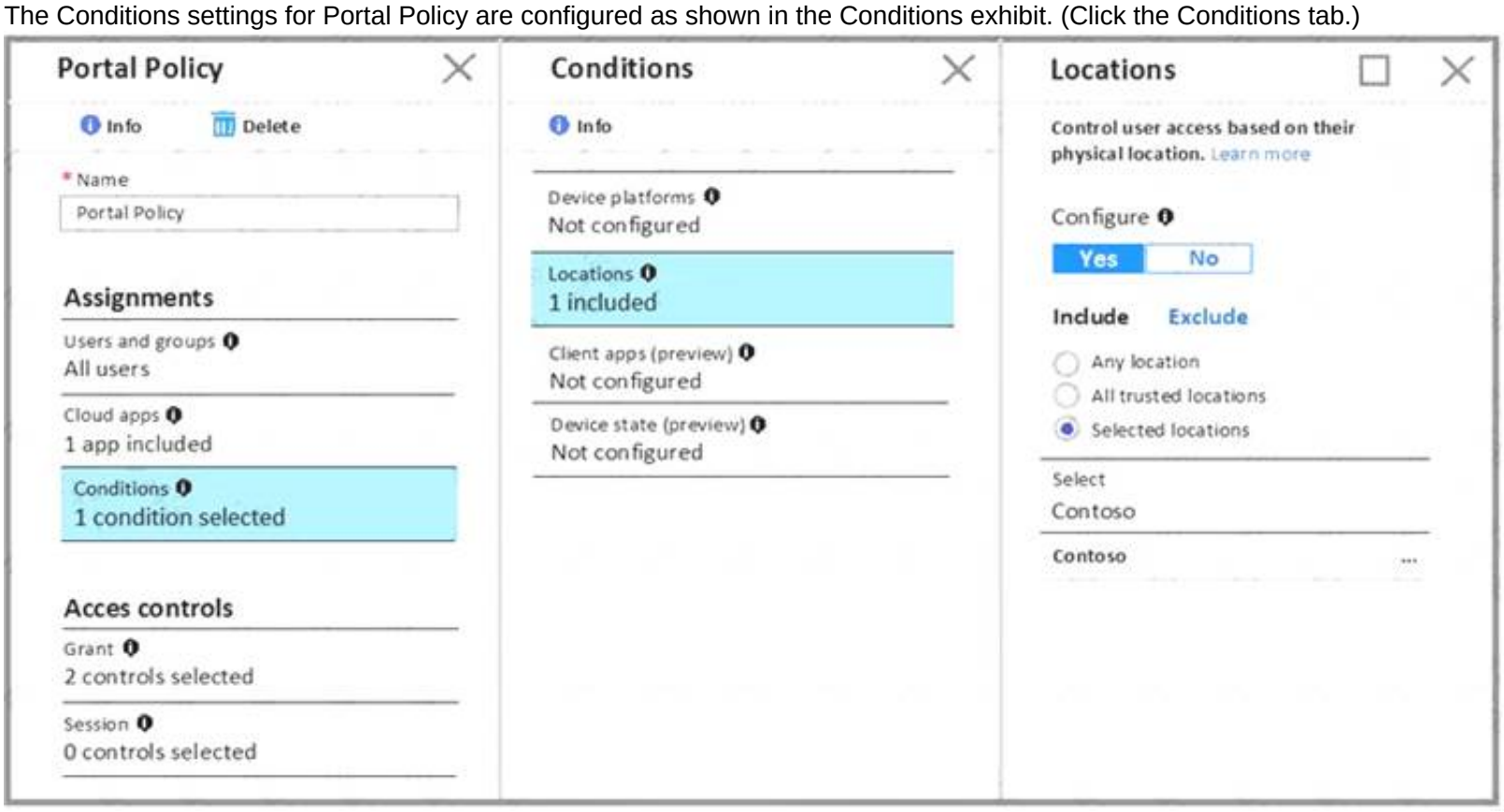
A. Yes
B. No

Answer: A

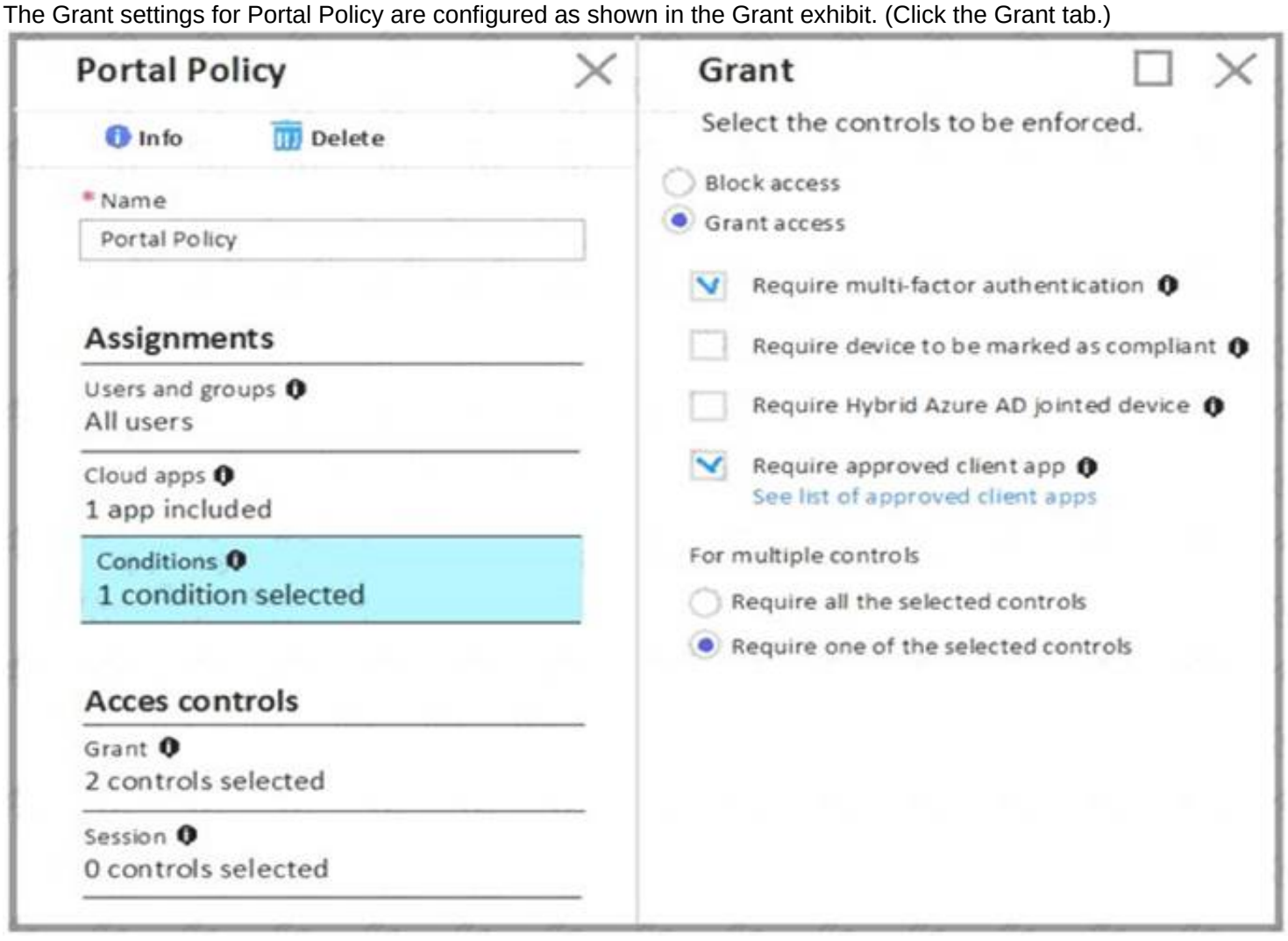
Explanation:

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

NEW QUESTION 192
- (Exam Topic 4)
You create a new Azure subscription that is associated to a new Azure Active Directory (Azure AD) tenant. You create one active conditional access policy named Portal Policy. Portal Policy is used to provide access to the Microsoft Azure Management cloud app.
The Conditions settings for Portal Policy are configured as shown in the Conditions exhibit. (Click the Conditions tab.)



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

Statements	Yes	No
Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	○	○
Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription.	○	○
Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	○	○

A. Mastered
B. Not Mastered

Answer: A

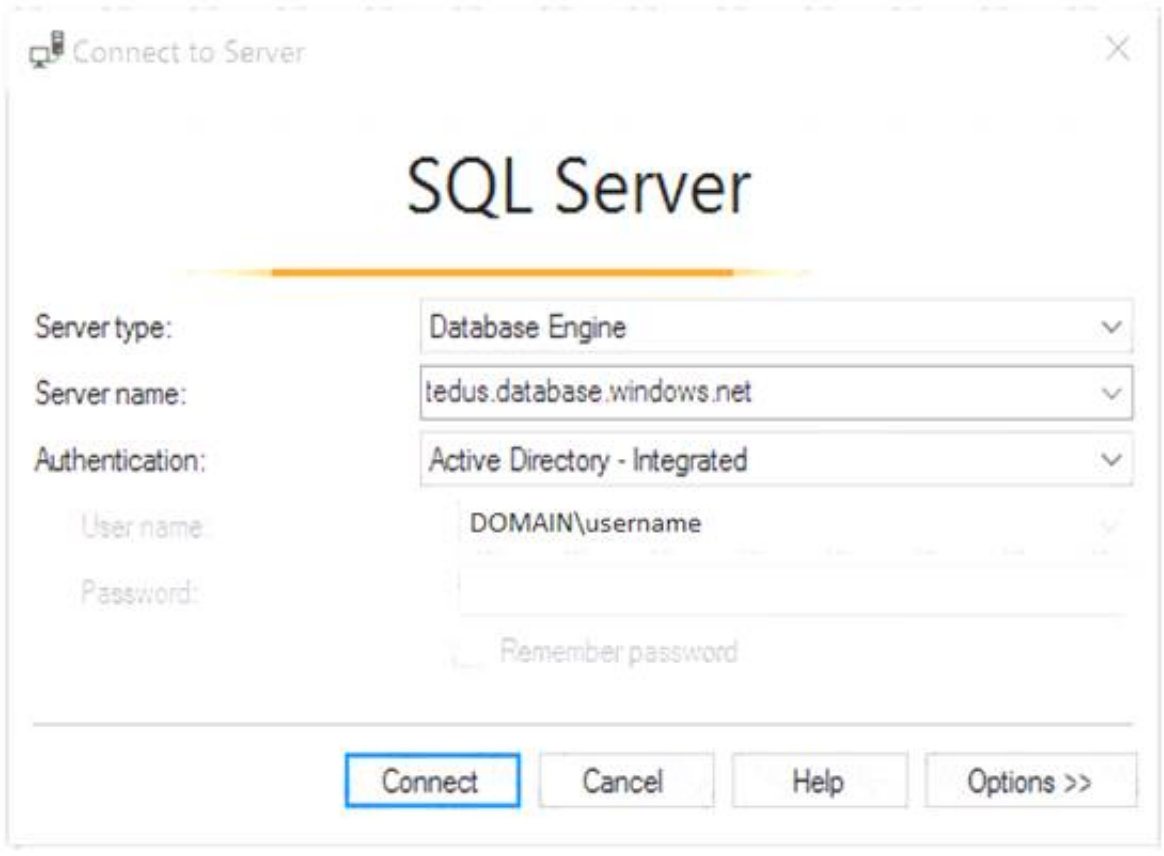
Explanation:
Box 1: No
The Contoso location is excluded
Box 2: NO
Box 3: NO
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

NEW QUESTION 193
- (Exam Topic 4)
You have a hybrid configuration of Azure Active Directory (Azure AD).
All users have computers that run Windows 10 and are hybrid Azure AD joined.
You have an Azure SQL database that is configured to support Azure AD authentication.
Database developers must connect to the SQL database by using Microsoft SQL Server Management Studio (SSMS) and authenticate by using their on-premises Active Directory account.
You need to tell the developers which authentication method to use to connect to the SQL database from SSMS. The solution must minimize authentication prompts.
Which authentication method should you instruct the developers to use?

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

Answer: C

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



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

NEW QUESTION 196
- (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.

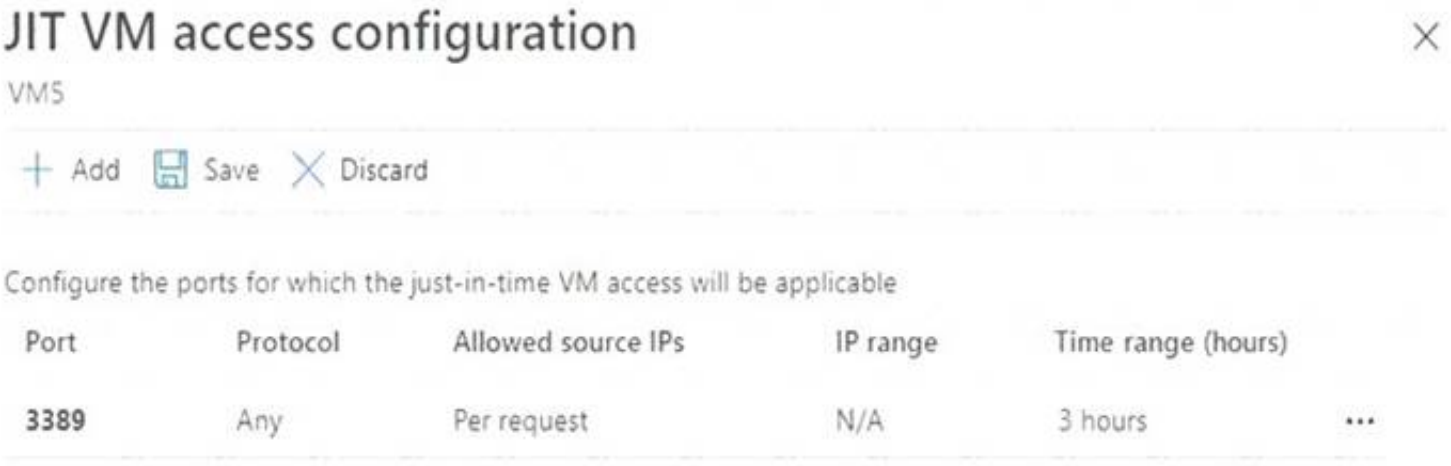
Answer: B

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

NEW QUESTION 199
- (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 200
- (Exam Topic 4)
You have an Azure subscription.
You configure the subscription to use a different Azure Active Directory (Azure AD) tenant. What are two possible effects of the change? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

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

Answer: AB

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

NEW QUESTION 201
- (Exam Topic 4)
You have Azure virtual machines that have Update Management enabled. The virtual machines are configured as shown in the following table.

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

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

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

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

A. Mastered
B. Not Mastered

Answer: A

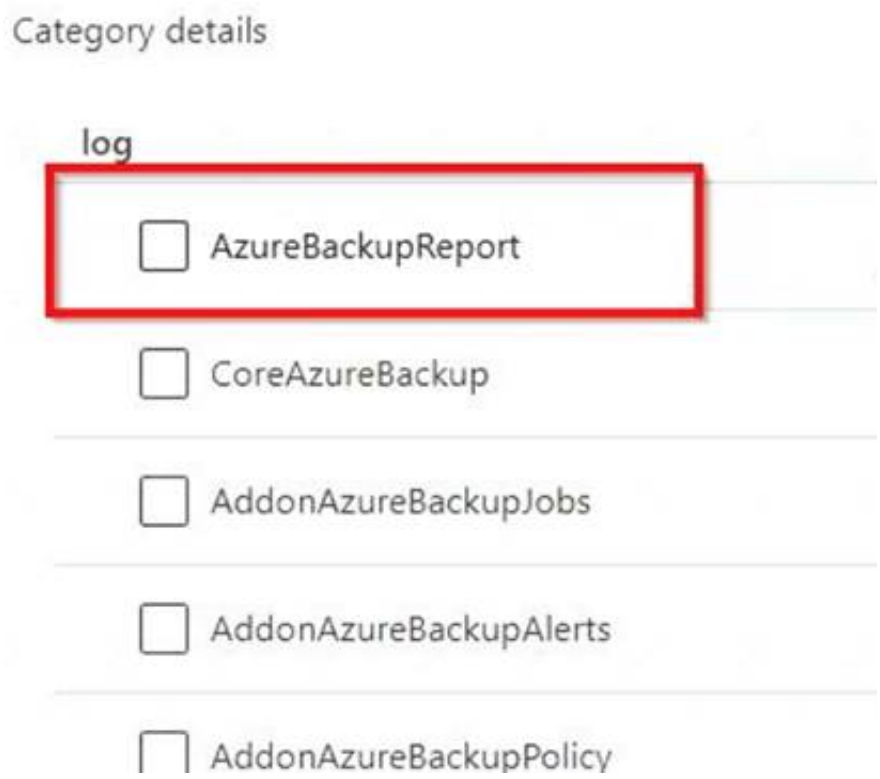
Explanation:
Update1: VM1 and VM2 only
VM3: Windows Server 2016 West US RG2 Update2: VM4 and VM5 only
VM6: CentOS 7.5 East US RG1
For Linux, the machine must have access to an update repository. The update repository can be private or public.
References:
https://docs.microsoft.com/en-us/azure/automation/automation-update-management

NEW QUESTION 203
- (Exam Topic 4)
You need to ensure that the AzureBackupReport log for the Vault1 Recovery Services vault is stored in the WS11641655 Azure Log Analytics workspace.
To complete this task, sign in to the Azure portal and modify the Azure resources.

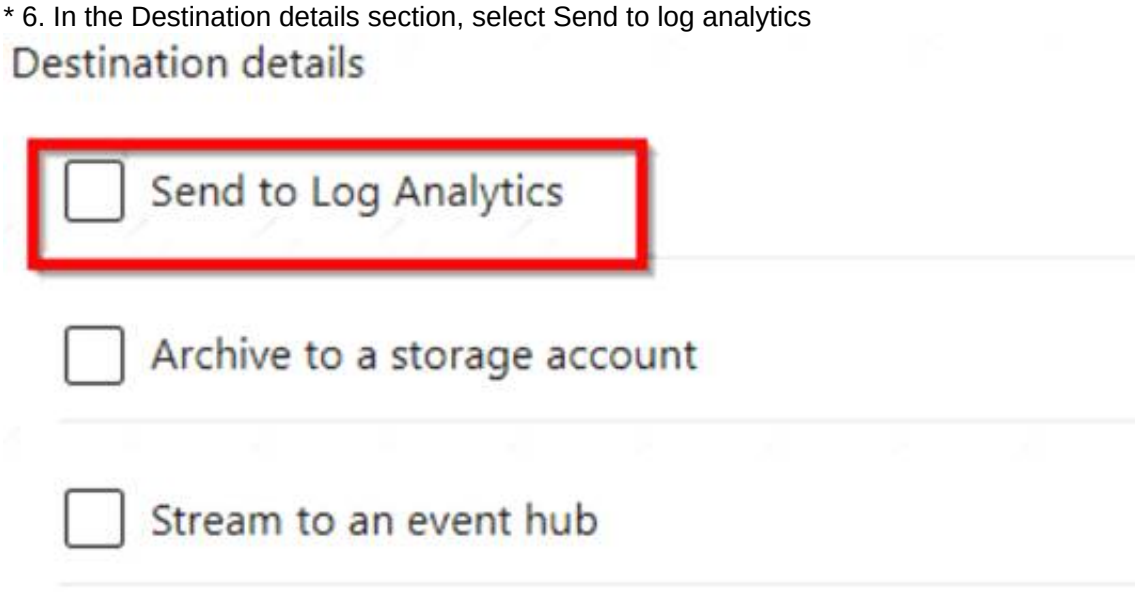
A. Mastered
B. Not Mastered

Answer: A

Explanation:
* 1. In the Azure portal, type Recovery Services Vaults in the search box, select Recovery Services Vaults from the search results then select Vault1. Alternatively, browse to Recovery Services Vaults in the left navigation pane.
* 2. In the properties of Vault1, scroll down to the Monitoring section and select Diagnostic Settings.
* 3. Click the Add a diagnostic setting link.
* 4. Enter a name in the Diagnostic settings name box.
* 5. In the Log section, select AzureBackupReport.



* 6. In the Destination details section, select Send to log analytics



* 7. Select the WS11641655 Azure Log Analytics workspace.
* 8. Click the Save button to save the changes. Reference:
https://docs.microsoft.com/en-us/azure/backup/backup-azure-diagnostic-events

NEW QUESTION 205
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Subscription. The subscription contains 50 virtual machines that run Windows Server 2012 R2 or Windows Server 2016.
You need to deploy Microsoft Antimalware to the virtual machines. Solution: You connect to each virtual machine and add a Windows feature. Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 207

- (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

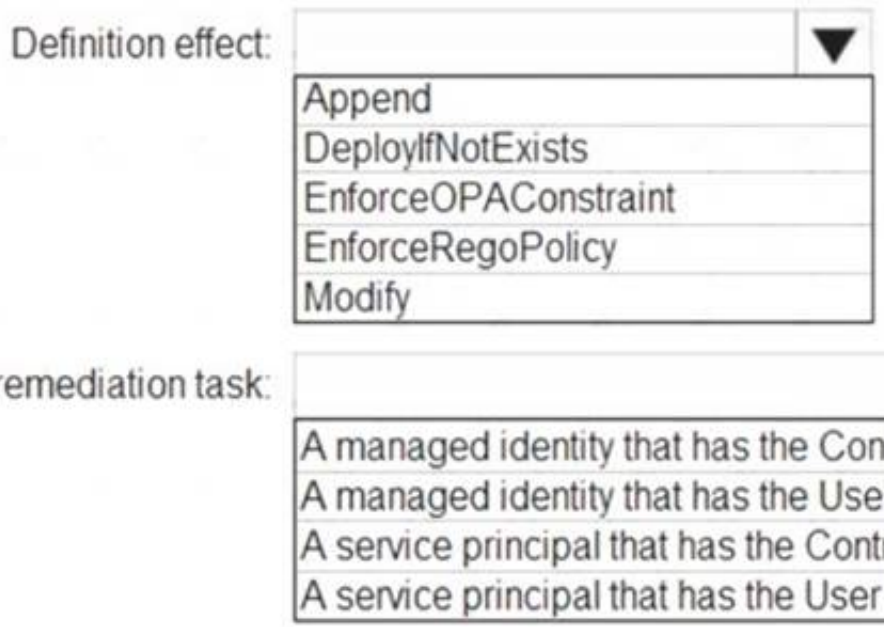
NEW QUESTION 209
- (Exam Topic 4)
You have an Azure subscription that contains a user named Adminl1 and a virtual machine named VM1. VM1 runs Windows Server 2019 and was deployed by using an Azure Resource Manager template. VM1 is the member of a backend pool of a public Azure Basic Load Balancer.
Admin1 reports that VM1 is listed as Unsupported on the Just in time VM access blade of Azure Security Center.
You need to ensure that Admin1 can enable just in time (JIT) VM access for VM1. What should you do?

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

Answer: A

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

NEW QUESTION 213
- (Exam Topic 4)
You have an Azure subscription.
You need to create and deploy an Azure policy that meets the following requirements:
- When a new virtual machine is deployed, automatically install a custom security extension.
- Trigger an autogenerated remediation task for non-compliant virtual machines to install the extension. What should you include in the policy? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 217
- (Exam Topic 4)
You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

You are assigned the Global administrator role for the tenant. You are responsible for managing Azure Security Center settings.
You need to create a custom sensitivity label. What should you do first?

A. Create a custom sensitive information type.
B. Elevate access for global administrators in Azure AD.
C. Upgrade the pricing tier of the Security Center to Standard.
D. Enable integration with Microsoft Cloud App Security.

Answer: A

Explanation:
First, you need to create a new sensitive information type because you can't directly modify the default rules. References:
https://docs.microsoft.com/en-us/office365/securitycompliance/customize-a-built-in-sensitive-information-type

NEW QUESTION 222
- (Exam Topic 4)
You have an Azure subscription that contains an Azure SQL database named SQL1. You plan to deploy a web app named App1.
You need to provide App1 with read and write access to SQL1. The solution must meet the following requirements:

- Provide App1 with access to SQL1 without storing a password.
- Use the principle of least privilege.
- Minimize administrative effort.

Which type of account should App1 use to access SQL1, and which database roles should you assign to App1? 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 Description automatically generated
Reference:
https://docs.microsoft.com/en-us/azure/app-service/tutorial-connect-msi-sql-database?tabs=windowsclient%2Cd

NEW QUESTION 224
- (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 226
- (Exam Topic 4)
You have an Azure subscription that contains an Azure Files share named share1 and a user named User1. Identity-based authentication is configured for share1. User1 attempts to access share1 from a Windows 10 device by using SMB. Which type of token will Azure Files use to authorize the request?

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

Answer: C

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

NEW QUESTION 228
- (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: D

NEW QUESTION 229
- (Exam Topic 4)
You have an Azure subscription that contains the virtual machines shown in the following table.

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

You create the Azure policies shown in the following table.

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

You create the resource locks shown in the following table.

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

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

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 233
- (Exam Topic 4)
You have an Azure subscription that contains a web app named App1 and an Azure key vault named Vault1. You need to configure App1 to store and access the secrets in Vault1.
How should you configure App1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Configure App1 to authenticate by using a:

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

Configure a Key Vault reference for App1 from the:

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 236
- (Exam Topic 4)
You have an Azure subscription that contains an Azure Sentinel workspace.
Azure Sentinel is configured to ingest logs from several Azure workloads. A third-party service management platform is used to manage incidents.
You need to identify which Azure Sentinel components to configure to meet the following requirements:
- When Azure Sentinel identifies a threat, an incident must be created.
- A ticket must be logged in the service management platform when an incident is created in Azure Sentinel.

Which component should you identify for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

NEW QUESTION 237
- (Exam Topic 4)
Your company has an Azure subscription named Sub1 that is associated to an Azure Active Directory Azure (Azure AD) tenant named contoso.com.
The company develops a mobile application named App1. App1 uses the OAuth 2 implicit grant type to acquire Azure AD access tokens.
You need to register App1 in Azure AD.
What information should you obtain from the developer to register the application?

A. a redirect URI
B. a reply URL
C. a key
D. an application ID

Answer: A

Explanation:
For Native Applications you need to provide a Redirect URI, which Azure AD will use to return token responses. References:
https://docs.microsoft.com/en-us/azure/active-directory/develop/v1-protocols-oauth-code

NEW QUESTION 240
- (Exam Topic 4)
You have an Azure virtual machines shown in the following table.

Name	Operating system	Region	Resource group
VM1	Windows Server 2012	East US	RG1
VM2	Windows Server 2012 R2	West Europe	RG1
VM3	Windows Server 2016	West Europe	RG2
VM4	Red Hat Enterprise Linux 7.4	East US	RG2

You create an Azure Log Analytics workspace named Analytics1 in RG1 in the East US region. Which virtual machines can be enrolled in Analytics1?

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

Answer: C

Explanation:
Note: Create a workspace
- In the Azure portal, click All services. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics.
- Click Create, and then select choices for the following items:

Provide a name for the new Log Analytics workspace, such as DefaultLAWorkspace. OMS workspaces are now referred to as Log Analytics workspaces.
Select a Subscription to link to by selecting from the drop-down list if the default selected is not appropriate. For Resource Group, select an existing resource group that contains one or more Azure virtual machines. Select the Location your VMs are deployed to. For additional information, see which regions Log Analytics is available in.

NEW QUESTION 241
- (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.

Answer Area

ASG1: [ ]

ASG2: [ ]

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

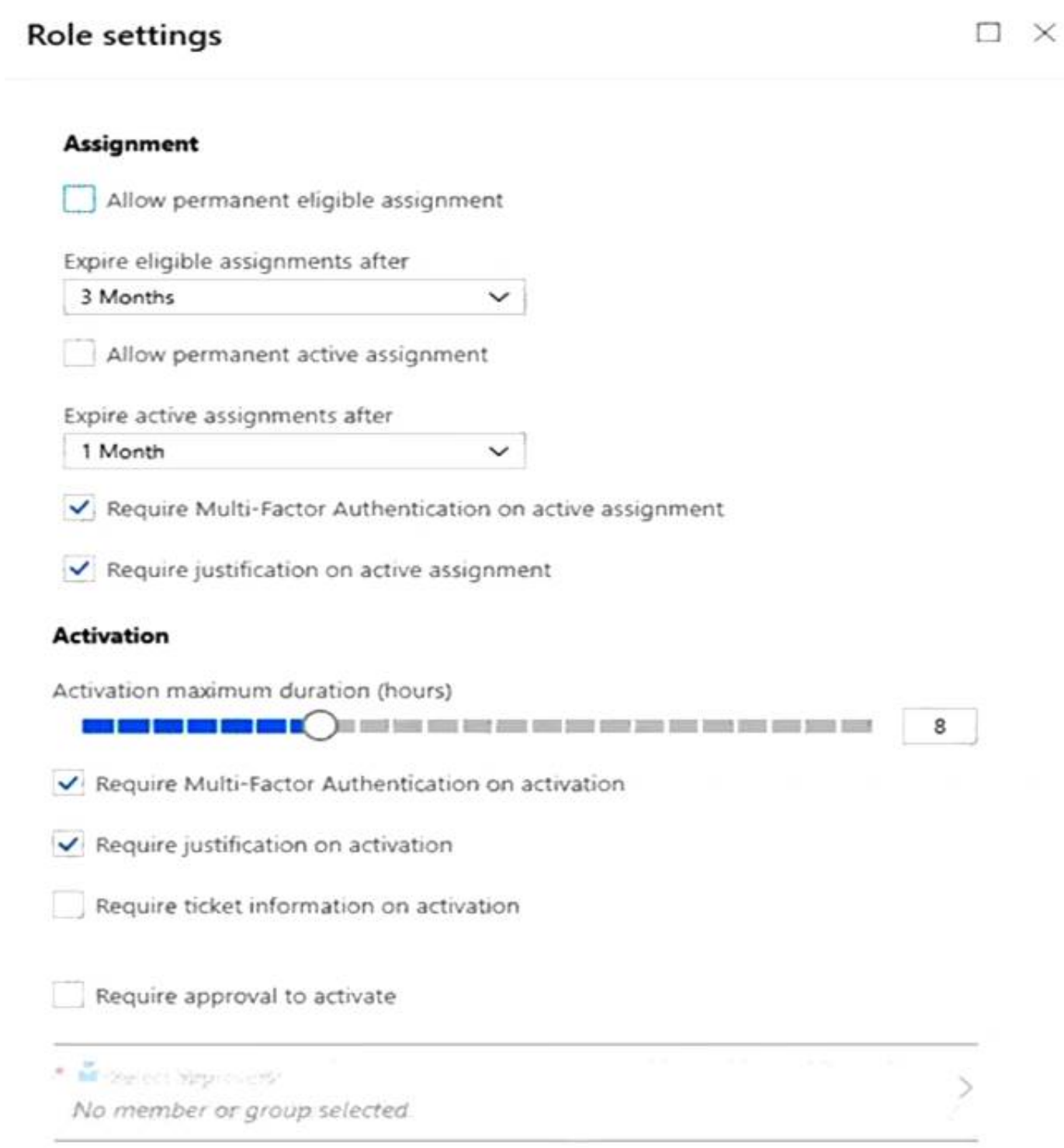
ASG1: VM2, VM3, and VM4 only

ASG2: VM1, VM2, and VM4 only

NEW QUESTION 243
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

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

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



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

Name	Assignment type
User1	Eligible
User2	Active
User3	Active

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

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 244
- (Exam Topic 4)
You need to recommend which virtual machines to use to host App1. The solution must meet the technical requirements for KeyVault1.
Which virtual machines should you use?

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

Answer: D

NEW QUESTION 247
- (Exam Topic 4)
A user named Debbie has the Azure app installed on her mobile device.
You need to ensure that debbie@contoso.com is alerted when a resource lock is deleted. To complete this task, sign in to the Azure portal.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
You need to configure an alert rule in Azure Monitor.
Type Monitor into the search box and select Monitor from the search results. Click on Alerts.
Click on +New Alert Rule.
In the Scope section, click on the Select resource link.
In the Filter by resource type box, type locks and select Management locks (locks) from the filtered results. Select the subscription then click the Done button.
In the Condition section, click on the Select condition link.
Select the Delete management locks condition the click the Done button. In the Action group section, click on the Select action group link.
Click the Create action group button to create a new action group.
Give the group a name such as Debbie Mobile App (it doesn't matter what name you enter for the exam) then click the Next: Notifications > button.
In the Notification type box, select the Email/SMS message/Push/Voice option.
In the Email/SMS message/Push/Voice window, tick the Azure app Push Notifications checkbox and enter debbie@contoso.com in the Azure account email field.
Click the OK button to close the window.
Enter a name such as Debbie Mobile App in the notification name box.
Click the Review & Create button then click the Create button to create the action group.
Back in the Create alert rule window, in the Alert rule details section, enter a name such as Management lock deletion in the Alert rule name field.
Click the Create alert rule button to create the alert rule.

NEW QUESTION 252
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Security Center for the centralized policy management of three Azure subscriptions. You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create an initiative and an assignment that is scoped to a management group. Does this meet the goal?

A. Yes
B. No

Answer: A

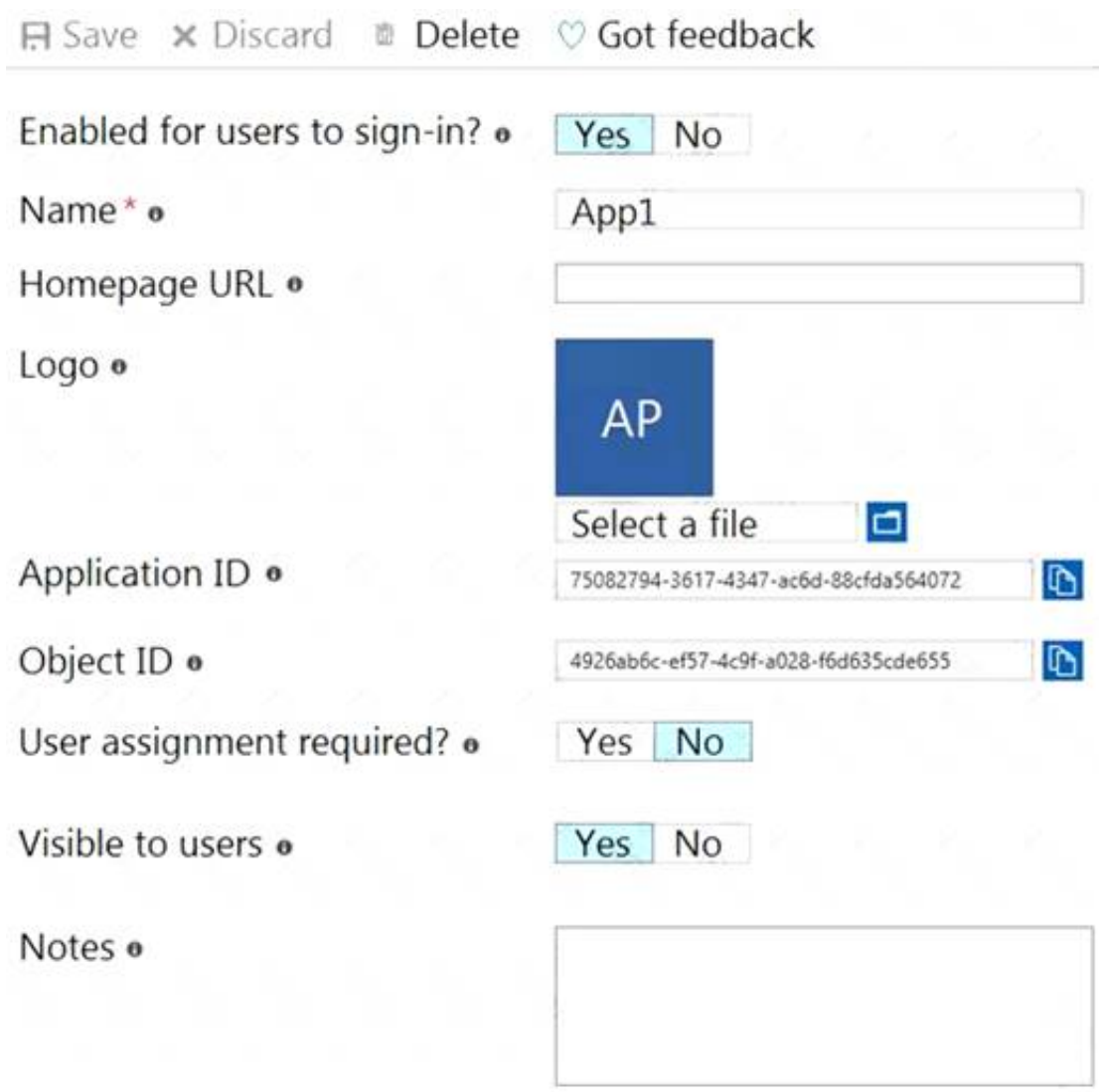
Explanation:
References:
https://docs.microsoft.com/en-us/azure/governance/policy/overview

NEW QUESTION 257
- (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 260
- (Exam Topic 4)
You have a Azure subscription that contains an Azure Container Registry named Registry1. The subscription uses the Standard use tier of Azure Security Center.
You upload several container images to Register1.
You discover that vulnerability security scans were not performed
You need to ensured that the images are scanned for vulnerabilities when they are uploaded to Registry1. What should you do?

A. From the Azure portal modify the Pricing tier settings.
B. From Azure CLI, lock the container images.
C. Upload the container images by using AzCopy
D. Push the container images to Registry1 by using Docker

Answer: A

Explanation:
Reference:
https://charbelnemnom.com/scan-container-images-in-azure-container-registry-with-azure-security-center/

NEW QUESTION 264
- (Exam Topic 4)
You have an Azure virtual machine named VM1.
From Azure Security Center, you get the following high-severity recommendation: “Install endpoint protection solutions on virtual machine”.
You need to resolve the issue causing the high-severity recommendation. What should you do?

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

Answer: A

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

NEW QUESTION 269
- (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 machine to the existing virtual network 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. the Contributor role for the subscription
B. the Network Contributor role for RG2
C. A custom RBAC role for the subscription
D. a custom RBAC role for RG2
E. the Network Contributor role for RG1.
F. the Virtual Machine Contributor role for RG1.

Answer: BF

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

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

Answer: D

Explanation:
A network security group (NSG) enables you to filter inbound traffic to, and outbound traffic from, a virtual machine (VM). You can log network traffic that flows through an NSG with Network Watcher's NSG flow log
capability. Steps include:
- Create a VM with a network security group
- Enable Network Watcher and register the Microsoft.Insights provider
- Enable a traffic flow log for an NSG, using Network Watcher's NSG flow log capability
- Download logged data
- View logged data Reference:

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

NEW QUESTION 278
- (Exam Topic 4)
You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

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

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

You need to ingest the CEF messages from the NVAs to Azure Sentinel.
What should you configure for each subscription? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 283
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.

Name	Type
storage1	Storage account
Vault1	Azure Key vault
Vault2	Azure Key vault

You plan to deploy the virtual machines shown in the following table.

Name	Role
VM1	• Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1
VM2	• Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1
VM3	• Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1 • Key Vault Reader for Vault2
VM4	• Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1 • Key Vault Reader for Vault2

You need to assign managed identities to the virtual machines. The solution must meet the following requirements:
- Assign each virtual machine the required roles.
- Use the principle of least privilege.

What is the minimum number of managed identities required?

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

Answer: B

Explanation:
We have two different sets of required permissions. VM1 and VM2 have the same permission requirements. VM3 and VM4 have the same permission requirements.
A user-assigned managed identity can be assigned to one or many resources. By using user-assigned managed identities, we can create just two managed identities: one with the permission requirements for VM1 and VM2 and the other with the permission requirements for VM3 and VM4.
Reference:

https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

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

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

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

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

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

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

Answer: C

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

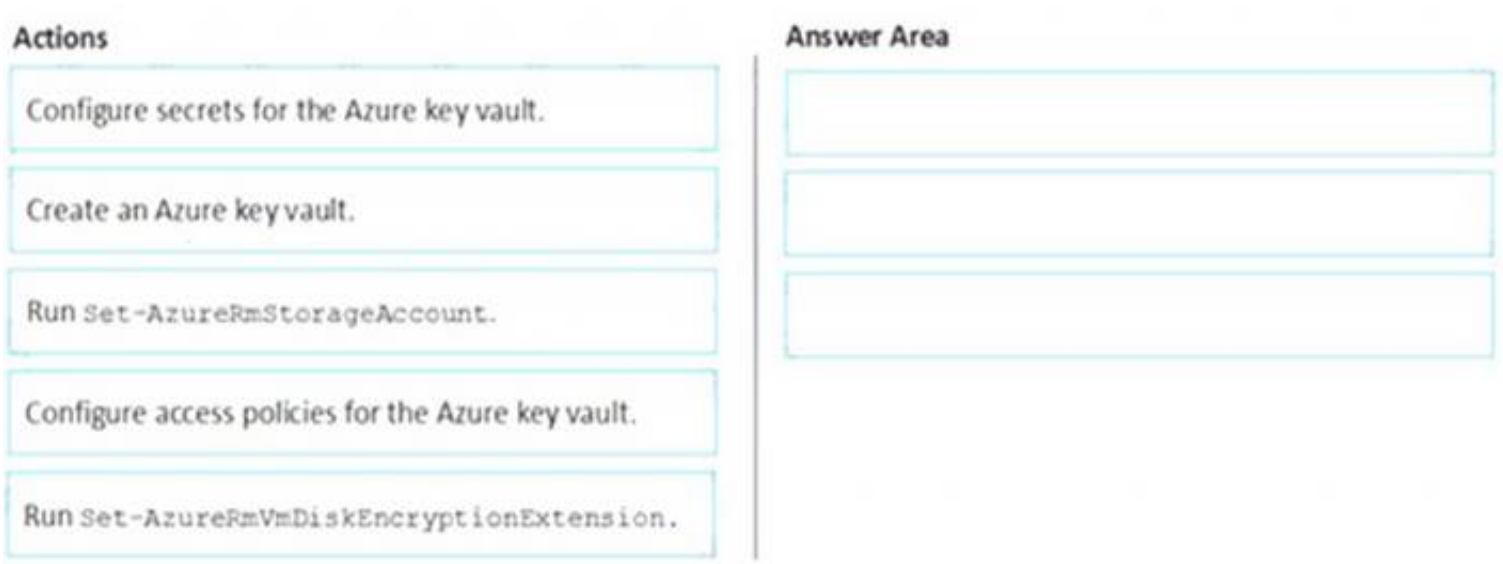
NEW QUESTION 290
- (Exam Topic 4)
Your network contains an Active Directory forest named contoso.com. The forest contains a single domain.
You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
You plan to deploy Azure AD Connect 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 294
- (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. Sub1 contains an Azure virtual machine named VM1 that runs Windows Server 2016.
You need to encrypt VM1 disks by using Azure Disk Encryption.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/encrypt-disks

NEW QUESTION 299
- (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.

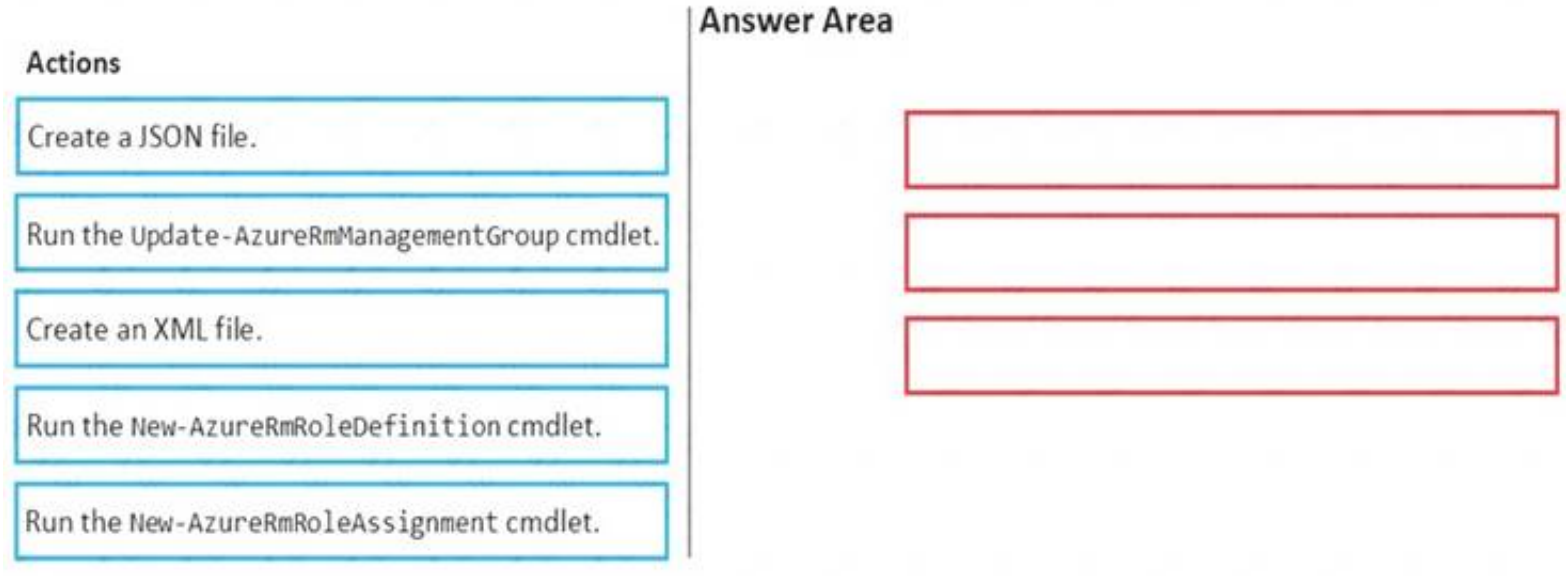
Which images are trusted images?

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 300
- (Exam Topic 4)
You have an Azure subscription named Sub1.
You have an Azure Active Directory (Azure AD) group named Group1 that contains all the members of your IT team.
You need to ensure that the members of Group1 can stop, start, and restart the Azure virtual machines in Sub1. The solution must use the principle of least privilege.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 303
- (Exam Topic 4)
You need to ensure that User2-11641655 has all the key permissions for KeyVault11641655. To complete this task, sign in to the Azure portal and modify the Azure resources.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
You need to assign the user the Key Vault Secrets Officer role.
- In the Azure portal, type Key Vaults in the search box, select Key Vaults from the search results then select KeyVault11641655. Alternatively, browse to Key Vaults in the left navigation pane.
- In the key vault properties, select Access control (IAM).
- In the Add a role assignment section, click the Add button.
- In the Role box, select the Key Vault Secrets Officer role from the drop-down list.
- In the Select box, start typing User2-11641655 and select User2-11641655 from the search results.
- Click the Save button to save the changes.

NEW QUESTION 308
- (Exam Topic 4)
You have an Azure subscription that contains the Azure Active Directory (Azure AD) resources shown in the following table.

Name	Description
User1	User
Group1	Security group that has a Membership type of Dynamic Device
Managed1	Managed identity
App1	Enterprise application

You create the groups shown in the following table.

Name	Description
Group5	Security group that has a Membership type of Assigned
Group6	Microsoft 365 group that has a Membership type of Assigned

Which resources can you add to Group5 and Group6? 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 Description automatically generated

NEW QUESTION 313

.....

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