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 are configuring and securing a network environment.
You deploy an Azure virtual machine named VM1 that is configured to analyze network traffic. You need to ensure that all network traffic is routed through VM1.
What should you configure?

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

Answer: C

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

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

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

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

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

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

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

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 4
- (Exam Topic 4)
You have an Azure subscription that contains 100 virtual machines. Azure Diagnostics is enabled on all the virtual machines.
You are planning the monitoring of Azure services in the subscription. You need to retrieve the following details:

- Identify the user who deleted a virtual machine three weeks ago.
- Query the security events of a virtual machine that runs Windows Server 2016.

What should you use in Azure Monitor? To answer, drag the appropriate configuration settings to the correct details. Each configuration setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Settings

- Activity log
- Logs
- Metrics
- Service Health

Answer Area

Identify the user who deleted a virtual machine three weeks ago: [ ]

Query the security events of a virtual machine that runs Windows Server 2016: [ ]

A. Mastered
B. Not Mastered

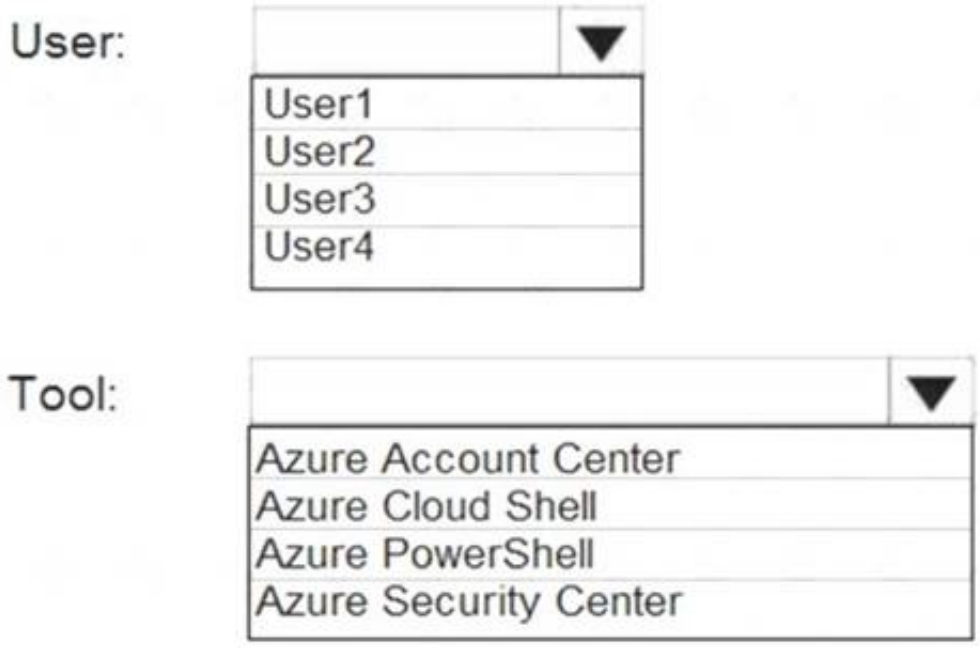
Answer: A

Explanation:
Box1: Activity log
Azure activity logs provide insight into the operations that were performed on resources in your subscription. Activity logs were previously known as “audit logs” or “operational logs,” because they report control-plane events for your subscriptions.
Activity logs help you determine the “what, who, and when” for write operations (that is, PUT, POST, or DELETE).
Box 2: Logs
Log Integration collects Azure diagnostics from your Windows virtual machines, Azure activity logs, Azure Security Center alerts, and Azure resource provider logs. This integration provides a unified dashboard for all your assets, whether they're on-premises or in the cloud, so that you can aggregate, correlate, analyze, and alert for security events.
References:
https://docs.microsoft.com/en-us/azure/security/azure-log-audit

NEW QUESTION 5
- (Exam Topic 4)
Your company has an Azure subscription named Subscription1 that contains the users shown in the following table.

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

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



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 6
- (Exam Topic 4)
You need to configure a virtual network named VNET2 to meet the following requirements:
- Administrators must be prevented from deleting VNET2 accidentally.
- Administrators must be able to add subnets to VNET2 regularly.

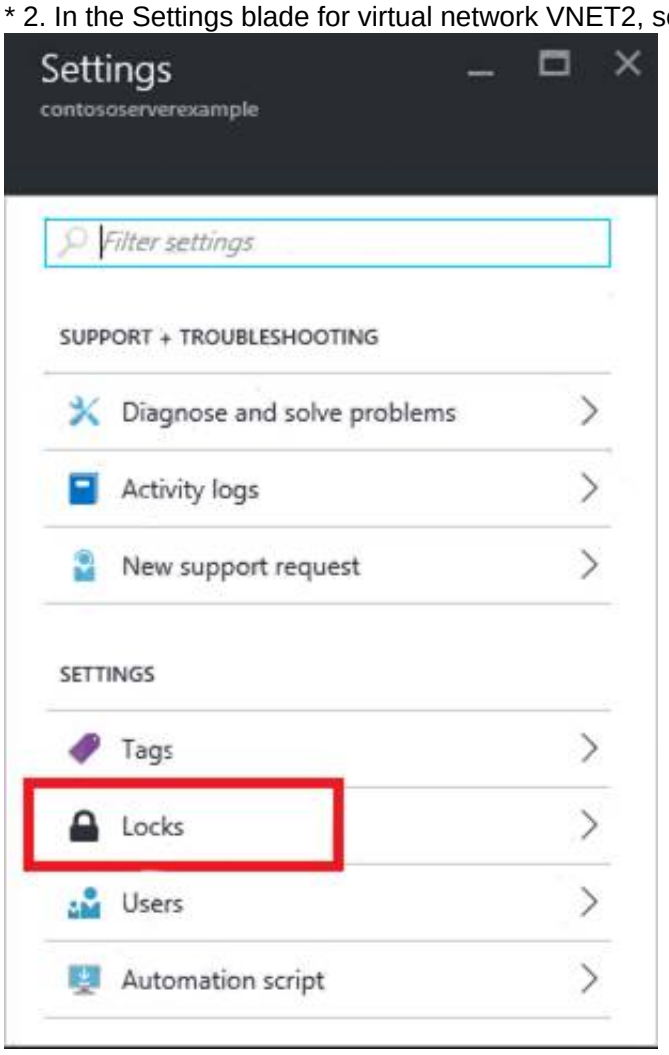
To complete this task, sign in to the Azure portal and modify the Azure resources.

A. Mastered
B. Not Mastered

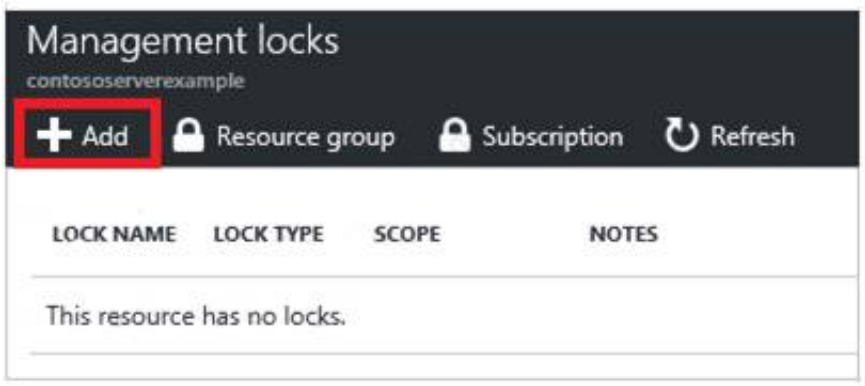
Answer: A

Explanation:
Locking prevents other users in your organization from accidentally deleting or modifying critical resources, such as Azure subscription, resource group, or

resource.
Note: In Azure, the term resource refers to an entity managed by Azure. For example, virtual machines, virtual networks, and storage accounts are all referred to as Azure resources.
* 1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET2. Alternatively, browse to Virtual Networks in the left navigation pane.
* 2. In the Settings blade for virtual network VNET2, select Locks.



* 3. To add a lock, select Add.



* 4. For Lock type select Delete lock, and click OK Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources

NEW QUESTION 7
- (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 8
- (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

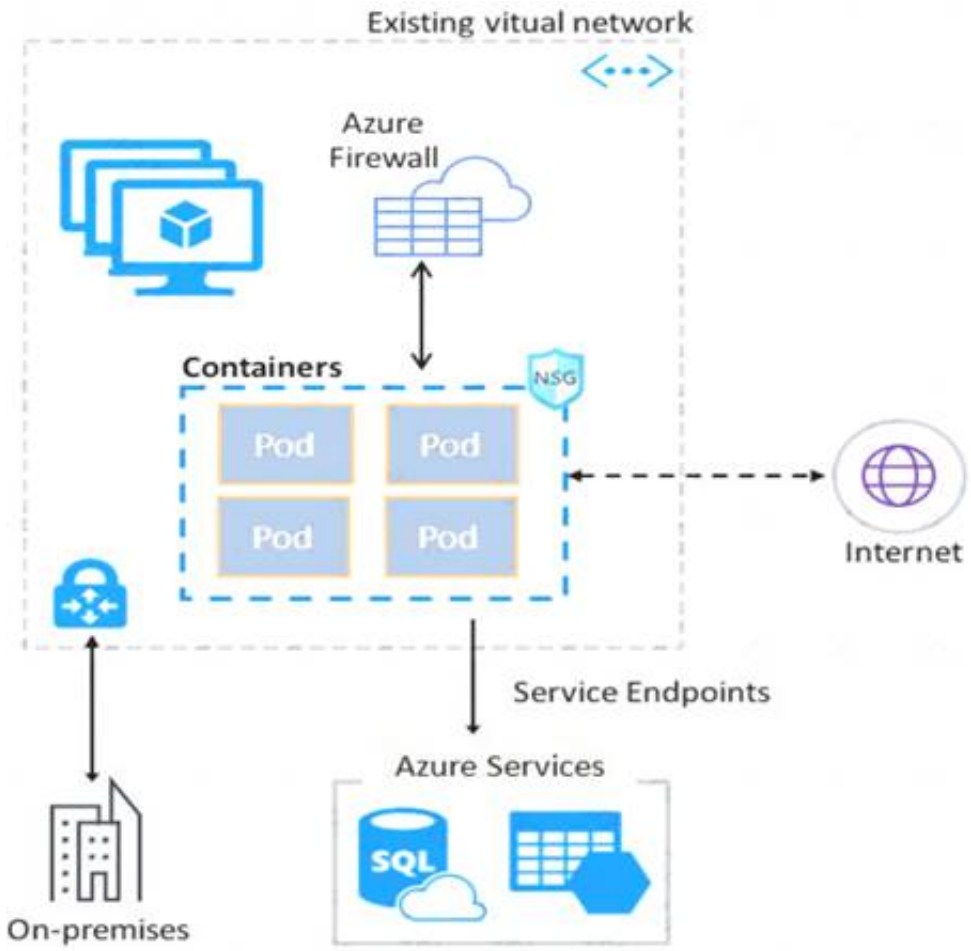
Answer: B

NEW QUESTION 9
- (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 10
- (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 10

- (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

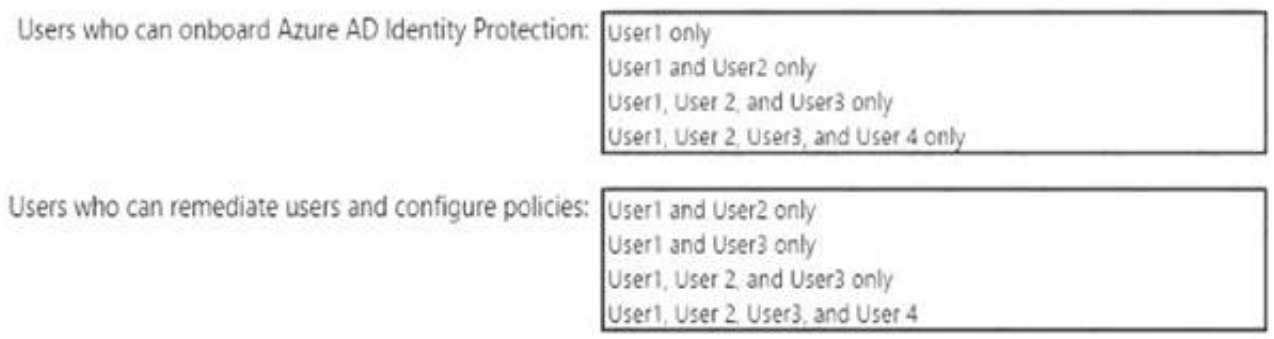
Answer: D

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

NEW QUESTION 14
- (Exam Topic 4)
You have an Azure subscription named Sub 1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

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

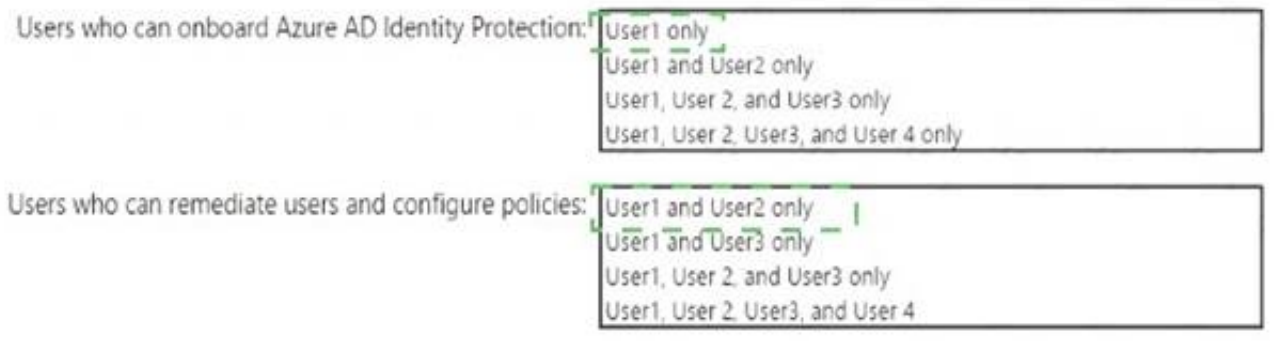
Each user is assigned an Azure AD Premium P2 license.
You plan lo onboard and configure Azure AD identity Protection.
Which users can onboard Azure AD Identity Protection, remediate users, and configure policies? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection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



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area



NEW QUESTION 16
- (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.

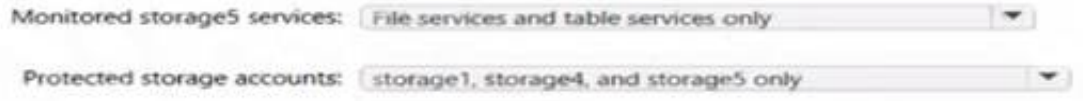
Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

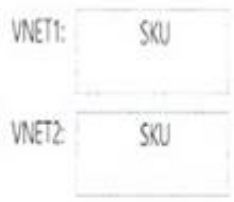
Answer Area



NEW QUESTION 19
- (Exam Topic 4)
You are configuring network connectivity for two Azure virtual networks named VNET1 and VNET2. You need to implement VPN gateways for the virtual networks to meet the following requirements:
* VNET1 must have six site-to-site connections that use BGP.
* VNET2 must have 12 site-to-site connections that use BGP.
* Costs must be minimized.
Which VPN gateway SKI) should you use for each virtual network? To answer, drag the appropriate SKUs to the correct networks. Each SKU may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point

SKUs

Answer Area



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 22
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions
will not appear in the review screen.
You use Azure Security Center for the centralized policy management of three Azure subscriptions. You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create a policy definition and assignments that are scoped to resource groups. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

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

NEW QUESTION 24
- (Exam Topic 4)
You have an Azure subscription that contains the virtual machines shown in the following table.

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

You create the Azure policies shown in the following table.

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

You create the resource locks shown in the following table.

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

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

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 26
- (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 29
- (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 34
- (Exam Topic 4)
You have an Azure subscription that contains the virtual machines shown in the following table.

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

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

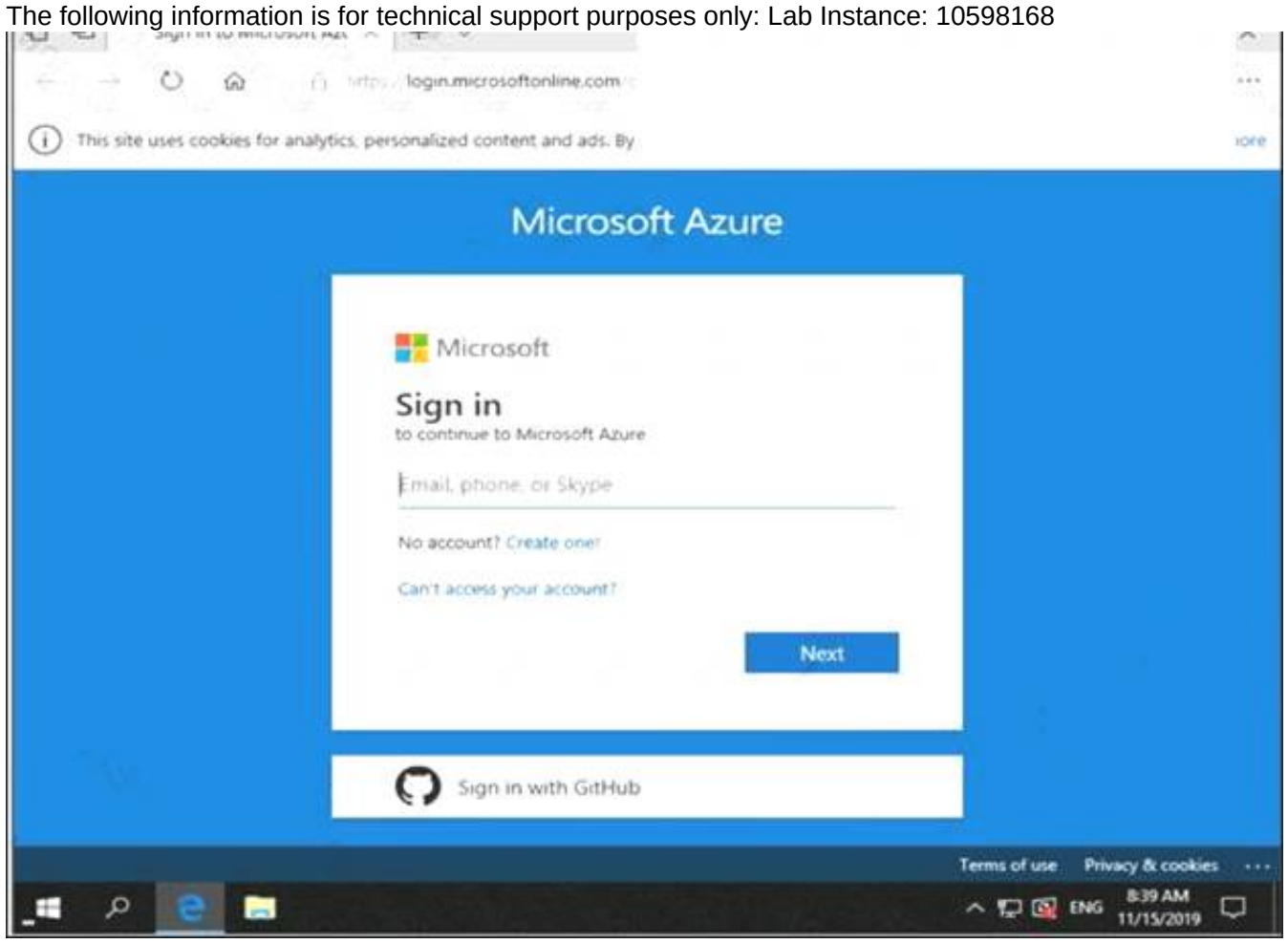
Name	Operating system
VM3	Windows Server 2016
VM4	Ubuntu Server 18.04 LTS

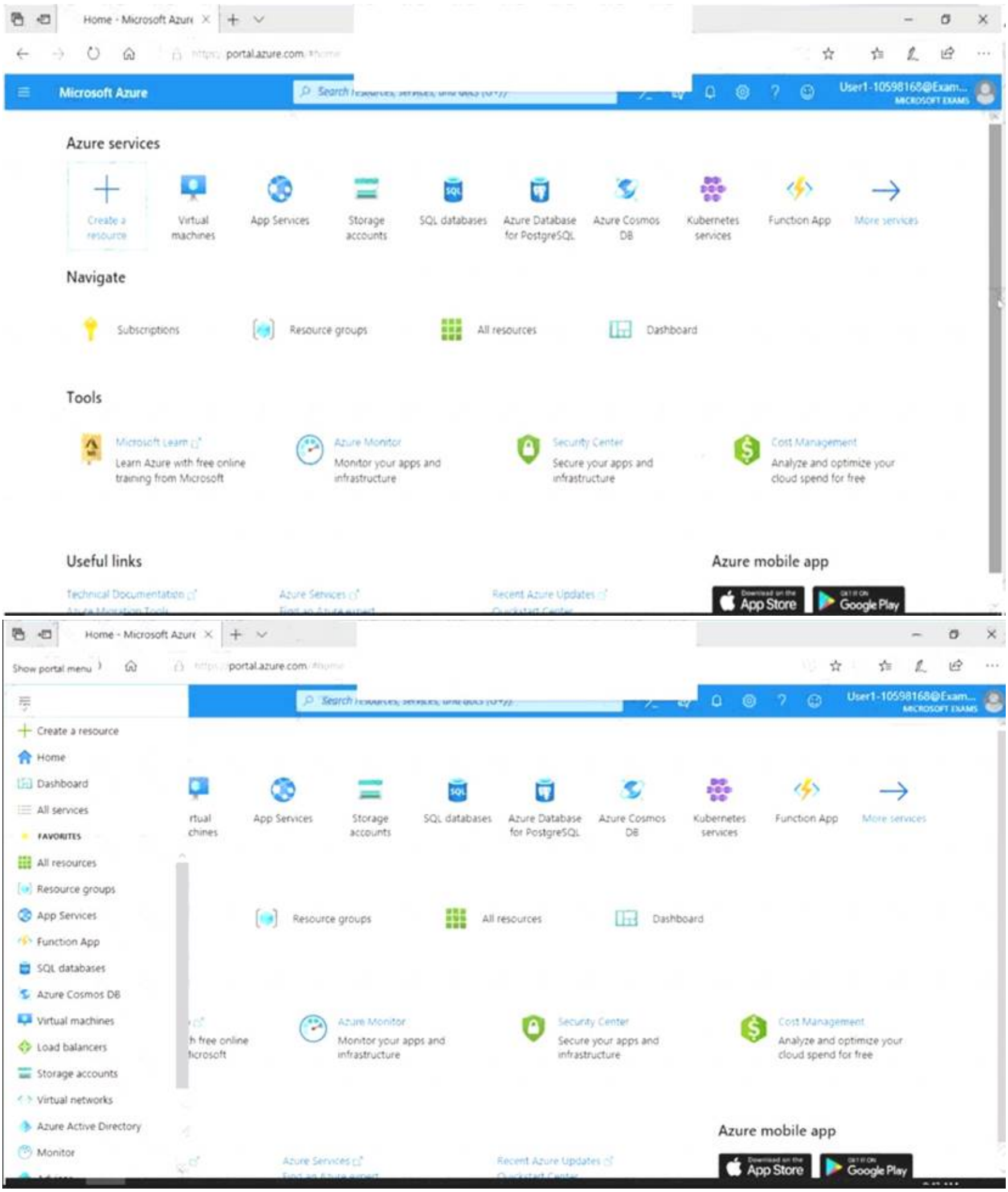
On which virtual machines is the Log Analytics agent installed?

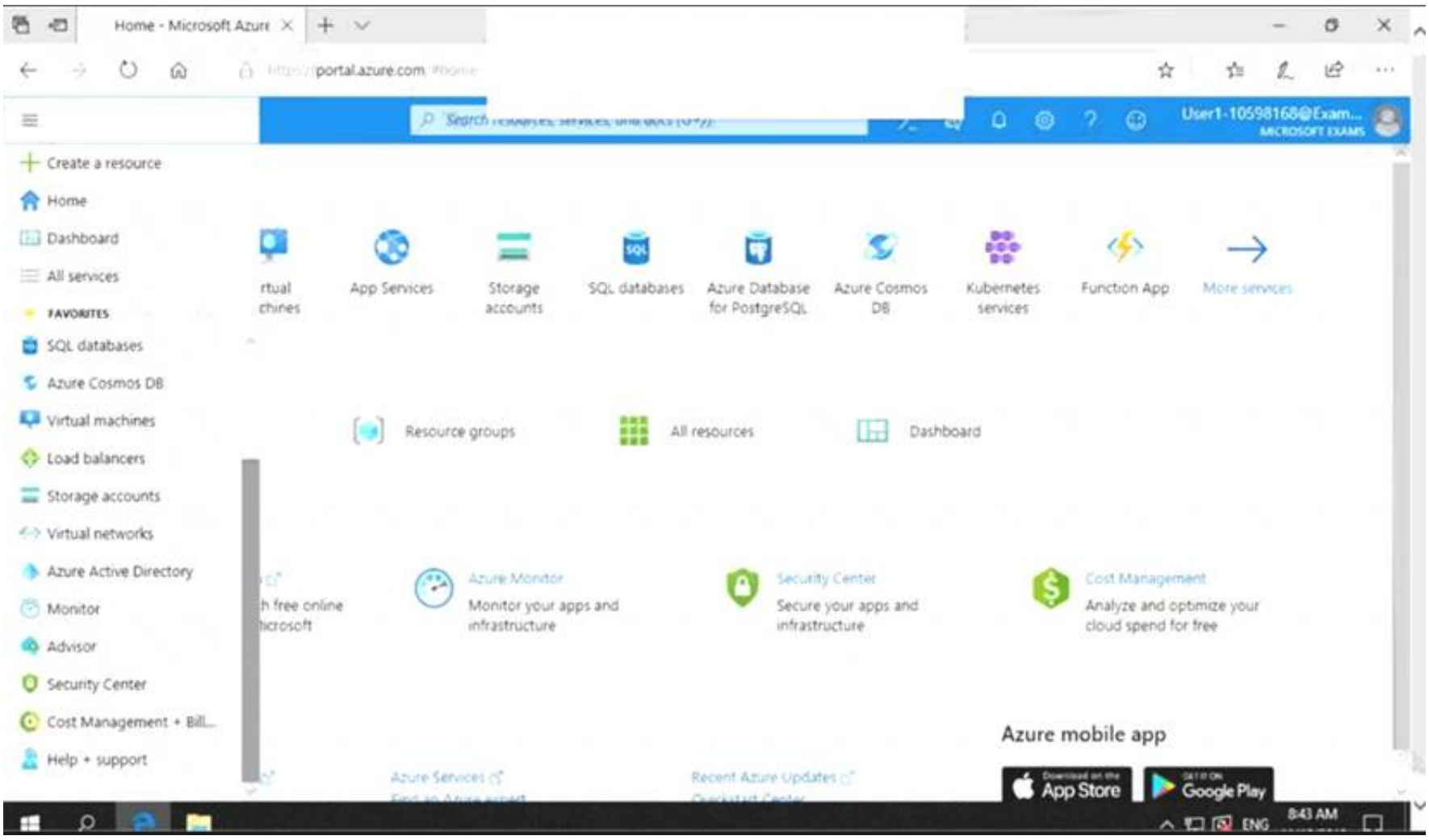
A. VM3 only
B. VM1 and VM3 only
C. VM3 and VM4 only
D. VM1, VM2, VM3, and VM4

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

NEW QUESTION 39
- (Exam Topic 4)
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below. Azure Username: User1-10598168@ExamUsers.com
Azure Password: Ag1Bh9!#Bd
The following information is for technical support purposes only: Lab Instance: 10598168




Home - Microsoft Azure
portal.azure.com
Microsoft Azure
Search resources, services, and docs (G+/)
User1-10598168@Exam...
MICROSOFT EXAMS
Azure services
Create a resource
Virtual machines
App Services
Storage accounts
SQL databases
Azure Database for PostgreSQL
Azure Cosmos DB
Kubernetes services
Function App
More services
Navigate
Subscriptions
Resource groups
All resources
Dashboard
Tools
Microsoft Learn
Learn Azure with free online training from Microsoft
Azure Monitor
Monitor your apps and infrastructure
Security Center
Secure your apps and infrastructure
Cost Management
Analyze and optimize your cloud spend for free
Useful links
Technical Documentation
Azure Services
Recent Azure Updates
Azure mobile app
App Store
Google Play
Show portal menu
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor

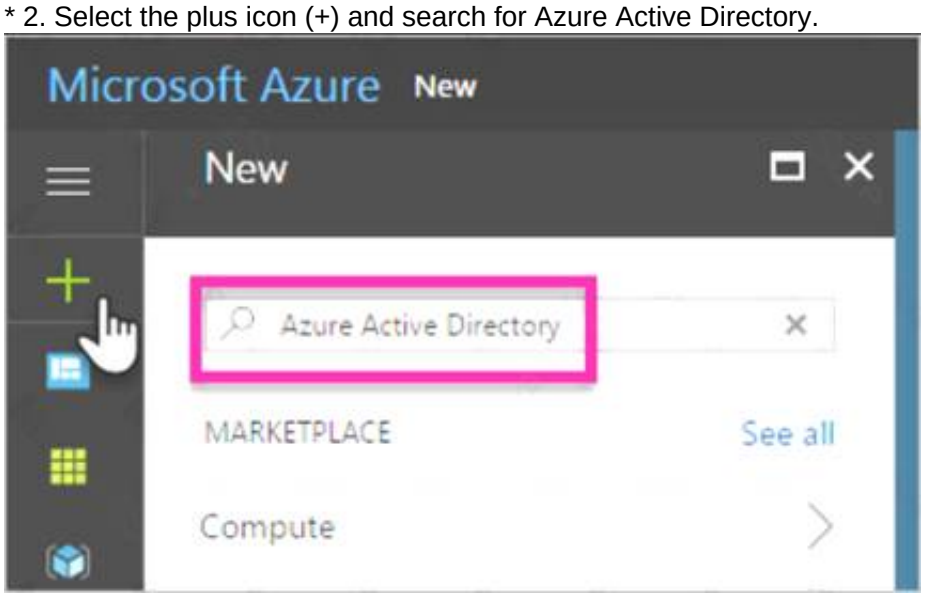


You need to create a new Azure Active Directory (Azure AD) directory named 10598168.onmicrosoft.com. The new directory must contain a user named user1@10598168.onmicrosoft.com who is configured to sign in by using Azure Multi-Factor Authentication (MFA).
To complete this task, sign in to the Azure portal.

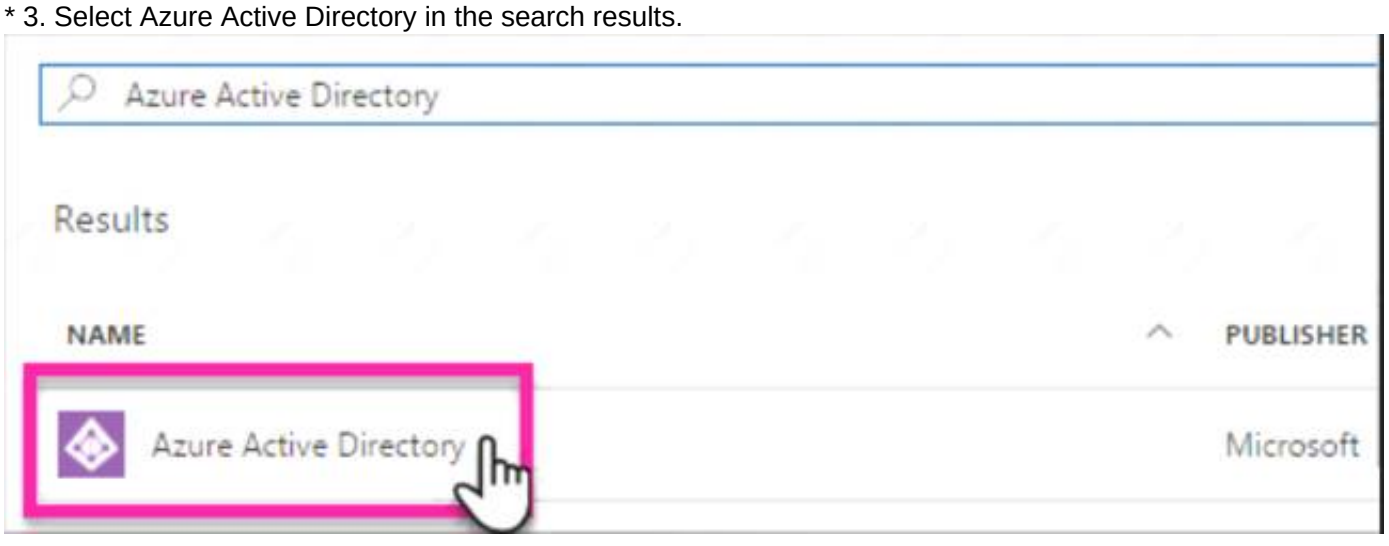
A. Mastered
B. Not Mastered

Answer: A

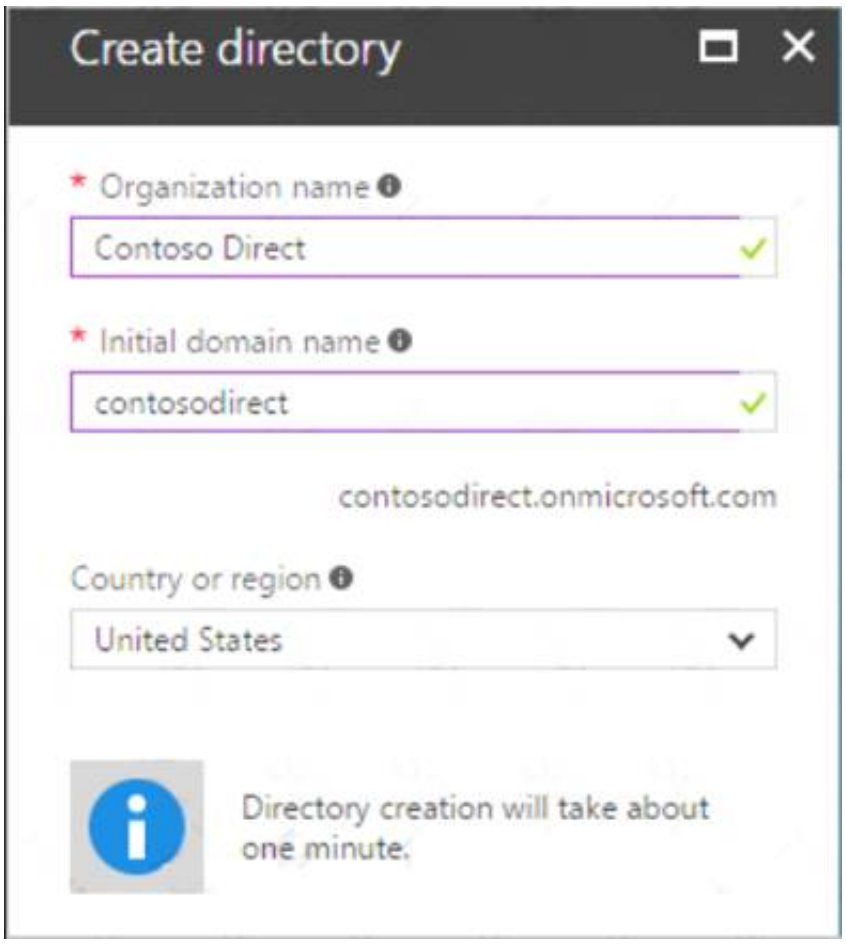
Explanation:
Step 1: Create an Azure Active Directory tenant
* 1. Browse to the Azure portal and sign in with an account that has an Azure subscription.
* 2. Select the plus icon (+) and search for Azure Active Directory.



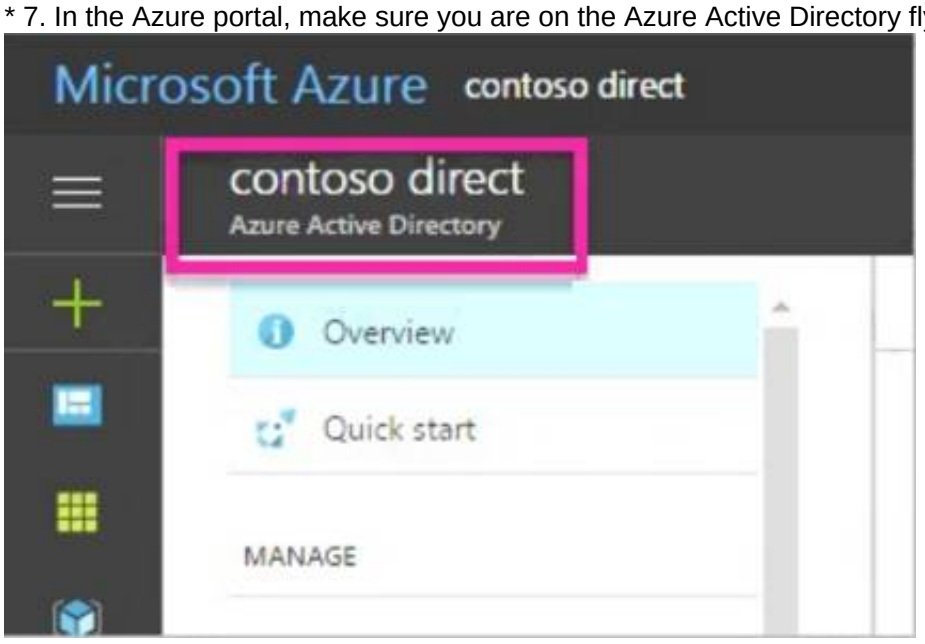
* 3. Select Azure Active Directory in the search results.



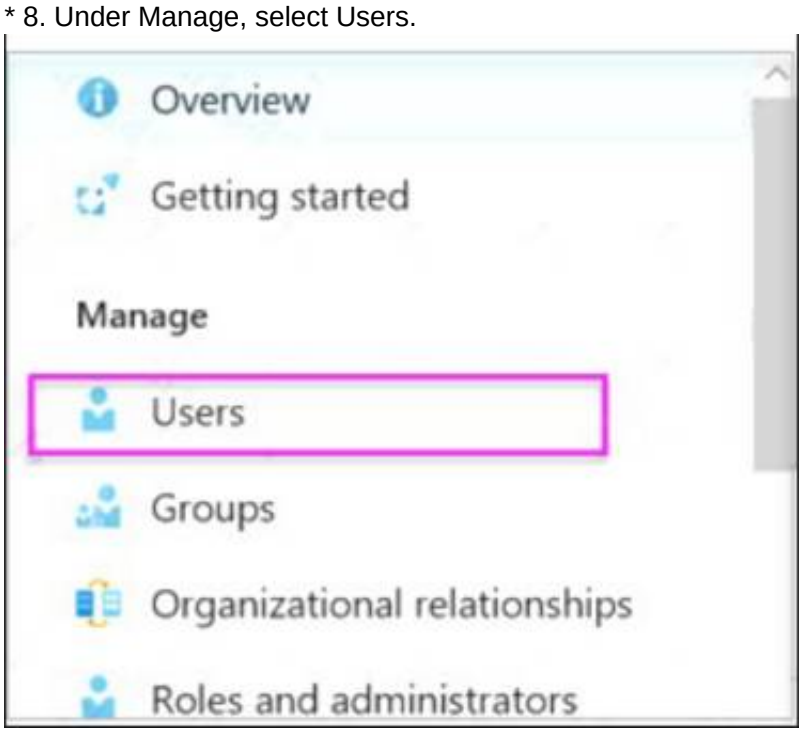
* 4. Select Create.
* 5. Provide an Organization name and an Initial domain name (10598168). Then select Create. Your directory is created.



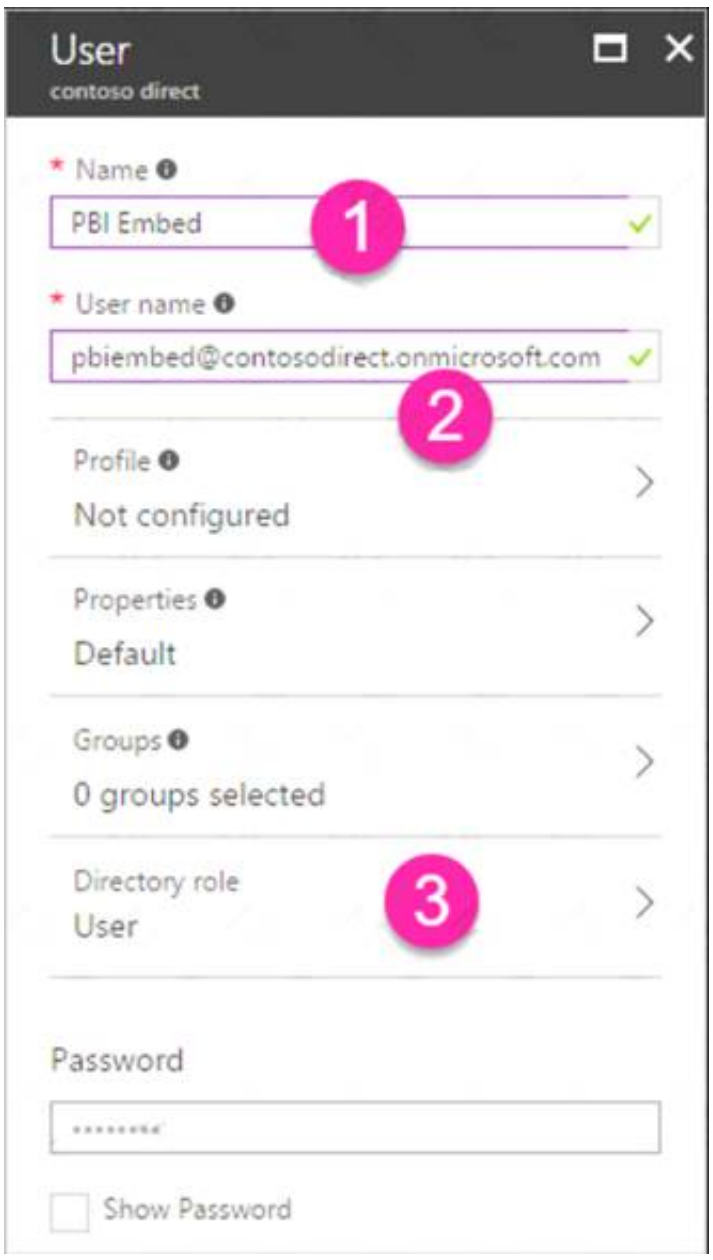
* 6. After directory creation is complete, select the information box to manage your new directory.Next, you're going to add tenant users.
Step 2: Create an Azure Active Directory tenant user
* 7. In the Azure portal, make sure you are on the Azure Active Directory fly out.



* 8. Under Manage, select Users.



* 9. Select All users and then select + New user.
* 10. Provide a Name and User name (user1) for the regular user tenant You can also show the temporary password. When you're done, select Create.
Name: user1
User name: user1@10598168.onmicrosoft.com

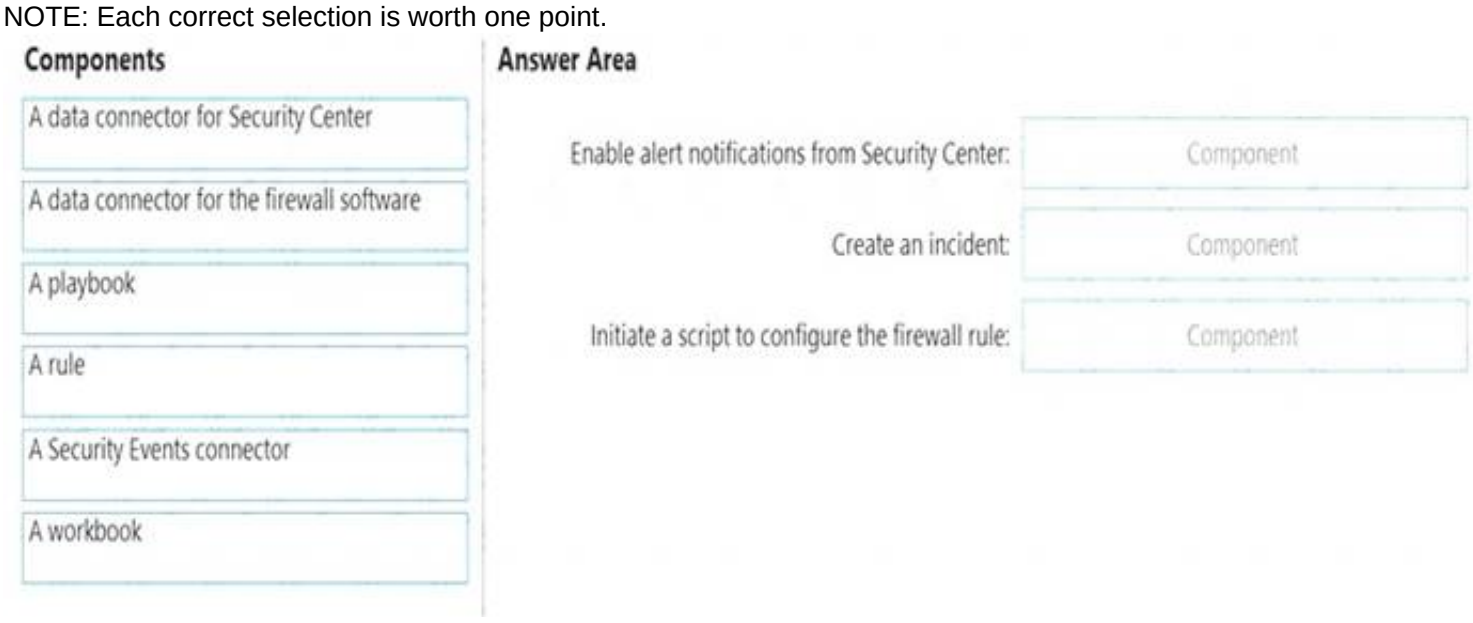


Reference:
https://docs.microsoft.com/en-us/power-bi/developer/create-an-azure-active-directory-tenant

NEW QUESTION 43
- (Exam Topic 4)
You have an Azure subscription that contains the following resources:

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

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



A. Mastered
B. Not Mastered

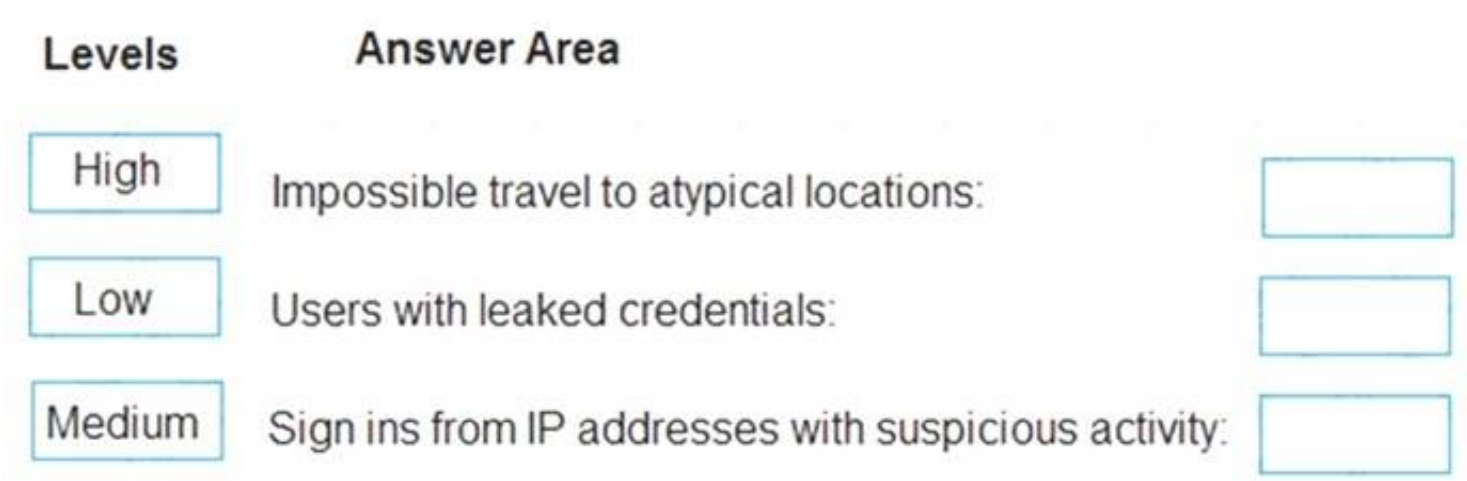
Answer: A

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

NEW QUESTION 44
- (Exam Topic 4)
You are implementing conditional access policies.
You must evaluate the existing Azure Active Directory (Azure AD) risk events and risk levels to configure and implement the policies.
You need to identify the risk level of the following risk events:

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

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

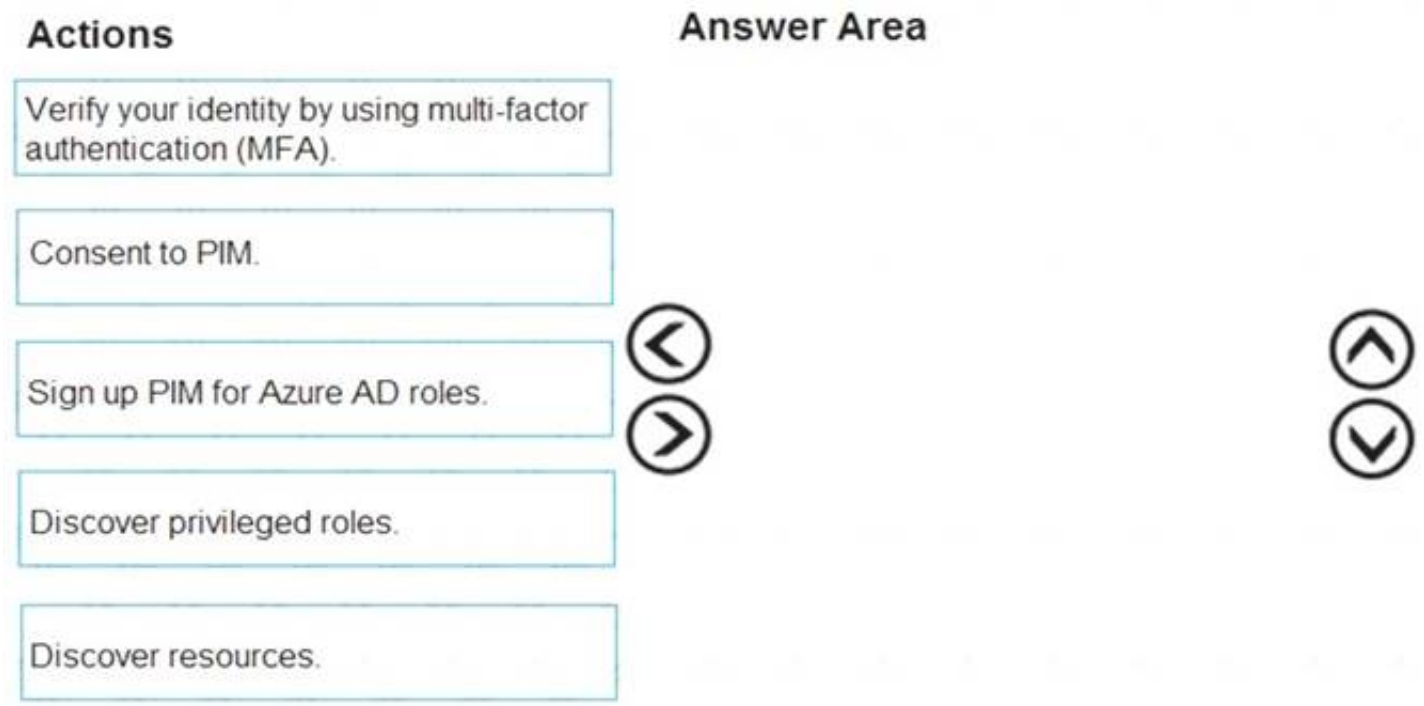


A. Mastered
B. Not Mastered

Answer: A

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

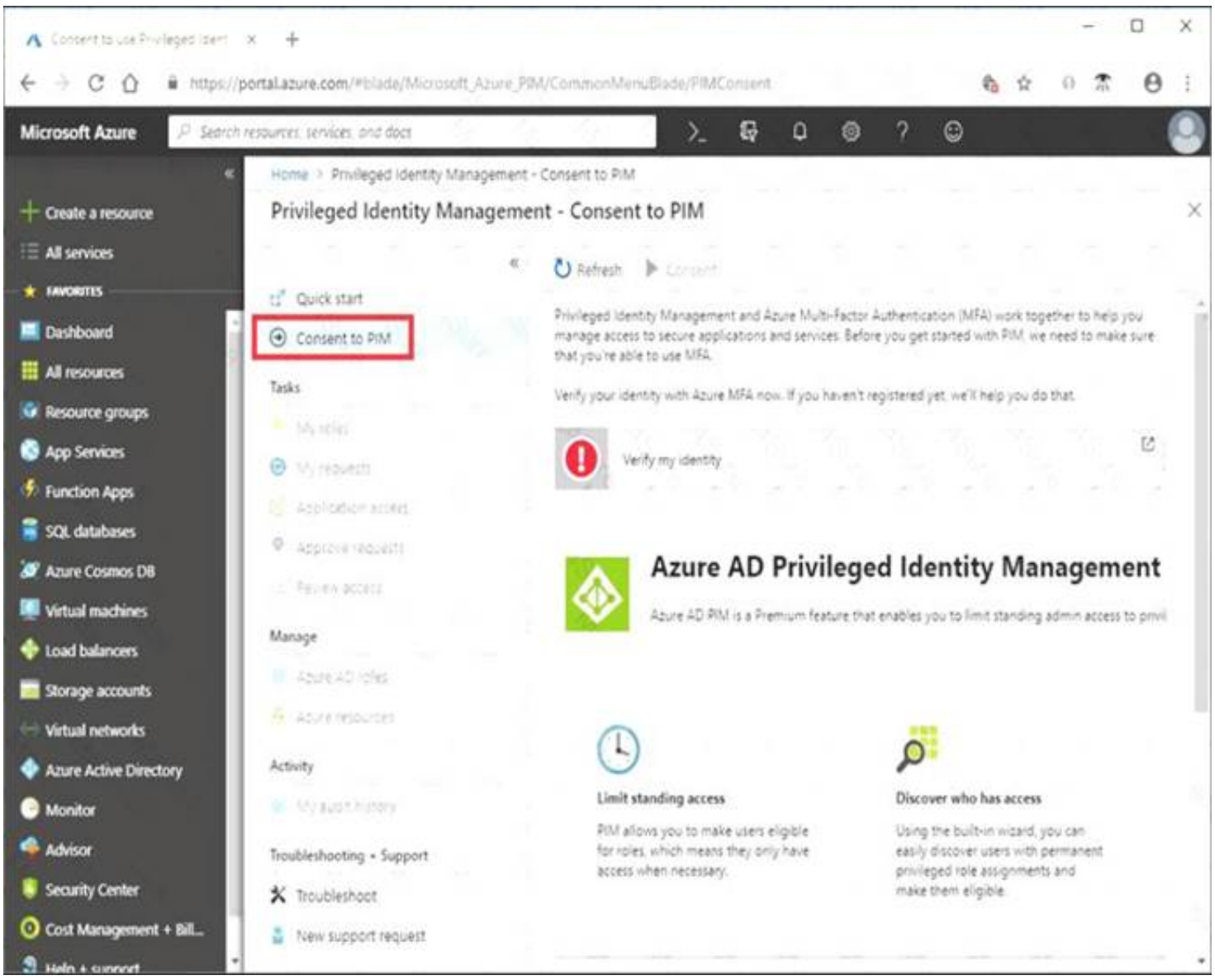
NEW QUESTION 49
- (Exam Topic 4)
You create an Azure subscription.
You need to ensure that you can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to secure Azure AD roles.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Step 1: Consent to PIM



Step: 2 Verify your identity by using multi-factor authentication (MFA)
Click Verify my identity to verify your identity with Azure MFA. You'll be asked to pick an account. Step 3: Sign up PIM for Azure AD roles
Once you have enabled PIM for your directory, you'll need to sign up PIM to manage Azure AD roles. References:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started

NEW QUESTION 51
- (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 55
- (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 57
- (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 60
- (Exam Topic 4)
You plan to use Azure Disk Encryption for several virtual machine disks.
You need to ensure that Azure Disk Encryption can retrieve secrets from the KeyVault11641655 Azure key vault.
To complete this task, sign in to the Azure portal and modify the Azure resources.

A. Mastered
B. Not Mastered

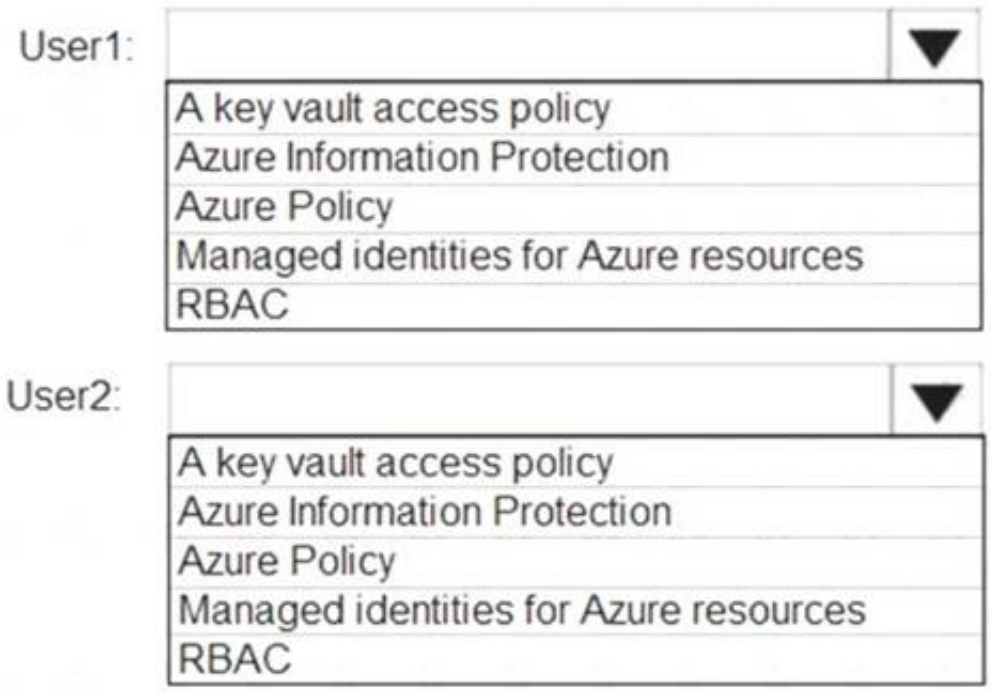
Answer: A

Explanation:
* 1. In the Azure portal, type 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.
* 2. In the Key Vault properties, scroll down to the Settings section and select Access Policies.
* 3. Select the Azure Disk Encryption for volume encryption

* 4. Click Save to save the changes.

NEW QUESTION 63
- (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 66
- (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.

```
[
    {
        "RoleAssignmentId": "3336fcbf-33d8-4c8a-85b6-d8edd964762b",
        "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa",
        "DisplayName": "User1",
        "SignInName": "User1@contoso.com",
        "RoleDefinitionName": "Owner",
        ...
    },
    {
        "RoleAssignmentId": "9d080a14-246e-4580-8b8b-077bfec22f7c",
        "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG1/providers/Microsoft.KeyVault/vaults/KeyVault1",
        "DisplayName": "User2",
        "SignInName": "User2@contoso.com",
        "RoleDefinitionName": "Key Vault Crypto Officer",
        "RoleAssignmentId": "
        "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG1/providers/Microsoft.KeyVault/vaults/KeyVault1",
        "DisplayName": "User3",
        "SignInName": "User3@contoso.com",
        "RoleDefinitionName": "Key Vault Secrets Officer",
        ...
    },
    {
        "RoleAssignmentId": "f1e46302-c5d0-4519-9ee7-128594eea97c",
        "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG3/providers/Microsoft.KeyVault/vaults/KeyVault1/keys/Key1",
        "DisplayName": "User4",
        "SignInName": "User4@contoso.com",
        "RoleDefinitionName": "Key Vault Administrator",
        ...
    }
]
```


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 69
- (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 71
- (Exam Topic 2)
You are evaluating the security of VM1, VM2, and VM3 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 the Internet, you can connect to the web server on VM1 by using HTTP.	○	○
From the Internet, you can connect to the web server on VM2 by using HTTP.	○	○
From the Internet, you can connect to the web server on VM3 by using HTTP.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
From the Internet, you can connect to the web server on VM1 by using HTTP.	○	○
From the Internet, you can connect to the web server on VM2 by using HTTP.	○	○
From the Internet, you can connect to the web server on VM3 by using HTTP.	○	○

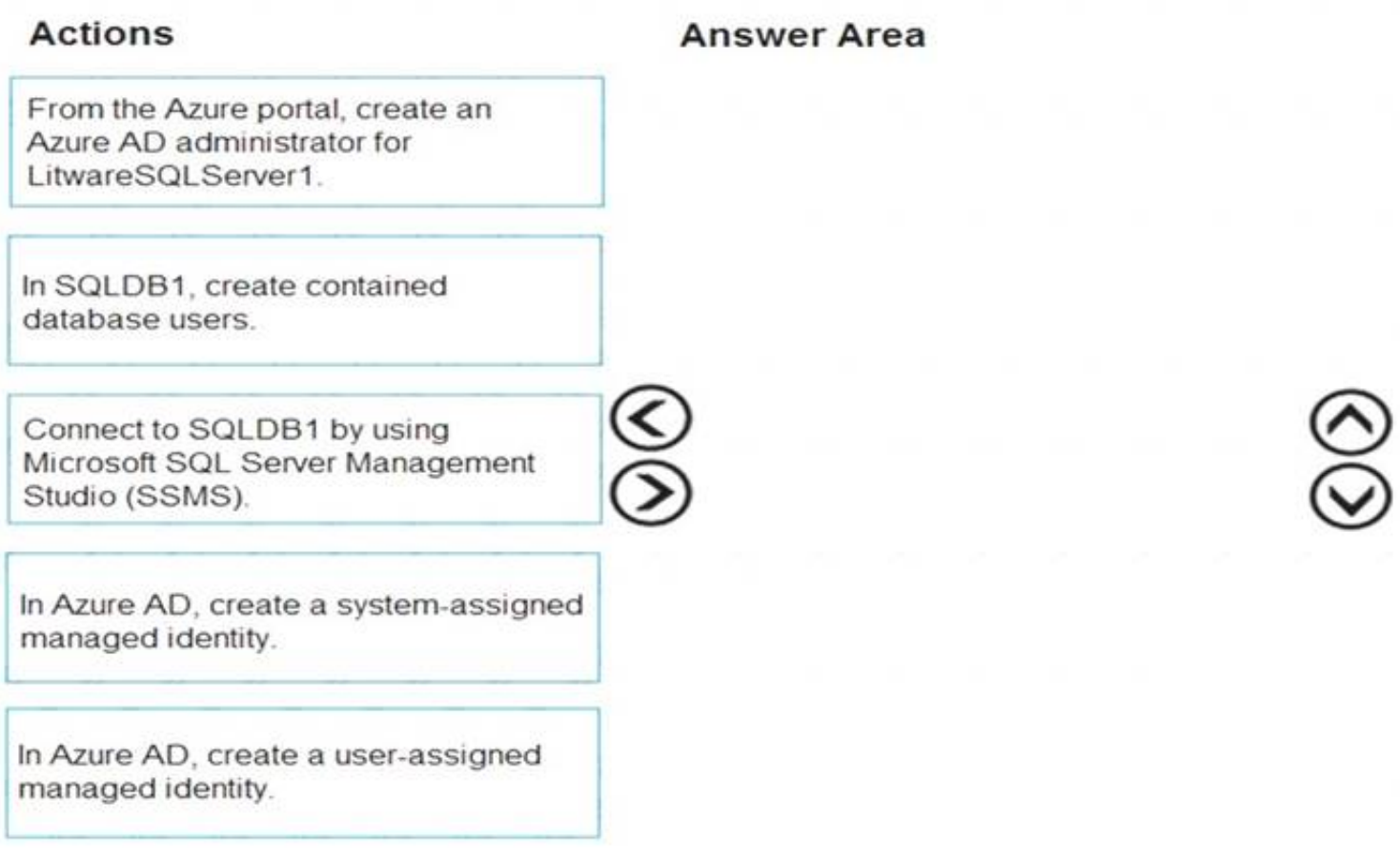
NEW QUESTION 76
- (Exam Topic 2)
You need to meet the technical requirements for VNetwork1. What should you do first?

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 77
- (Exam Topic 1)
You need to configure SQLDB1 to meet the data and application requirements.
Which three actions should you recommend be performed 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:
From the Azure portal, create an Azure AD administrator for LitwareSQLServer1 Connect to SQLDB1 by using SSMS
In SQLDB1, create contained database users https://www.youtube.com/watch?v=pEPyPsGEevw

NEW QUESTION 78
- (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 82
- (Exam Topic 1)
You need to meet the identity and access requirements for Group1. What should you do?

A. Add a membership rule to Group1.
B. Delete Group1. Create a new group named Group1 that has a membership type of Office 365. Add users and devices to the group.
C. Modify the membership rule of Group1.
D. Change the membership type of Group1 to Assigne
E. Create two groups that have dynamic membership
F. Add the new groups to Group1.

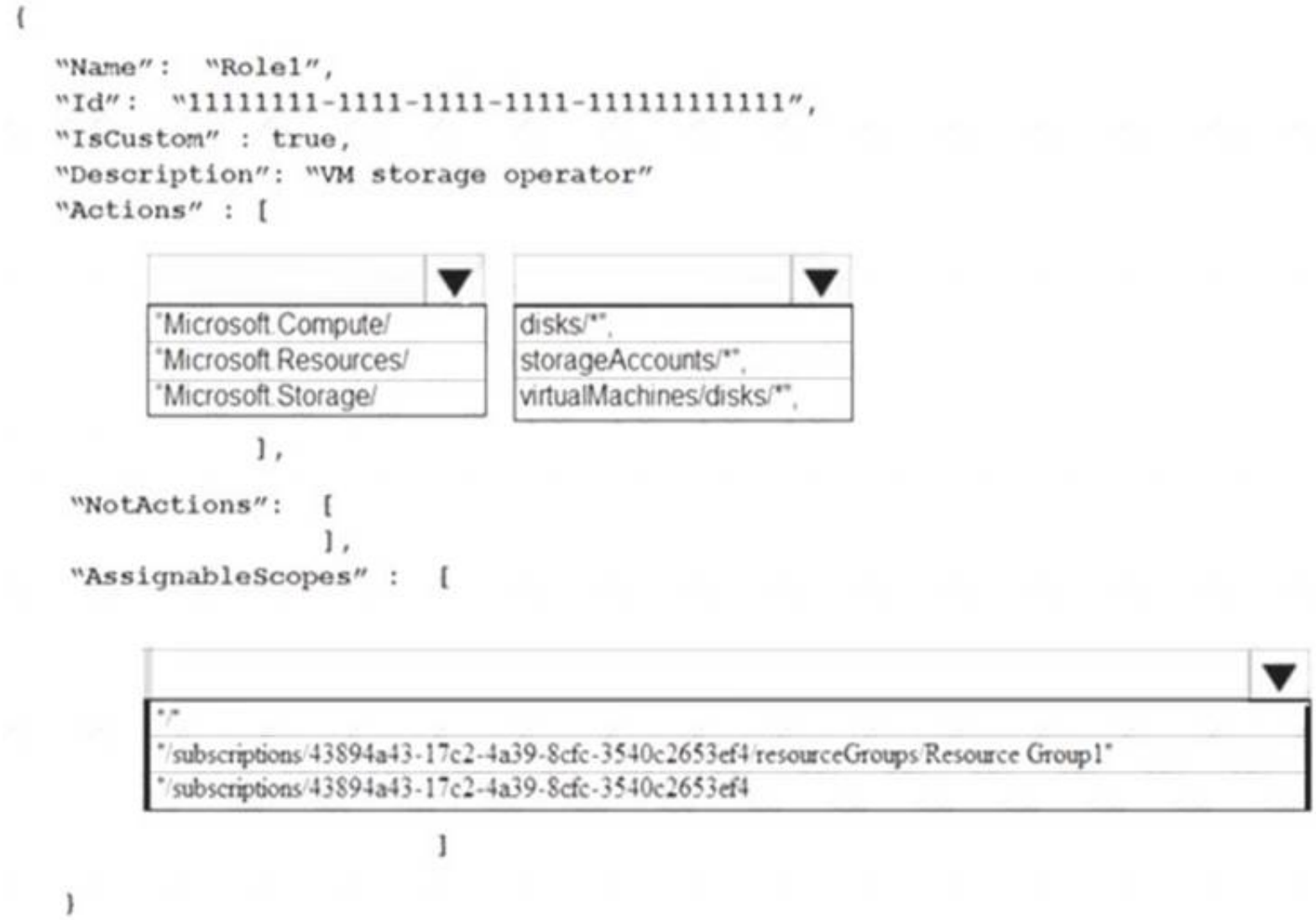
Answer: D

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership Scenario:
Litware identifies the following identity and access requirements: All San Francisco users and their devices must be members of Group1.
The tenant currently contain this group:

Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.

References:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-create-azure-porta

NEW QUESTION 86
- (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

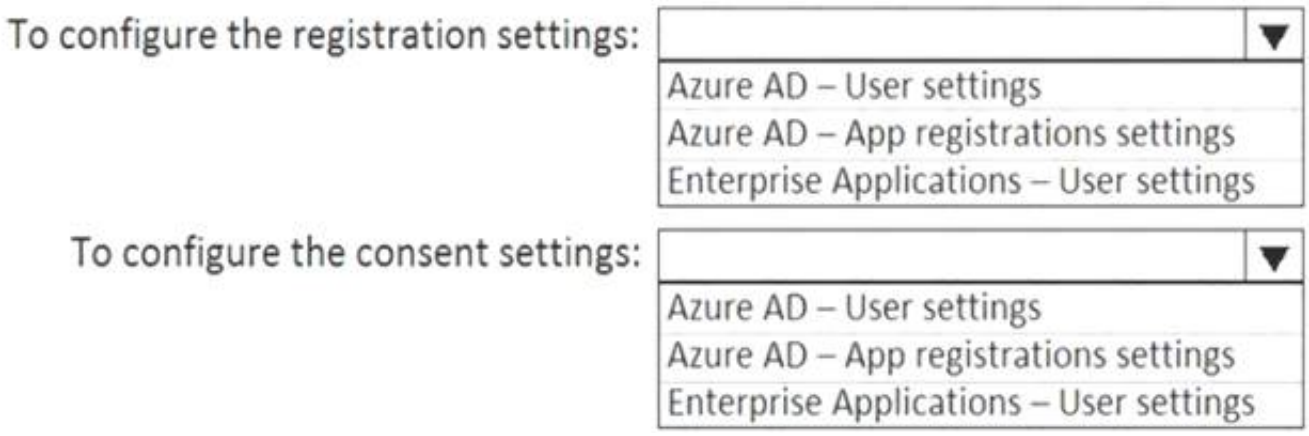
Explanation:
1) Microsoft.Compute/
2) disks
3) /subscrption/{subscriptionId}/resourceGroups/{Resource Group Id}
A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.

NEW QUESTION 89
- (Exam Topic 1)
You need to ensure that you can meet the security operations requirements. What should you do first?
A. Turn on Auto Provisioning in Security Center.
B. Integrate Security Center and Microsoft Cloud App Security.
C. Upgrade the pricing tier of Security Center to Standard.
D. Modify the Security Center workspace configuration.

Answer: C

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

NEW QUESTION 92
- (Exam Topic 1)
You need to ensure that the Azure AD application registration and consent configurations meet the identity and access requirements.
What should you use in the Azure portal? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 93
- (Exam Topic 4)
You have an Azure subscription that contains the virtual machines shown in the following table.

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

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

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

On which virtual machines is the Microsoft Monitoring agent installed?

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

Answer: D

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

NEW QUESTION 95
- (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 100
- (Exam Topic 4)
You have an Azure web app named WebApp1. You upload a certificate to WebApp1.
You need to make the certificate accessible to the app code of WebApp1.
What should you do?

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

Answer: B

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

NEW QUESTION 105
- (Exam Topic 4)
You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

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

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

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


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

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 109
- (Exam Topic 4)
You have an Azure subscription that contains an Azure SQL database named sql1. You plan to audit sql1.
You need to configure the audit log destination. The solution must meet the following requirements:
- Support querying events by using the Kusto query language.
- Minimize administrative effort. What should you configure?

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

Answer: C

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

NEW QUESTION 111
- (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 112
- (Exam Topic 4)
You have an Azure Container Registry named Registry1.
You add role assignment for Registry1 as shown in the following table.

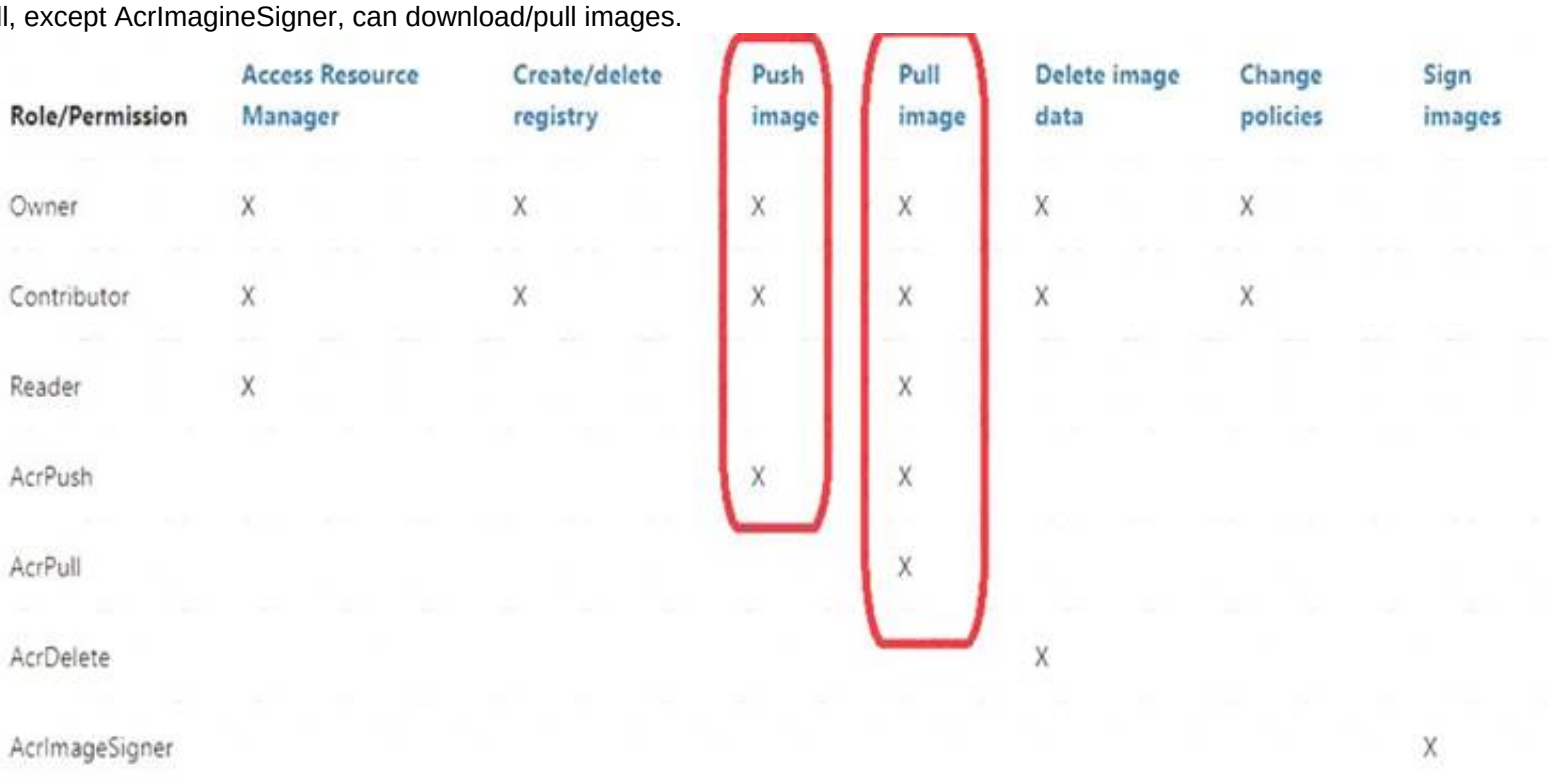
User	Role
User1	AcrPush
User2	AcrPull
User3	AcrImageSigner
User4	Contributor

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

A. Mastered
B. Not Mastered

Answer: A

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



Role/Permission	Access Resource Manager	Create/delete registry	Push image	Pull image	Delete image data	Change policies	Sign images
Owner	X	X	X	X	X	X	
Contributor	X	X	X	X	X	X	
Reader	X			X			
AcrPush			X	X			
AcrPull				X			
AcrDelete					X		
AcrImageSigner							X

References:
https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles

NEW QUESTION 115
- (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 118
- (Exam Topic 4)
You have the Azure Information Protection conditions shown in the following table.

Name	Pattern	Case sensitivity
Condition1	White	On
Condition2	Black	Off

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

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

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

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

- No label
- Label1 only
- Label2 only
- Label1 and Label2

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

- No label
- Label1 only
- Label2 only
- Label1 and Label2

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Label 2 only
How multiple conditions are evaluated when they apply to more than one label
- The labels are ordered for evaluation, according to their position that you specify in the policy: The label positioned first has the lowest position (least sensitive) and the label positioned last has the highest position (most sensitive).
- The most sensitive label is applied.
- The last sublabel is applied.

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

NEW QUESTION 119
- (Exam Topic 4)
You need to prevent administrators from performing accidental changes to the Homepage app service plan. To complete this task, sign in to the Azure portal.

A. Mastered
B. Not Mastered

Answer: A

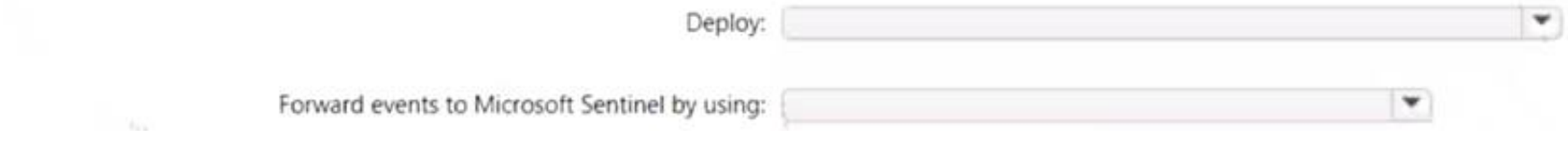
Explanation:
You need to configure a 'lock' for the app service plan. A read-only lock ensures that no one can make changes to the app service plan without first deleting the lock.
- In the Azure portal, type App Service Plans in the search box, select App Service Plans from the search results then select Homepage. Alternatively, browse to

App Service Plans in the left navigation pane.

- In the properties of the app service plan, click on Locks.
- Click the Add button to add a new lock.
- Enter a name in the Lock name field. It doesn't matter what name you provide for the exam.
- For the Lock type, select Read-only.
- Click OK to save the changes.

NEW QUESTION 122
- (Exam Topic 4)
You have a Microsoft Sentinel deployment.
You need to connect a third-party security solution to the deployment. The third-party solution will send
Common Event Format (CER-formatted messages.
What should you include in the solution? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area



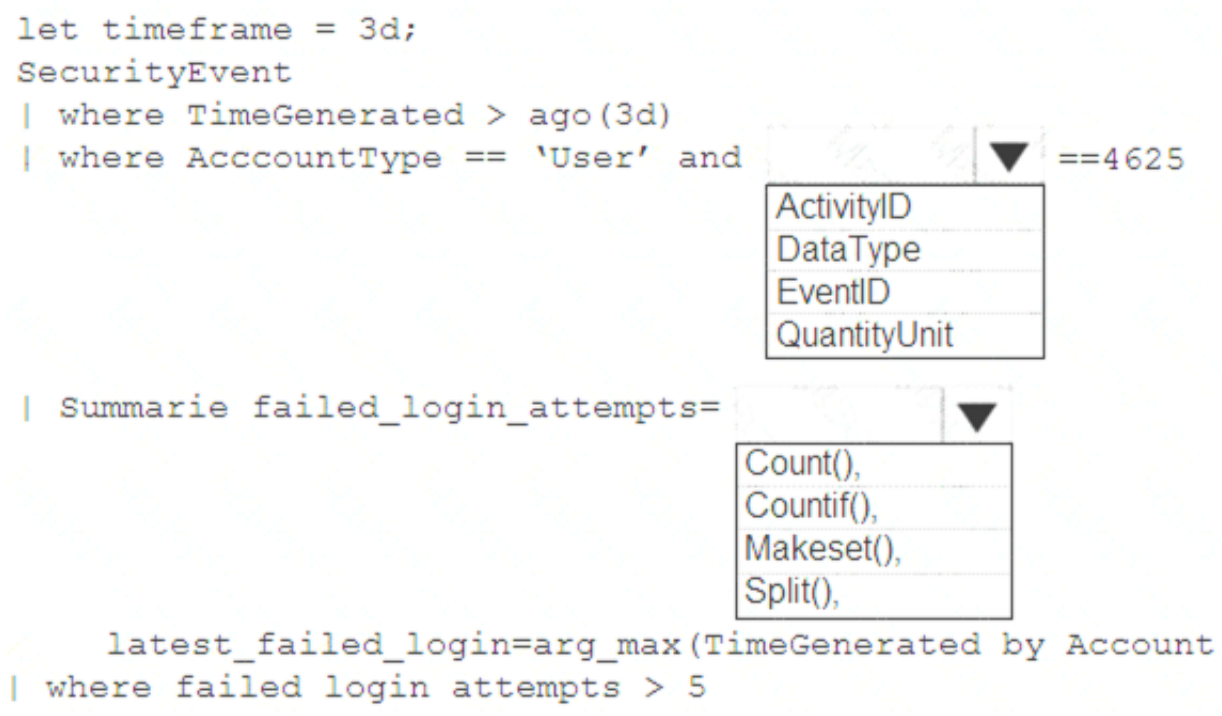
A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

NEW QUESTION 127
- (Exam Topic 4)
You suspect that users are attempting to sign in to resources to which they have no access.
You need to create an Azure Log Analytics query to identify failed user sign-in attempts from the last three days. The results must only show users who had more than five failed sign-in attempts.
How should you configure the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 128
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to rt As a result, these questions will not appear in the review screen.
You have an Azure subscription named Sub1.
You have an Azure Storage account named Sa1 in a resource group named RG1.
Users and applications access the blob service and the file service in Sal by using several shared access signatures {SASs) and stored access policies.
You discover that unauthorized users accessed both the rile service and the blob service. You need to revoke all access to Sa1.
Solution: You regenerate the access keys. Does this meet the goal?

A. Yes
B. No

Answer: A

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

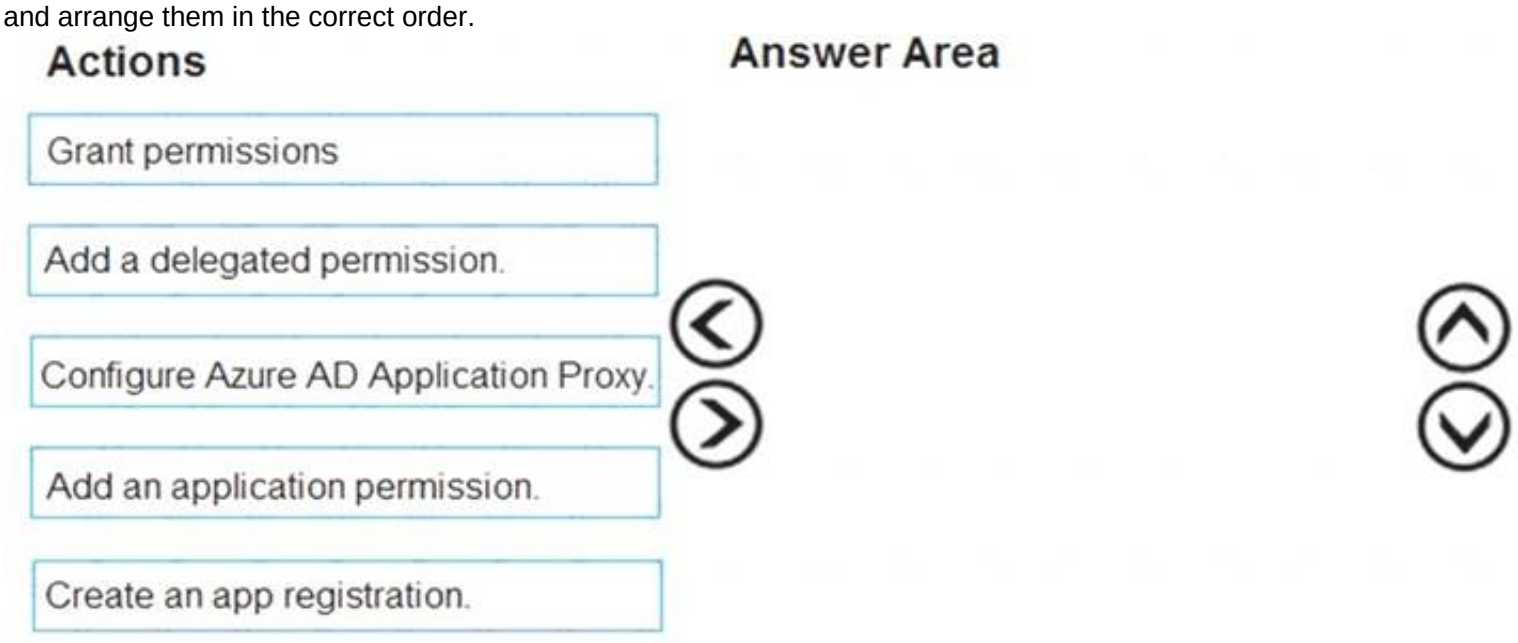
NEW QUESTION 131
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct 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 132
- (Exam Topic 4)
Your company has an Azure Active Directory (Azure AD) tenant named contoso.com.
The company is developing an application named App1. App1 will run as a service on server that runs Windows Server 2016. App1 will authenticate to contoso.com and access Microsoft Graph to read directory data.
You need to delegate the minimum required permissions to App1.
Which three actions should you perform in sequence from the Azure portal? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

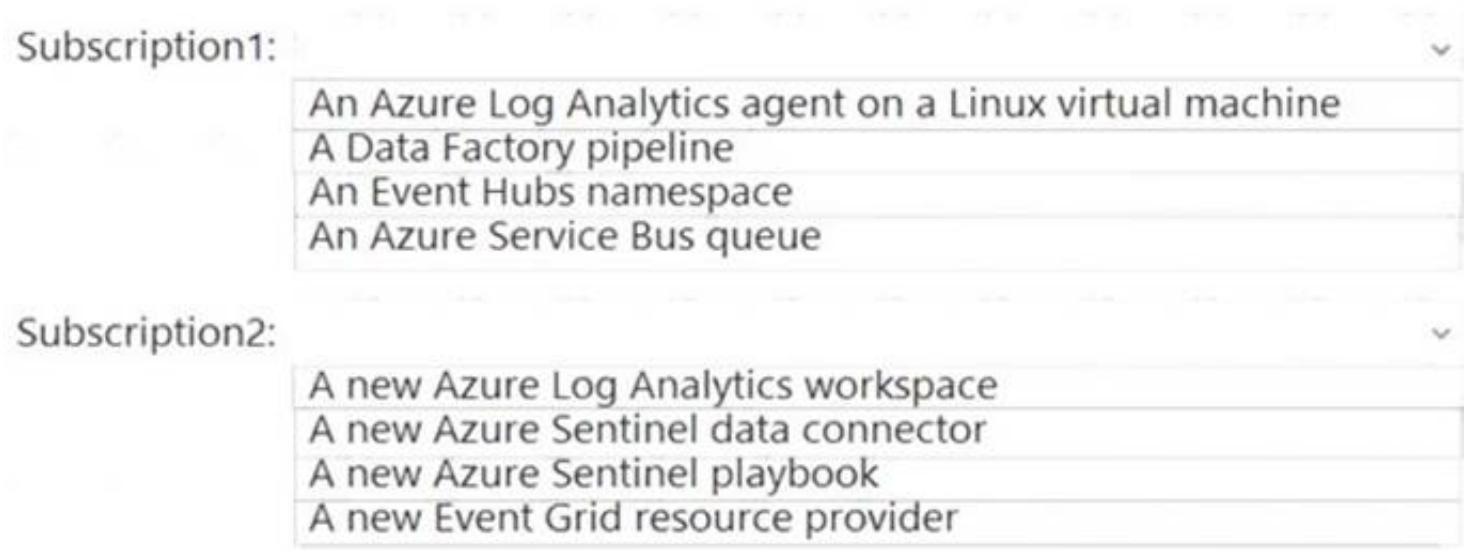
Explanation:
Step 1: Create an app registration
First the application must be created/registered.
Step 2: Add an application permission
Application permissions are used by apps that run without a signed-in user present.
Step 3: Grant permissions

NEW QUESTION 135
- (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 137
- (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/

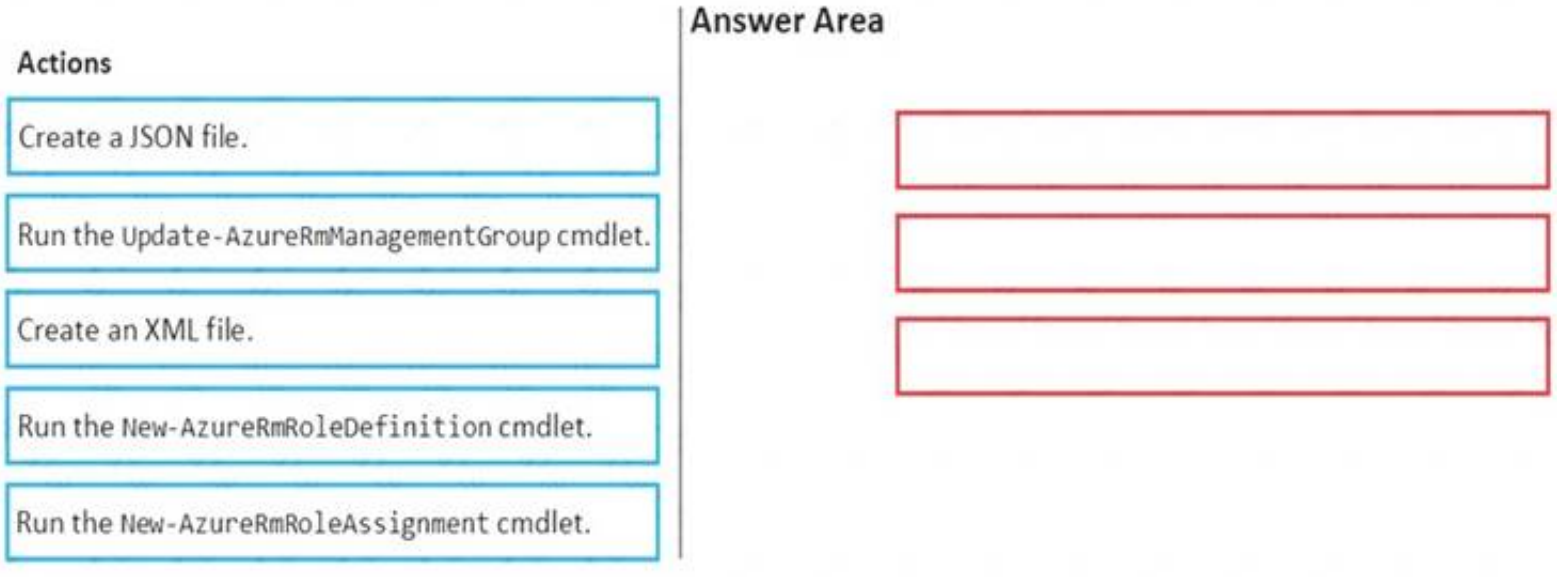
NEW QUESTION 141
- (Exam Topic 4)
Your network contains an Active Directory forest named contoso.com. The forest contains a single domain.
You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
You plan to deploy Azure AD Connect 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 144
- (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 145
- (Exam Topic 4)
You company has an Azure Active Directory (Azure AD) tenant named contoso.com. You plan to create several security alerts by using Azure Monitor.
You need to prepare the Azure subscription for the alerts. What should you create first?

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

Answer: B

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

NEW QUESTION 148
- (Exam Topic 4)
You need to ensure that the events in the NetworkSecurityGroupRuleCounter log of the

VNET01-Subnet0-NSG network security group (NSG) are stored in the logs11597200 Azure Storage account for 30 days.
To complete this task, sign in to the Azure portal.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
You need to configure the diagnostic logging for the NetworkSecurityGroupRuleCounter log.

- In the Azure portal, type Network Security Groups in the search box, select Network Security Groups from the search results then select VNET01-Subnet0-NSG. Alternatively, browse to Network Security Groups in the left navigation pane.
- In the properties of the Network Security Group, click on Diagnostic Settings.
- Click on the Add diagnostic setting link.
- Provide a name in the Diagnostic settings name field. It doesn't matter what name you provide for the exam.
- In the Log section, select NetworkSecurityGroupRuleCounter.
- In the Destination details section, select Archive to a storage account.
- In the Storage account field, select the logs11597200 storage account.
- In the Retention (days) field, enter 30.
- Click the Save button to save the changes.

NEW QUESTION 149
- (Exam Topic 4)
You have an Azure subscription named Subscription1.
You need to view which security settings are assigned to Subscription1 by default. Which Azure policy or initiative definition should you review?

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

Answer: B

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

NEW QUESTION 152
- (Exam Topic 4)
You have a web app named WebApp1.
You create a web application firewall (WAF) policy named WAF1. You need to protect WebApp1 by using WAF1.
What should you do first?

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

Answer: A

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

NEW QUESTION 156
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant named Contoso.com and an Azure Service (AKS) cluster AKS1.
You discover that AKS1 cannot be accessed by using accounts from Contoso.com
You need to ensure AKS1 can be accessed by using accounts from Contoso.com The solution must minimize administrative effort.
What should you do first?

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

Answer: A

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

NEW QUESTION 161
- (Exam Topic 4)
You have an Azure subscription named Subscription1.
You deploy a Linux virtual machine named VM1 to Subscription1. You need to monitor the metrics and the logs of VM1.
D18912E1457D5D1DDCBD40AB3BF70D5D

What should you use?

A. the AzurePerformanceDiagnostics extension
B. Azure HDInsight
C. Linux Diagnostic Extension (LAD) 3.0
D. Azure Analysis Services

Answer: A

NEW QUESTION 162
- (Exam Topic 4)
You need to create a web app named Intranet11597200 and enable users to authenticate to the web app by using Azure Active Directory (Azure AD).
To complete this task, sign in to the Azure portal.

A. Mastered
B. Not Mastered

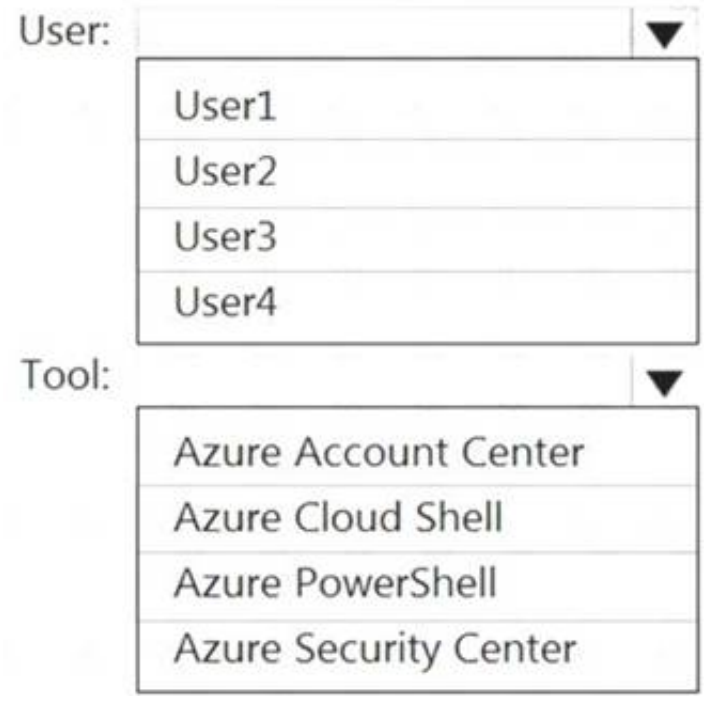
Answer: A

Explanation:
- In the Azure portal, type App services in the search box and select App services from the search results.
- Click the Create app service button to create a new app service.
- In the Resource Group section, click the Create new link to create a new resource group.
- Give the resource group a name such as Intranet11597200RG and click OK.
- In the Instance Details section, enter Intranet11597200 in the Name field.
- In the Runtime stack field, select any runtime stack such as .NET Core 3.1.
- Click the Review + create button.
- Click the Create button to create the web app.
- Click the Go to resource button to open the properties of the new web app.
- In the Settings section, click on Authentication / Authorization.
- Click the App Service Authentication slider to set it to On.
- Click Save to save the changes.

NEW QUESTION 166
- (Exam Topic 4)
Your company has an Azure subscription named Subscription1. Subscription1 is associated with the Azure Active Directory tenant that includes the users shown in the following table.

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

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



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 167
- (Exam Topic 4)
You have an Azure subscription that contains an Azure SQL database named SQL1 and an Azure key vault named KeyVault1. KeyVault1 stores the keys shown in the following table.

Name	Type	RSA key size	Elliptic curve name
Key1	RSA	2048	Not applicable
Key2	RSA	3072	Not applicable
Key3	RSA	4096	Not applicable
Key4	EC	Not applicable	P-512

You reed to configure Transparent Data Encryption (TDE). TDE will use a customer-managed key for SQL1?

A. Key1. Key2 Key3. and Key4
B. Key1 only
C. Key2 only
D. Key1 and key2 only
E. Key2 and Key3 only

Answer: E

NEW QUESTION 171
- (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	Enabled
User2	Group1	Disabled
User3	Group1	Disabled

You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings:
- Assignments: Include Group1, exclude Group2
- Conditions: Sign-in risk level: Medium and above
- Access Allow access, Require multi-factor authentication

You need to identify what occurs when the users sign in to Azure AD.
What should you identify for each user? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

When User1 signs in from an anonymous IP address, the user will:
- Be blocked
- Be prompted for MFA
- Sign in by using a username and password only

When User2 signs in from an unfamiliar location, the user will:
- Be blocked
- Be prompted for MFA
- Sign in by using a username and password only

When User3 signs in from an infected device, the user will:
- Be blocked
- Be prompted for MFA
- Sign in by using a username and password only

A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/ https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks
53 - (Exam Topic 4)
You have an Azure subscription that contains two virtual machines named VM1 and VM2 that run Windows Server 2019.
You are implementing Update Management in Azure Automation. You plan to create a new update deployment named Update1.
You need to ensure that Update! meets the following requirements:
• Automatically applies updates to VM1 and VM2.
• Automatically adds any new Windows Server 2019 virtual machines to Update1. What should you include in Update1?
A. a security group that has a Membership type of Dynamic Device
B. a security group that has a Membership type of Assigned

C. a Kusto query language query
D. a dynamic group query
Answer: D

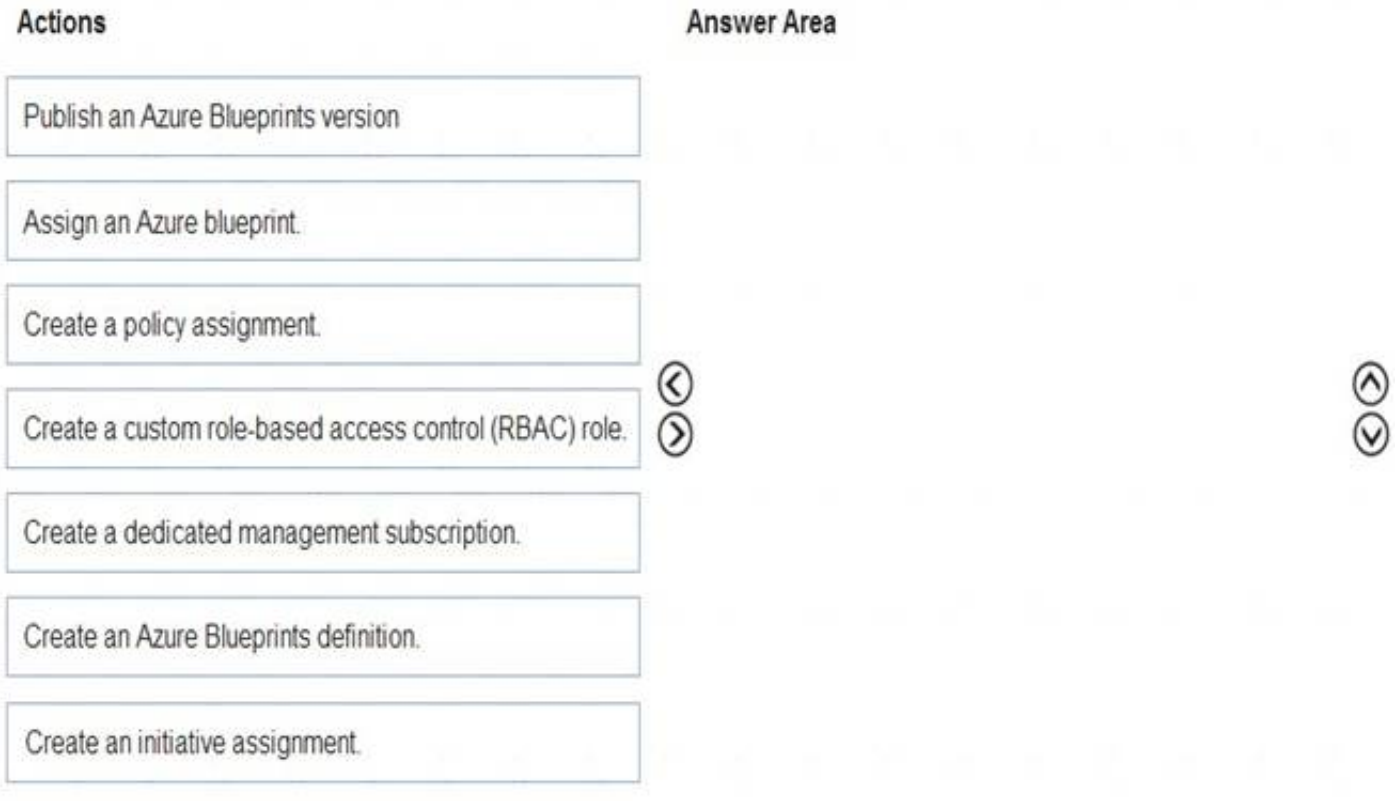
NEW QUESTION 174
- (Exam Topic 4)
Your network contains an on-premises Active Directory domain named corp.contoso.com.
You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
You sync all on-premises identities to Azure AD.
You need to prevent users who have a givenName attribute that starts with TEST from being synced to Azure AD. The solution must minimize administrative effort.
What should you use?

A. Synchronization Rules Editor
B. Web Service Configuration Tool
C. the Azure AD Connect wizard
D. Active Directory Users and Computers

Answer: A

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

NEW QUESTION 176
- (Exam Topic 4)
You have five Azure subscriptions linked to a single Azure Active Directory (Azure AD) tenant. You create an Azure Policy initiative named SecurityPolicyInitiative1.
You identify which standard role assignments must be configured on all new resource groups.
You need to enforce SecurityPolicyInitiative1 and the role assignments when a new resource group is created. Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 180
- (Exam Topic 4)
You have an Azure subscription named Sub1 that contains the resources shown in the following table.

Name	Type	Region	Resource group
Sa1	Azure Storage account	East US	RG1
VM1	Azure virtual machine	East US	RG2
KV1	Azure key vault	East US 2	RG1
SQL1	Azure SQL database	East US 2	RG2

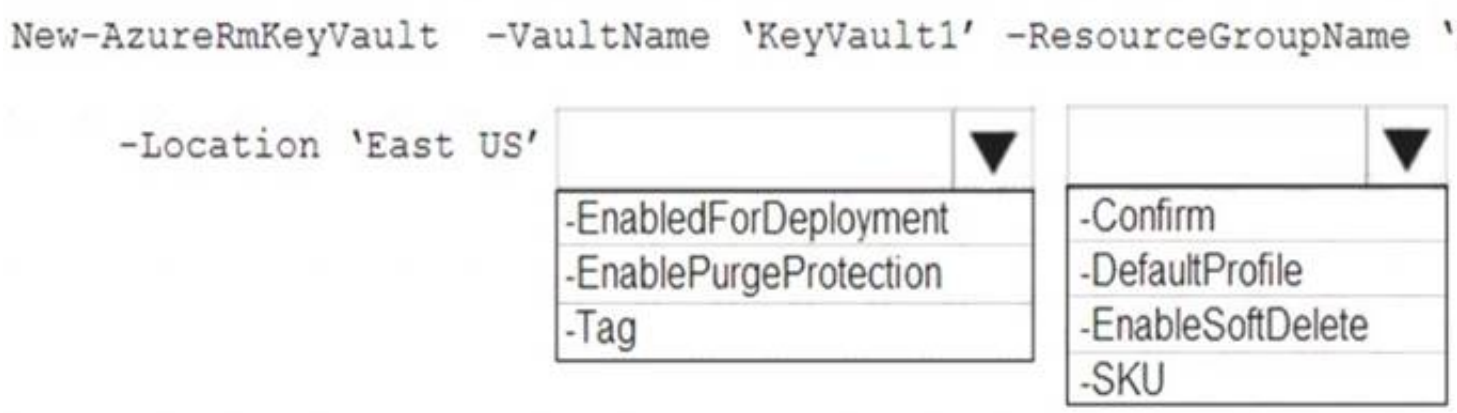
You need to ensure that you can provide VM1 with secure access to a database on SQL1 by using a contained database user.
What should you do?

A. Enable a managed service identity on VM1.
B. Create a secret in KV1.
C. Configure a service endpoint on SQL1.
D. Create a key in KV1.

Answer: A

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm

NEW QUESTION 185
- (Exam Topic 4)
You need to create an Azure key vault. The solution must ensure that any object deleted from the key vault be retained for 90 days.
How should you complete the command? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 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 an Azure Subscription. The subscription contains 50 virtual machines that run Windows Server 2012 R2 or Windows Server 2016.
You need to deploy Microsoft Antimalware to the virtual machines. Solution: You add an extension to each virtual machine.
Does this meet the goal?

A. Yes
B. No

Answer: A

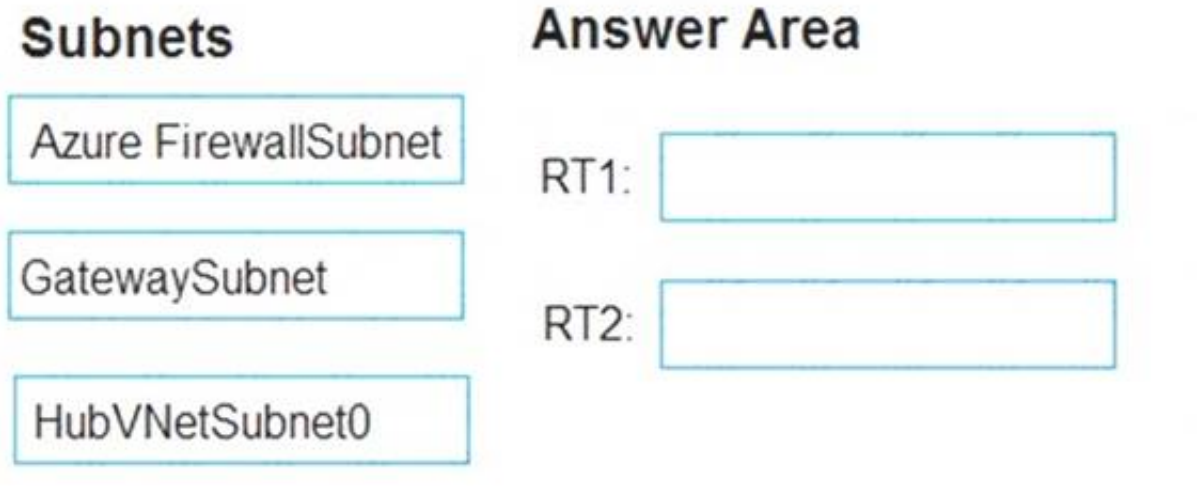
Explanation:
You can use Visual Studio to enable and configure the Microsoft Antimalware service. This entails selecting Microsoft Antimalware extension from the dropdown list under Installed Extensions and click Add to configure with default antimalware configuration.
References:
https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware

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

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

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

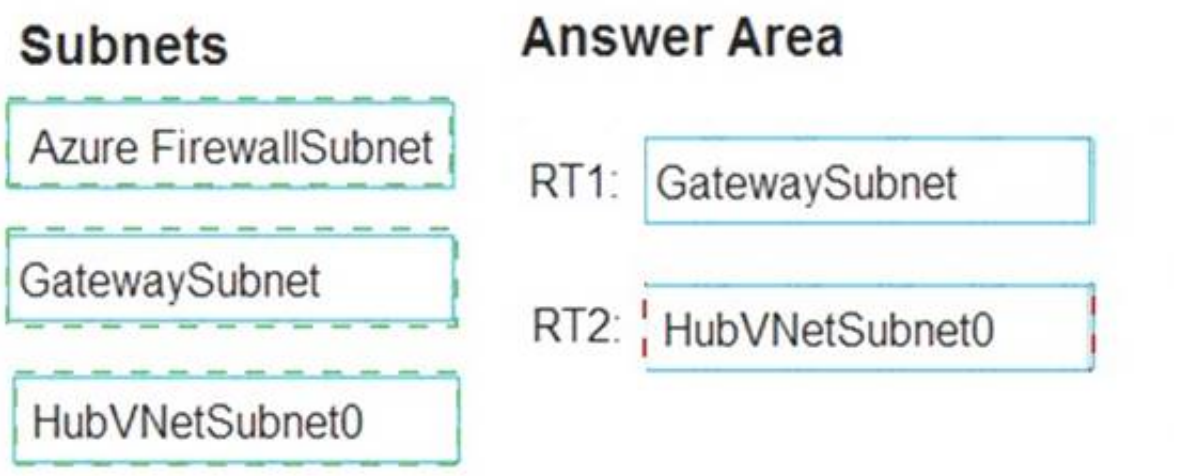
You need to ensure that traffic between SpokeVNetSubnet0 and the on-premises network flows through the Azure firewall.
To which subnet should you associate each route table? To answer, drag the appropriate subnets to the correct route tables. Each subnet may be used once, more than once, or not at all.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



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 198
- (Exam Topic 4)
You have an Azure Active directory tenant that syncs with an Active Directory Domain Services (AD DS) domain.
You plan to create an Azure file share that will contain folders and files.
Which identity store can you use to assign permissions to the Azure file share and folders within the share? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 200
- (Exam Topic 4)

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

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

Answer: D

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

NEW QUESTION 205
- (Exam Topic 4)
You have a management group named Group1 that contains an Azure subscription named sub1. Sub1 has a subscription ID of 11111111-1234-1234-1234-1111111111.
You need to create a custom Azure role-based access control (RBAC) role that will delegate permissions to manage the tags on all the objects in Group1.
What should you include in 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:
Text, application Description automatically generated
Note: Assigning a custom RBAC role as the Management Group level is currently in preview only. So, for now the answer to the assignable scope is the subscription level.
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal#step-5-assignable-scopes

NEW QUESTION 208
.....

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