# Exam Questions az-500

Microsoft Azure Security Technologies

**https://www.2passeasy.com/dumps/az-500/**

**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 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 have an Azure subscription that contains 100 virtual machines and has Azure Security Cent,-. Standard tier enabled.
You plan to perform a vulnerability scan of each virtual machine.
You need to deploy the vulnerability scanner extension to the virtual machines by using an Azure Resource Manager template.
Which two values should you specify in the code to automate the deployment of the extension to the virtual machines? Each correct answer presents part of the solution.

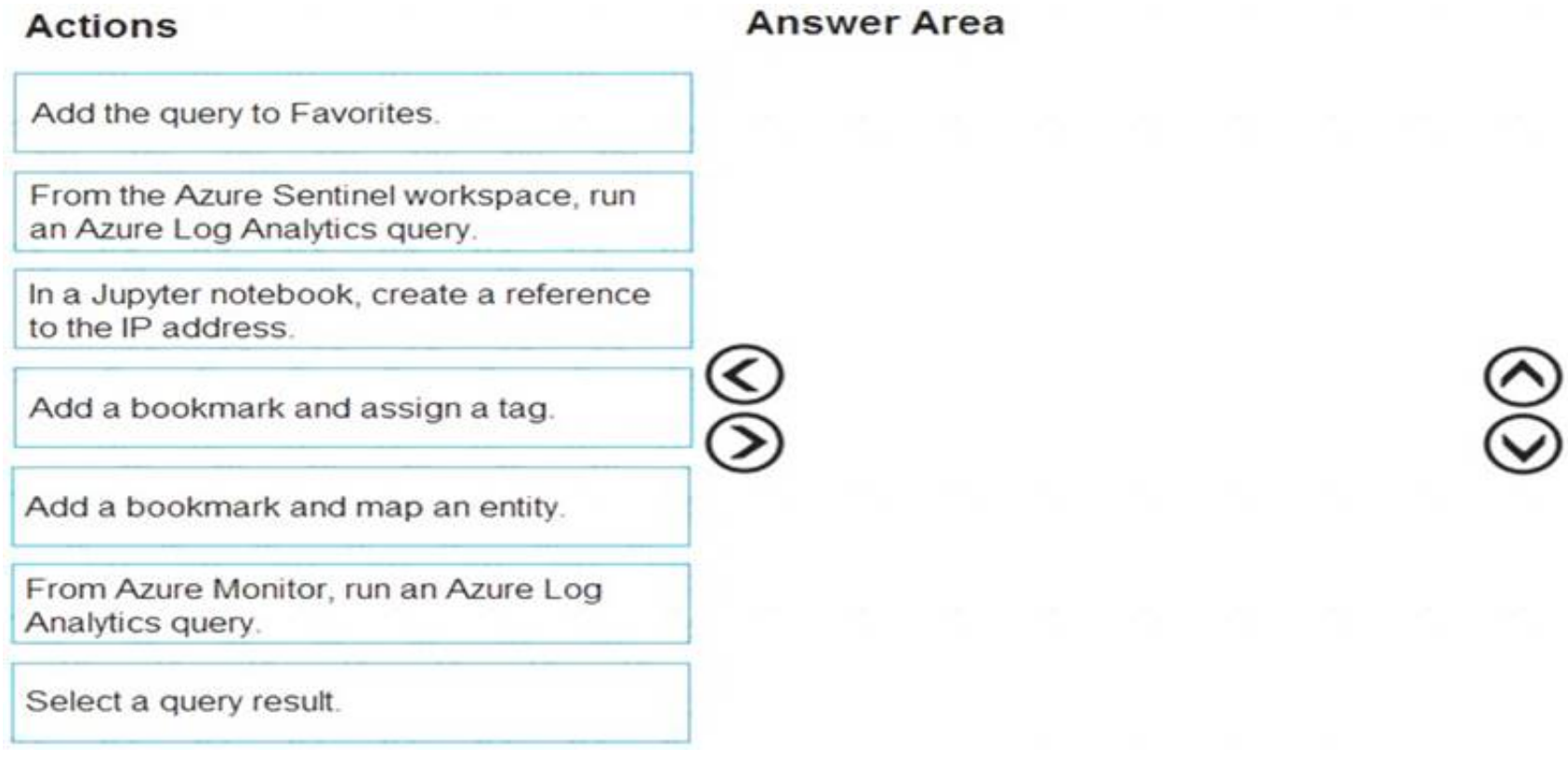
NOTE: Each correct selection is worth one point.

A. the user assigned managed identity
B. the Key Vault managed storage account Key
C. the Azure Active Directory (Azure AD) ID
D. the system-assigned managed identity
E. the primary shared key
F. the workspace ID

**Answer:** AC

**Explanation:**
https://docs.microsoft.com/en-us/azure/azure-arc/servers/onboard-service-principal

**NEW QUESTION 5**
- (Exam Topic 4)
You have an Azure Sentinel workspace that has an Azure Active Directory (Azure AD) data connector. You are threat hunting suspicious traffic from a specific IP address.
You need to annotate an intermediate event stored in the workspace and be able to reference the IP address when navigating through the investigation graph.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.




A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 6**
- (Exam Topic 4)
Your company uses Azure DevOps.
You need to recommend a method to validate whether the code meets the company's quality standards and code review standards.
What should you recommend implementing in Azure DevOps?

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

**Answer:** C

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

**NEW QUESTION 7**
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.

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

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

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

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

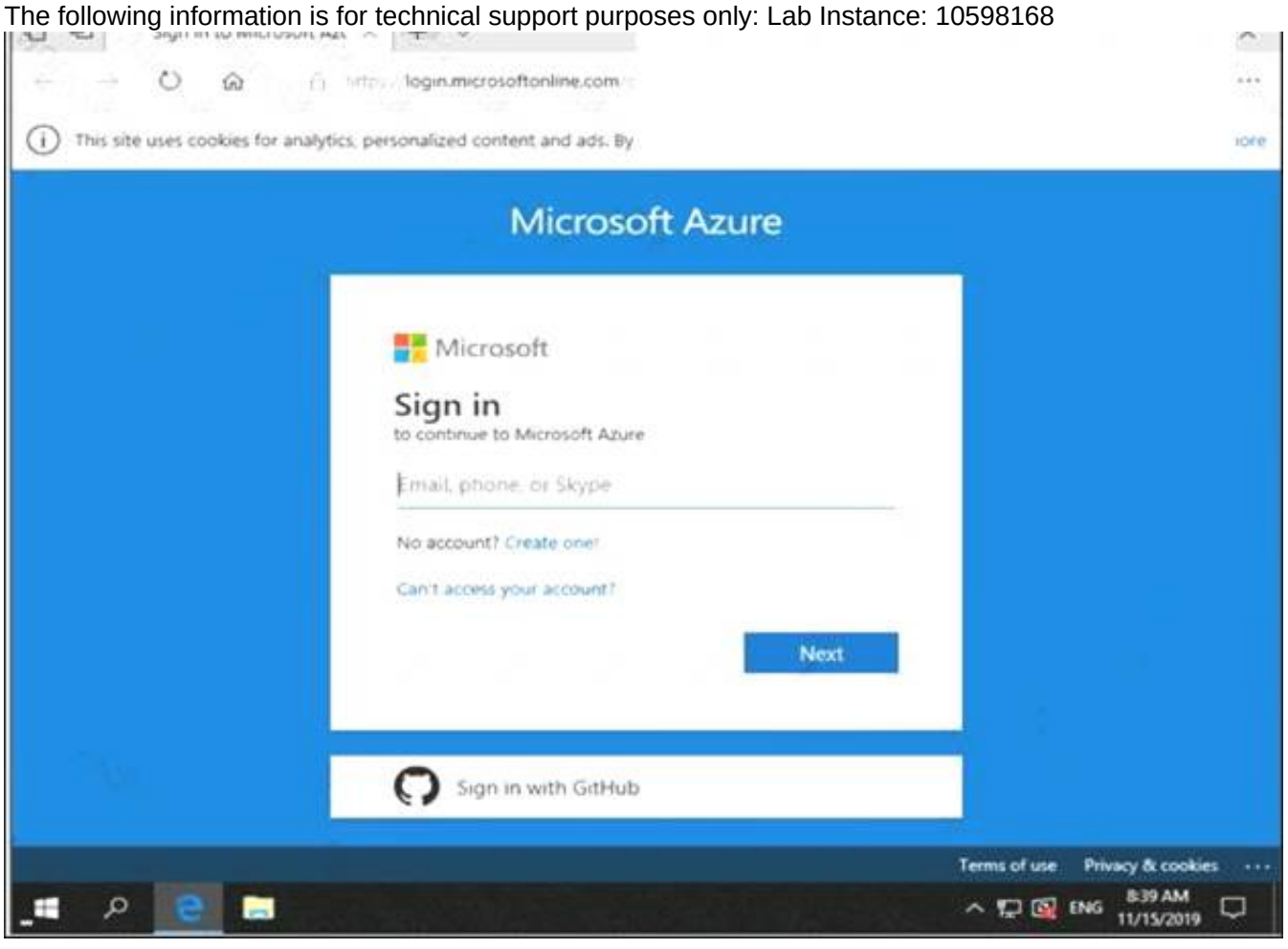
| Statements | Yes | No |
|---|---|---|
| SQL1 will have TDE enabled automatically. | ○ | ○ |
| The deployment of SQL2 will fail. | ○ | ○ |
| SQL3 will be deployed and marked as noncompliant. | ○ | ○ |

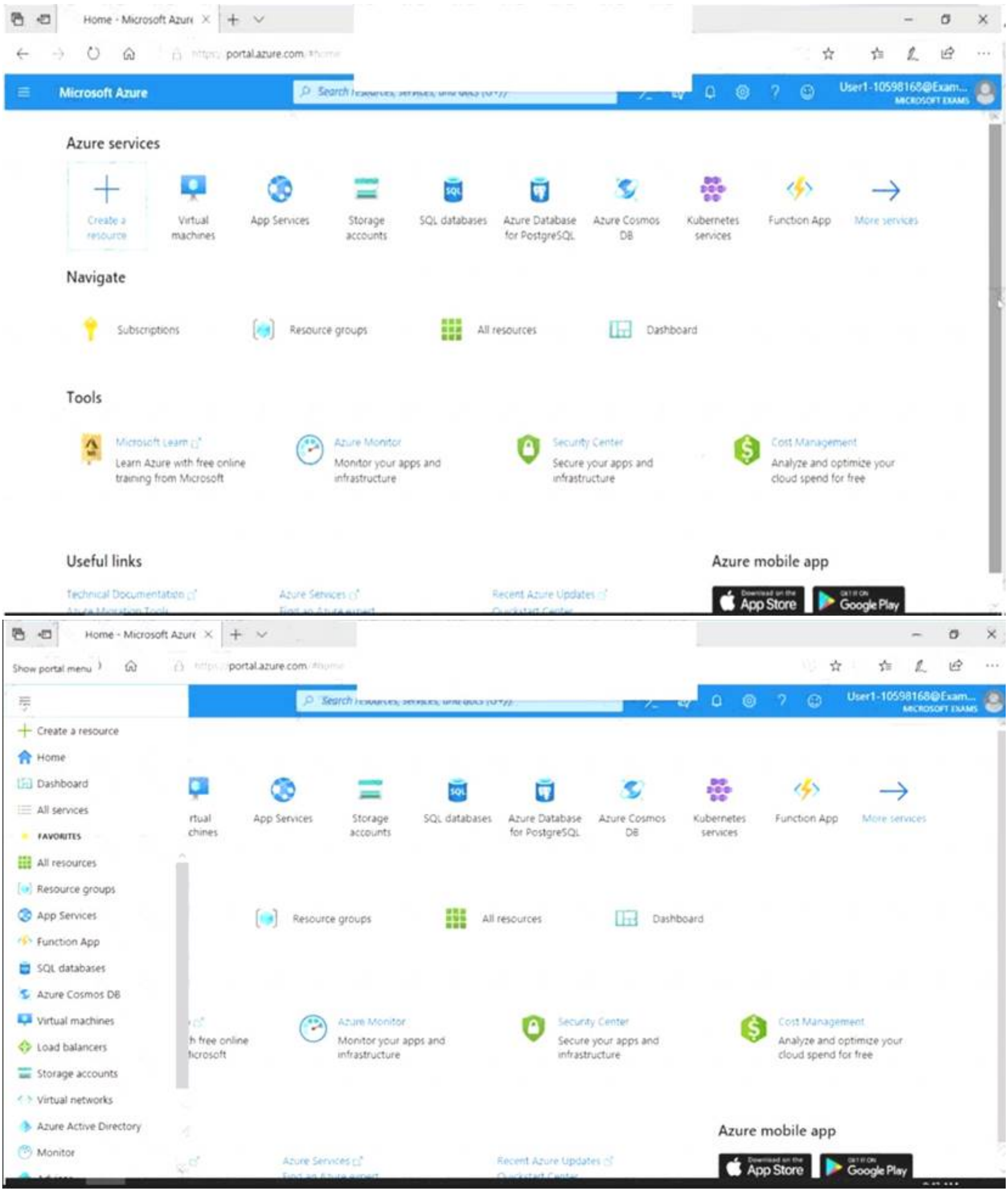
A. Mastered
B. Not Mastered

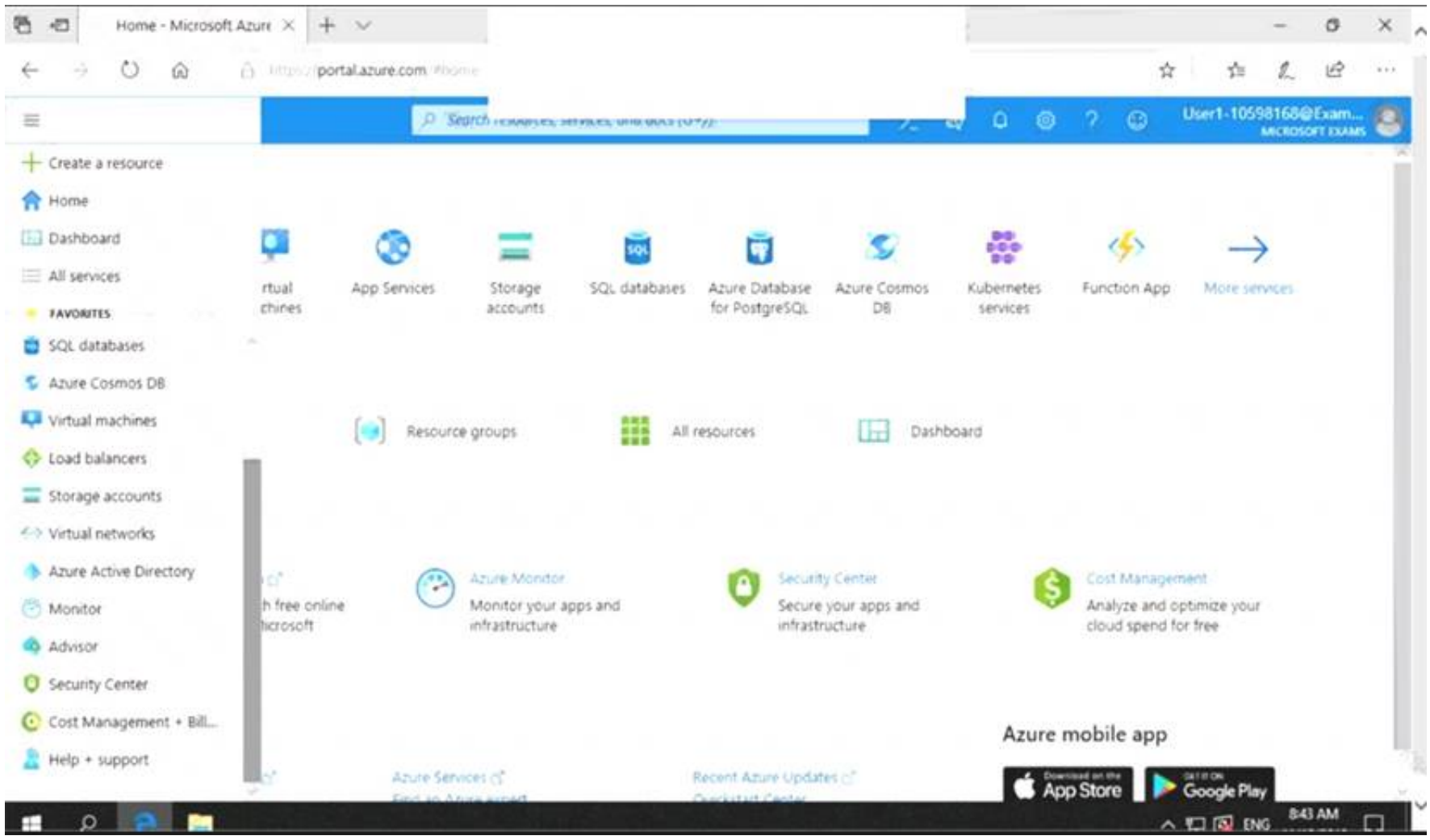
**Answer:** A

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

**NEW QUESTION 8**
- (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 add the network interface of a virtual machine named VM1 to an application security group named ASG1.
To complete this task, sign in to the Azure portal.

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

- In the Search resources, services, and docs box at the top of the portal, begin typing the name of a virtual machine, VM1 that has a network interface that you want to add to, or remove from, an application security group.
- When the name of your VM appears in the search results, select it.
- Under SETTINGS, select Networking. Select Configure the application security groups, select the application security groups that you want to add the network interface to, or unselect the application security groups that you want to remove the network interface from, and then select Save.

Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface

**NEW QUESTION 9**
- (Exam Topic 4)
You have the Azure virtual networks shown in the following table.

| Name | Location | Subnet | Peered network |
|---|---|---|---|
| VNET1 | East US | Subnet1 | VNET2 |
| VNET2 | West US | Subnet2, Subnet3 | VNET1 |
| VNET4 | East US | Subnet4 | *None* |

You have the Azure virtual machines shown in the following table.

| Name | Application security group | Network security group (NSG) | Connected to | Public IP address |
|---|---|---|---|---|
| VM1 | ASG1 | NSG1 | Subnet1 | No |
| VM2 | ASG2 | NSG1 | Subnet2 | No |
| VM3 | ASG2 | NSG1 | Subnet3 | Yes |
| VM4 | ASG4 | NSG1 | Subnet4 | Yes |

The firewalls on all the virtual machines allow ping traffic. NSG1 is configured as shown in the following exhibit. Inbound security rules

| Priority | Name | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|---|
| 110 | Allow_RDP | 3389 | Any | Any | Any | Allow ... |
| 130 | Rule1 | Any | Any | ASG1 | Any | Allow ... |
| 140 | Rule2 | Any | Any | ASG2 | Any | Allow ... |
| 150 | Rule3 | Any | Any | ASG4 | Any | Allow ... |
| 160 | Rule4 | Any | Any | Any | Any | Deny ... |
| 65000 | AllowVnetInBound | Any | Any | VirtualNetwork | VirtualNetwork | Allow ... |
| 65001 | AllowAzureLoadBalan... | Any | Any | AzureLoadBalancer | Any | Allow ... |
| 65500 | DenyAllInBound | Any | Any | Any | Any | Deny ... |

Outbound security rules

| Priority | Name | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|---|
| 65000 | AllowVnetOutBound | Any | Any | VirtualNetwork | VirtualNetwork | Allow ... |
| 65001 | AllowInternetOutBou... | Any | Any | Any | Internet | Allow ... |
| 65500 | DenyAllOutBound | 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 |
|---|---|---|
| VM1 can ping VM3 successfully. | ○ | ○ |
| VM2 can ping VM4 successfully. | ○ | ○ |
| VM3 can be accessed by using Remote Desktop from the internet. | ○ | ○ |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Box 1: Yes
VM1 and VM3 are on peered VNets. The firewall rules with a source of ASG1 and ASG2 allow 'any' traffic on 'any' protocol so pings are allowed between VM1 and VM3.
Box 2: No
VM2 and VM4 are on separate VNets and the VNets are not peered. Therefore, the pings would have to go over the Internet. VM4 does have a public IP and the firewall allows pings. However, for VM2 to be able to ping VM4, VM2 would also need a public IP address. In Azure, pings don't go out through the default gateway as they would in a physical network. For an Azure VM to ping external IPs, the VM must have a public IP address assigned to it.
Box 3: Yes
VM3 has a public IP address and the firewall allows traffic on port 3389.

**NEW QUESTION 10**
- (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

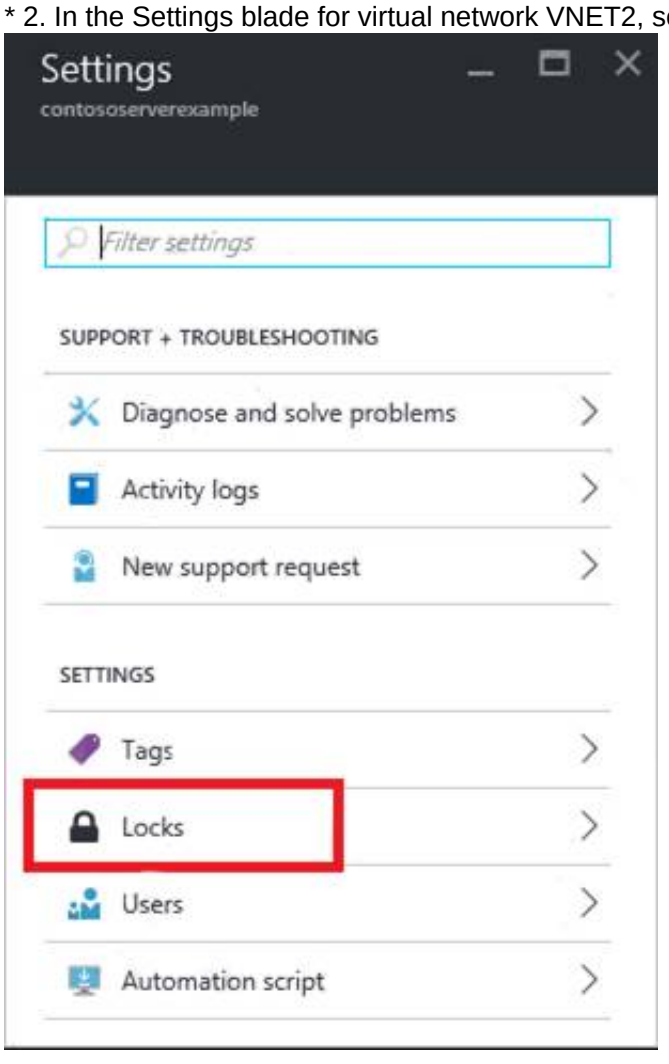
**NEW QUESTION 10**
- (Exam Topic 4)
You need to configure a virtual network named VNET2 to meet the following requirements:
- Administrators must be prevented from deleting VNET2 accidentally.
- Administrators must be able to add subnets to VNET2 regularly.

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

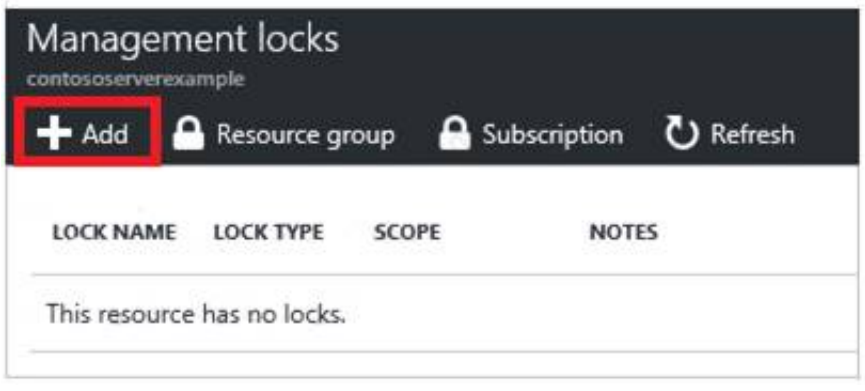
A. Mastered
B. Not Mastered

**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 15**
- (Exam Topic 4)
Your company has two offices in Seattle and New York. Each office connects to the Internet by using a NAT device. The offices use the IP addresses shown in the following table.

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

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

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

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


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

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

A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 19**
- (Exam Topic 4)
You have three on-premises servers named Server1, Server2, and Server3 that run Windows Server1 and Server2 and located on the Internal network. Server3 is located on the premises network. All servers have
access to Azure.
From Azure Sentinel, you install a Windows firewall data connector.
You need to collect Microsoft Defender Firewall data from the servers for Azure Sentinel. What should you do?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 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 25**
- (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 30**
- (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 31**
- (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

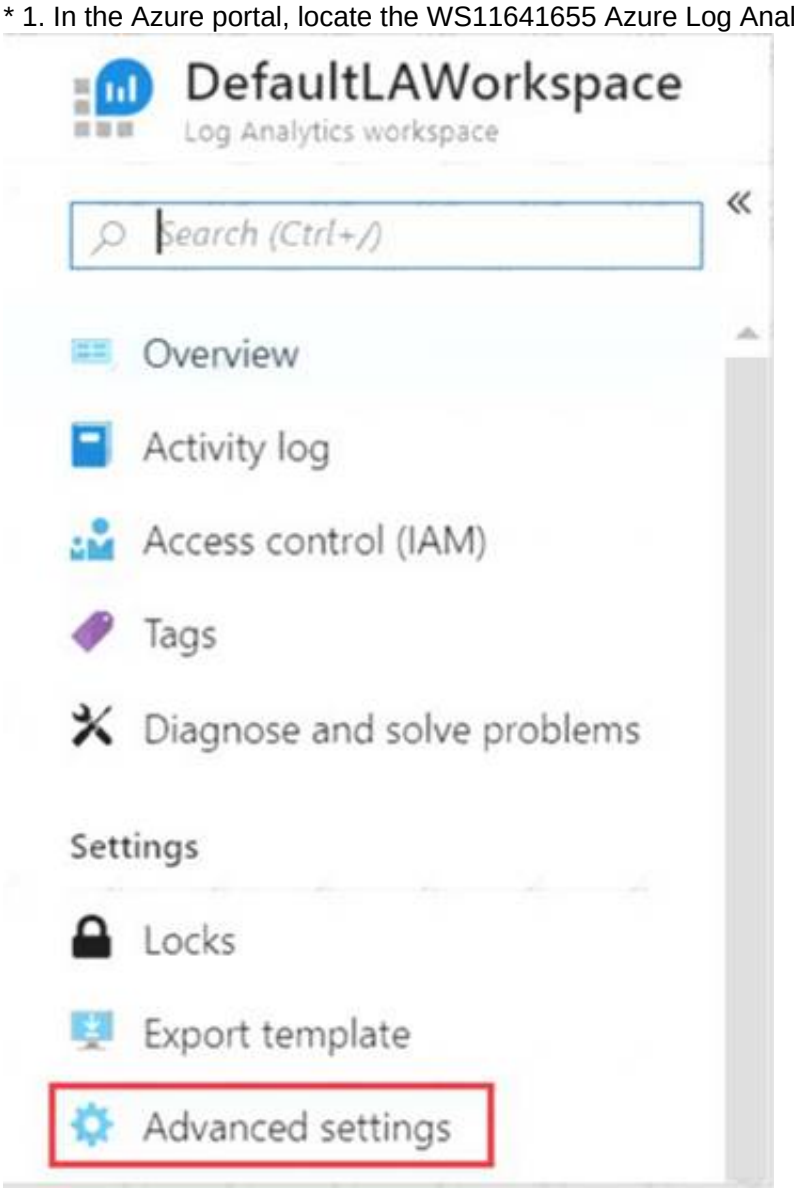
**Explanation:**
Just-in-time (JIT) virtual machine (VM) access can be used to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.
Note: When just-in-time is enabled, Security Center locks down inbound traffic to your Azure 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)
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 39**
- (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.

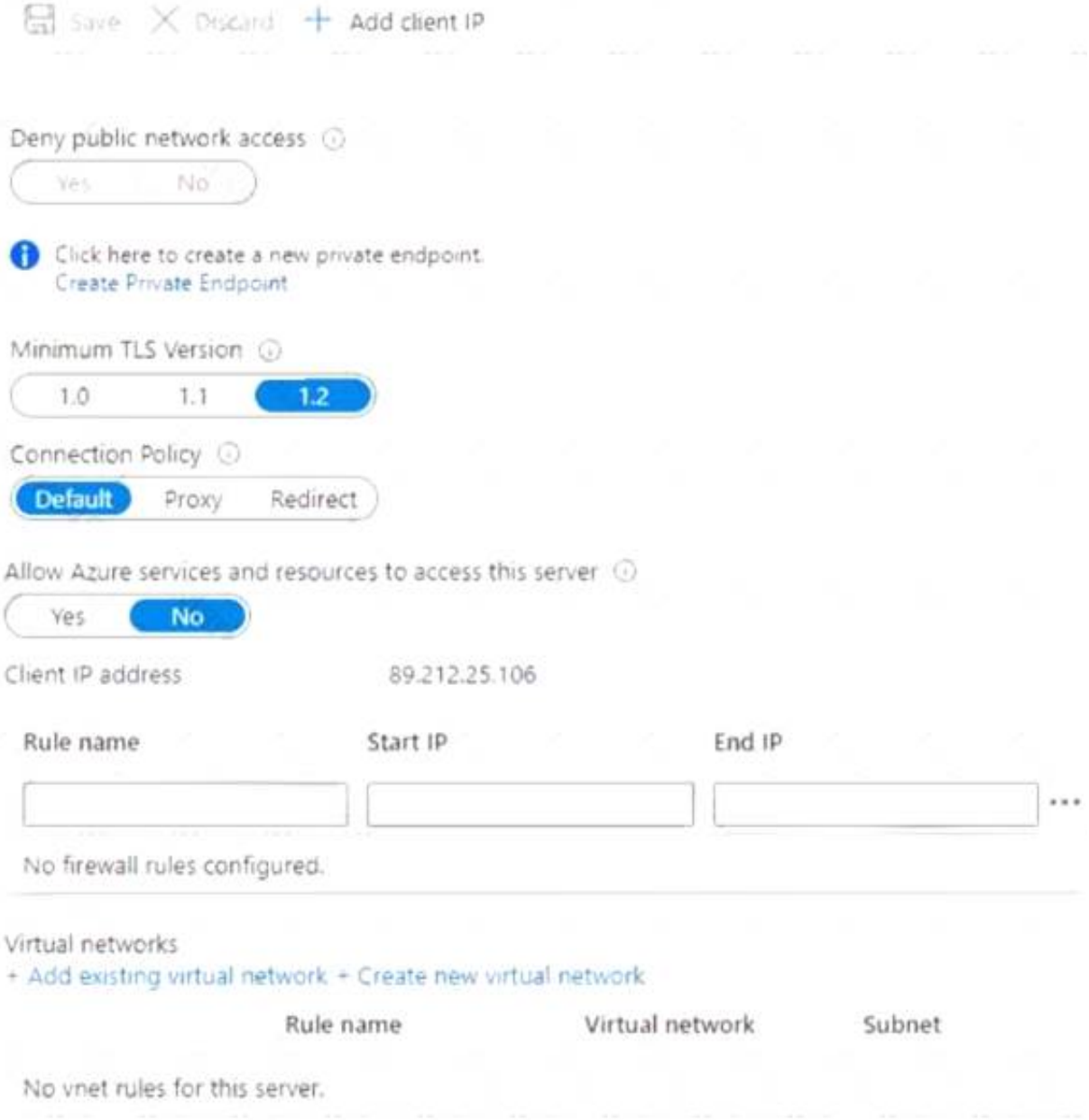
| Name | Location | Performance | Premium account type |
|---|---|---|---|
| storage1 | East US | Standard | *Not applicable* |
| storage2 | East US | Premium | Block blobs |
| storage3 | East US | Premium | File shares |
| storage4 | East US 2 | Standard | *Not applicable* |

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 40**
- (Exam Topic 4)
You have an Azure subscription that contains an Azure SQL Database logic server named SQL! and an Azure virtual machine named VM1. VM1 uses a private IP address only.
The Firewall and virtual networks settings for SQL1 are shown in the following exhibit.




You need to ensure that VM1 can connect to SQL1. The solution must use the principle of least privilege. What should you do?

A. Add an existing virtual network.
B. Set Connection Policy to Proxy.
C. Create a new firewall rule.
D. Set Allow Azure services and resources to access this server to Yes.

**Answer:** C

**NEW QUESTION 41**
- (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 43**
- (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

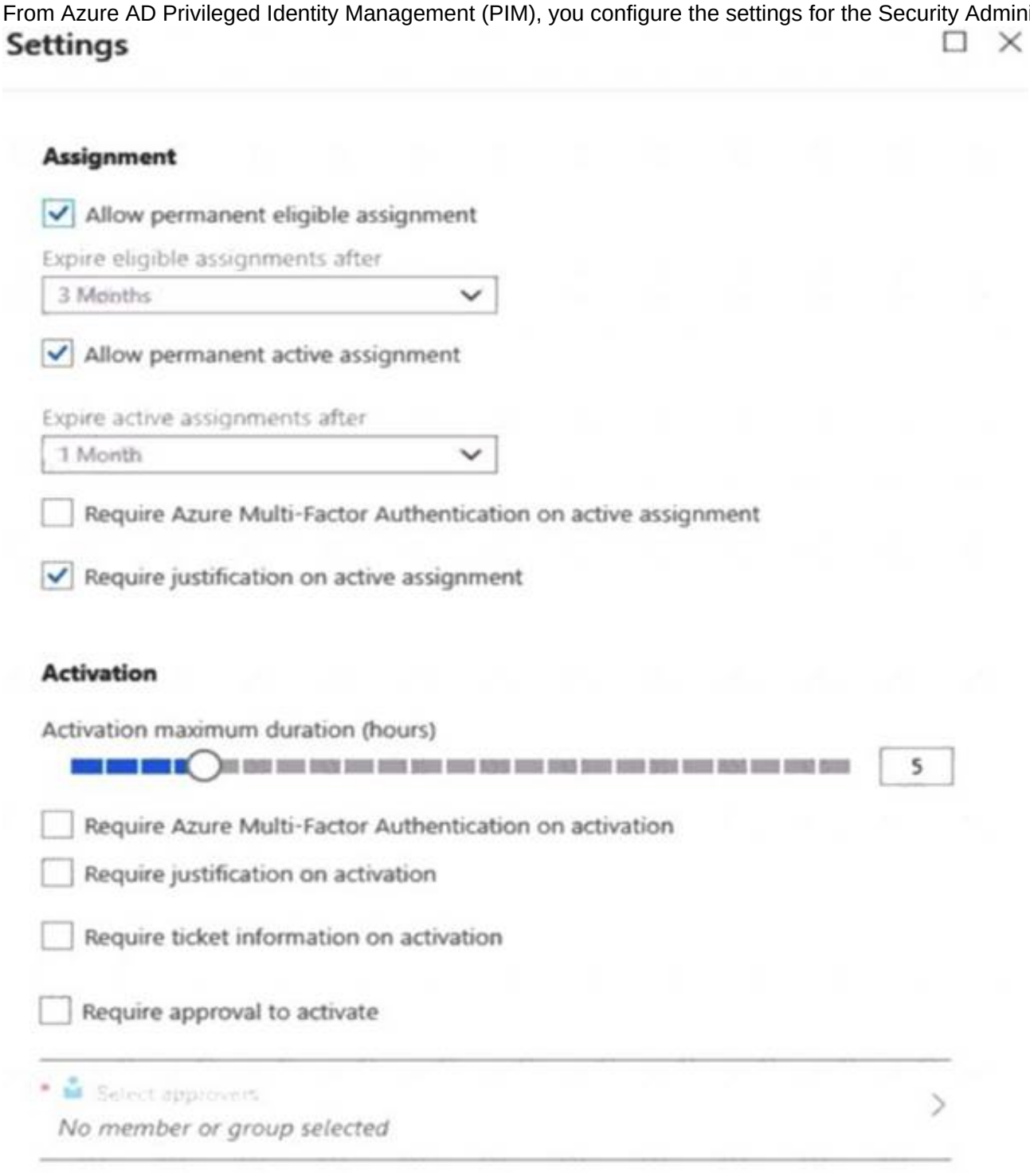
**Answer:** B

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

| Name | Member of |
|---|---|
| User1 | Group1 |
| User2 | Group2 |
| User3 | Group1, Group2 |

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




From PIM, you assign the Security Administrator role to the following groups:
- Group1: Active assignment type, permanently assigned
- Group2: Eligible assignment type, permanently eligible

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

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

A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 50**
- (Exam Topic 4)
You have 20 Azure subscriptions and a security group named Group1. The subscriptions are children of the root management group.
Each subscription contains a resource group named RG1.
You need to ensure that for each subscription RG1 meets the following requirements:
- The members of Group1 are assigned the Owner role.
- The modification of permissions to RG1 is prevented.

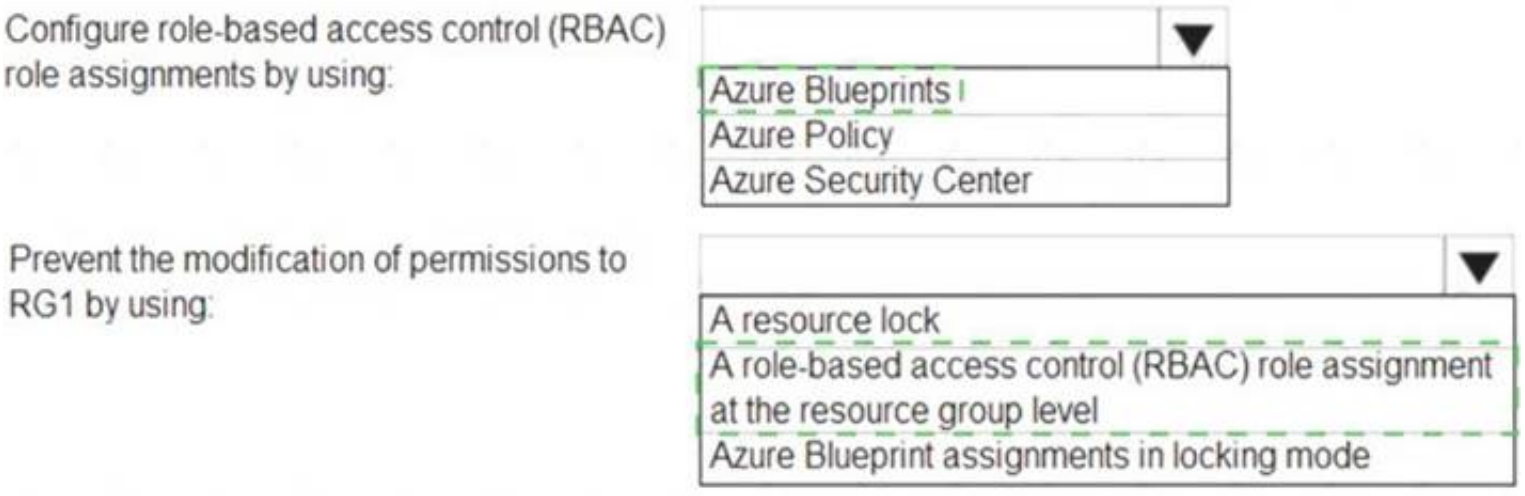
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

| | |
|---|---|
| Configure role-based access control (RBAC) role assignments by using: | Azure Blueprints<br>Azure Policy<br>Azure Security Center |
| Prevent the modification of permissions to RG1 by using: | A resource lock<br>A role-based access control (RBAC) role assignment at the resource group level<br>Azure Blueprint assignments in locking mode |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**




**NEW QUESTION 53**
- (Exam Topic 4)
You have an Azure subscription named Sub1.
In Azure Security Center, you have a workflow automation named WF1. WF1 is configured to send an email message to a user named User1.
You need to modify WF1 to send email messages to a distribution group named Alerts. What should you use to modify WF1?

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

**Answer:** C

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

**NEW QUESTION 58**
- (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 59**
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

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

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

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

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

A. Mastered
B. Not Mastered

**Answer:** A

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

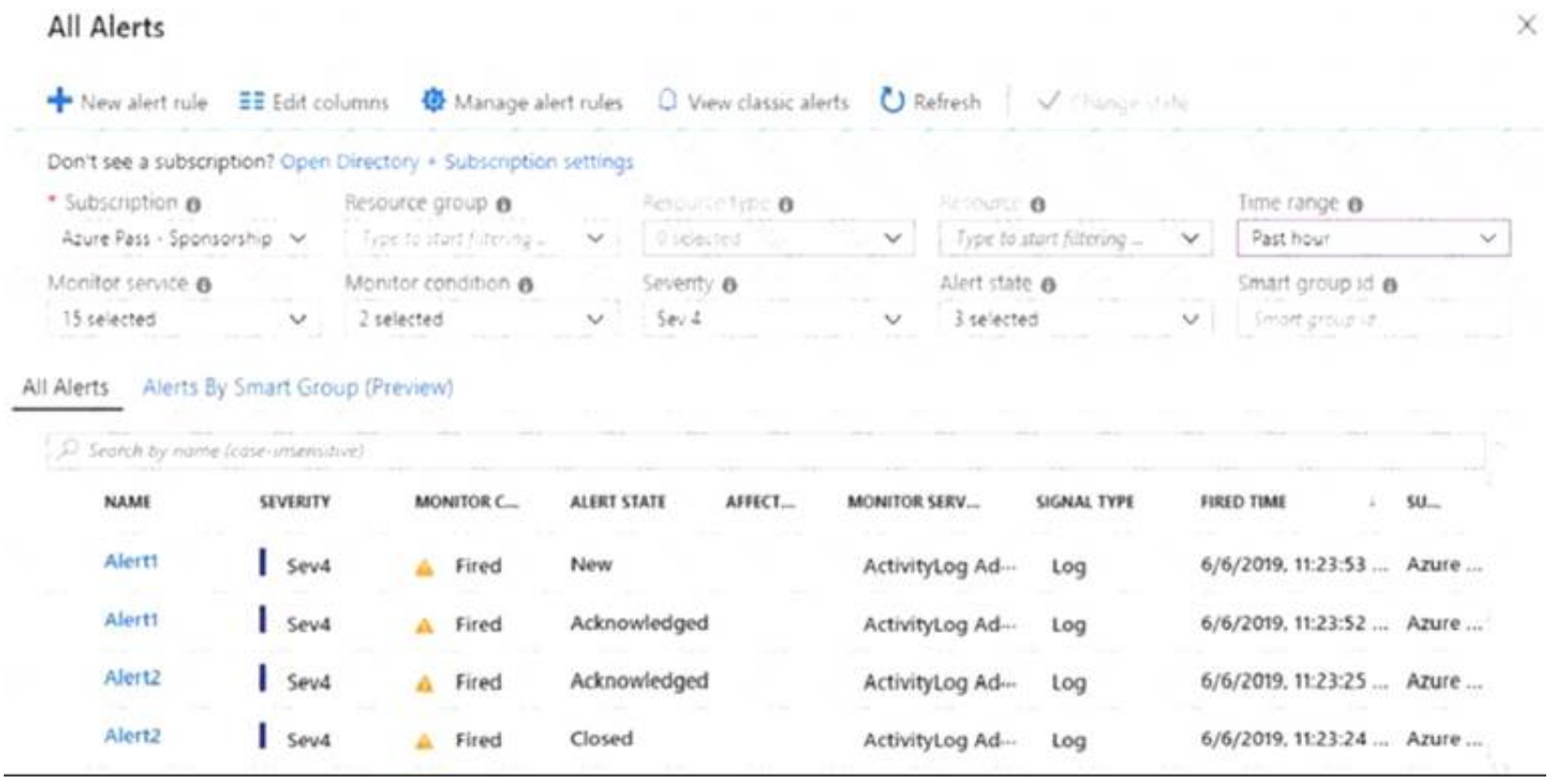
| Sign-in Activity | Risk Level |
|---|---|
| Users with leaked credentials | High |
| Sign-ins from anonymous IP addresses | Medium |
| Impossible travel to atypical locations | Medium |
| Sign-ins from infected devices | Medium |
| Sign-ins from IP addresses with suspicious activity | Low |
| Sign-ins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

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

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

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

**NEW QUESTION 64**
- (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.

The state of Alert1 that was fired at 11:23:52

- cannot be changed
- can be changed to Closed only
- can be changed to New only
- can be changed to New or Closed

The state of Alert2 that was fired at 11:23:24

- cannot be changed
- can be changed to Acknowledged only
- can be changed to New only
- can be changed to New or Acknowledged

A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 66**
- (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 69**
- (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 72**
- (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 75**
- (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 77**
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.
You need to ensure that User1 can create and manage administrative units. The solution must use the principle of least privilege.
Which role should you assign to User1?

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

**Answer:** A

**NEW QUESTION 81**
- (Exam Topic 4)
You are troubleshooting a security issue for an Azure Storage account You enable Azure Storage Analytics logs and archive It to a storage account. What should you use to retrieve the diagnostics logs?

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

**Answer:** A

**NEW QUESTION 83**
- (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 85**
- (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?

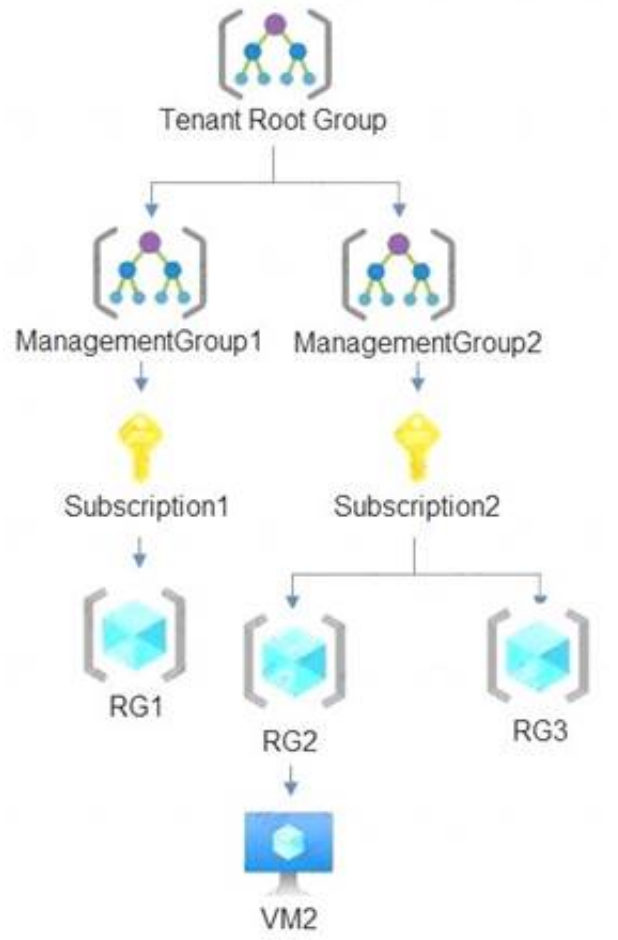
A. VM3 only
B. VM1 and VM3 only
C. VM3 and VM4 only
D. VM1, VM2, VM3, and VM4

**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 87**

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




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

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

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

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

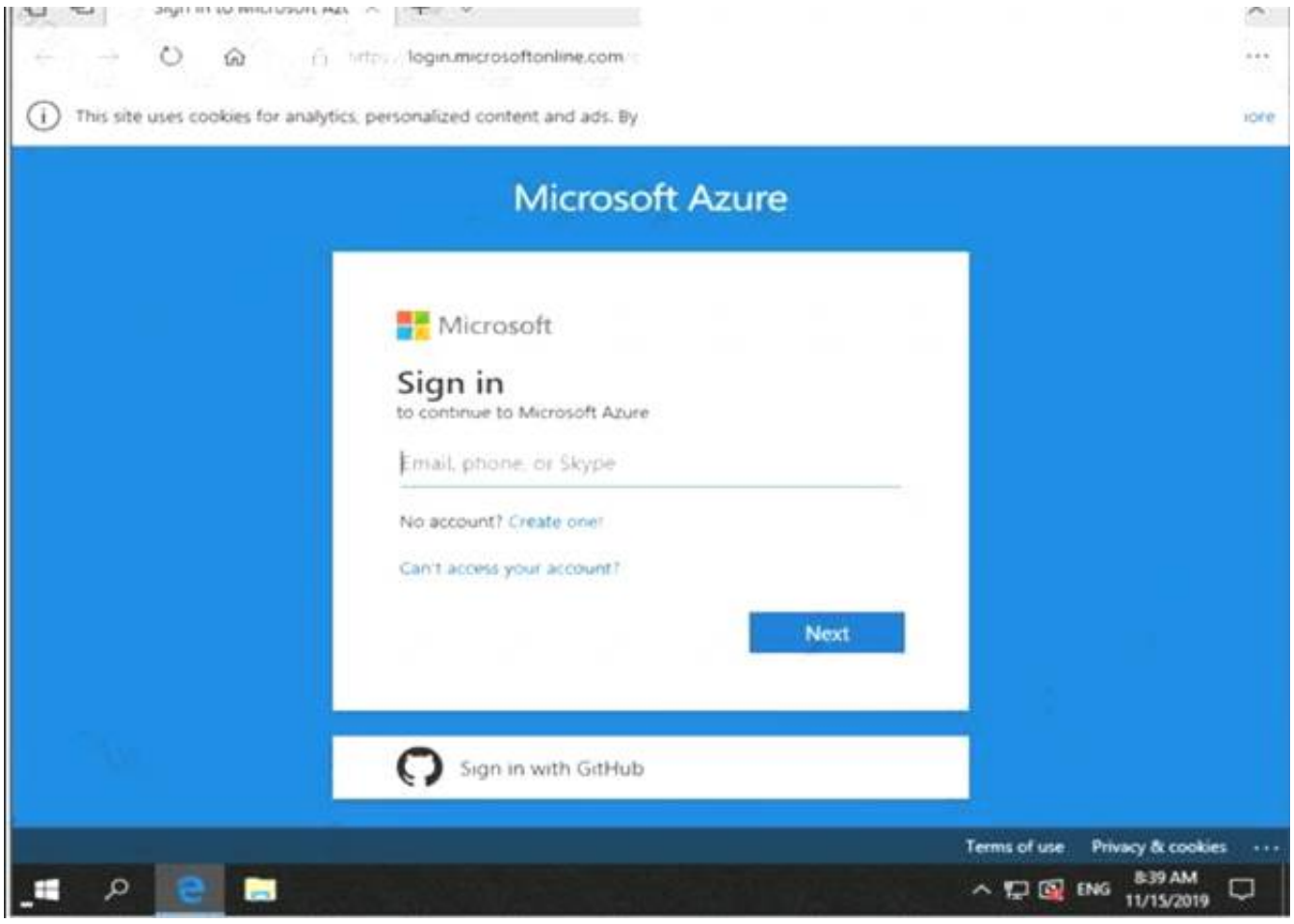
A. Mastered
B. Not Mastered

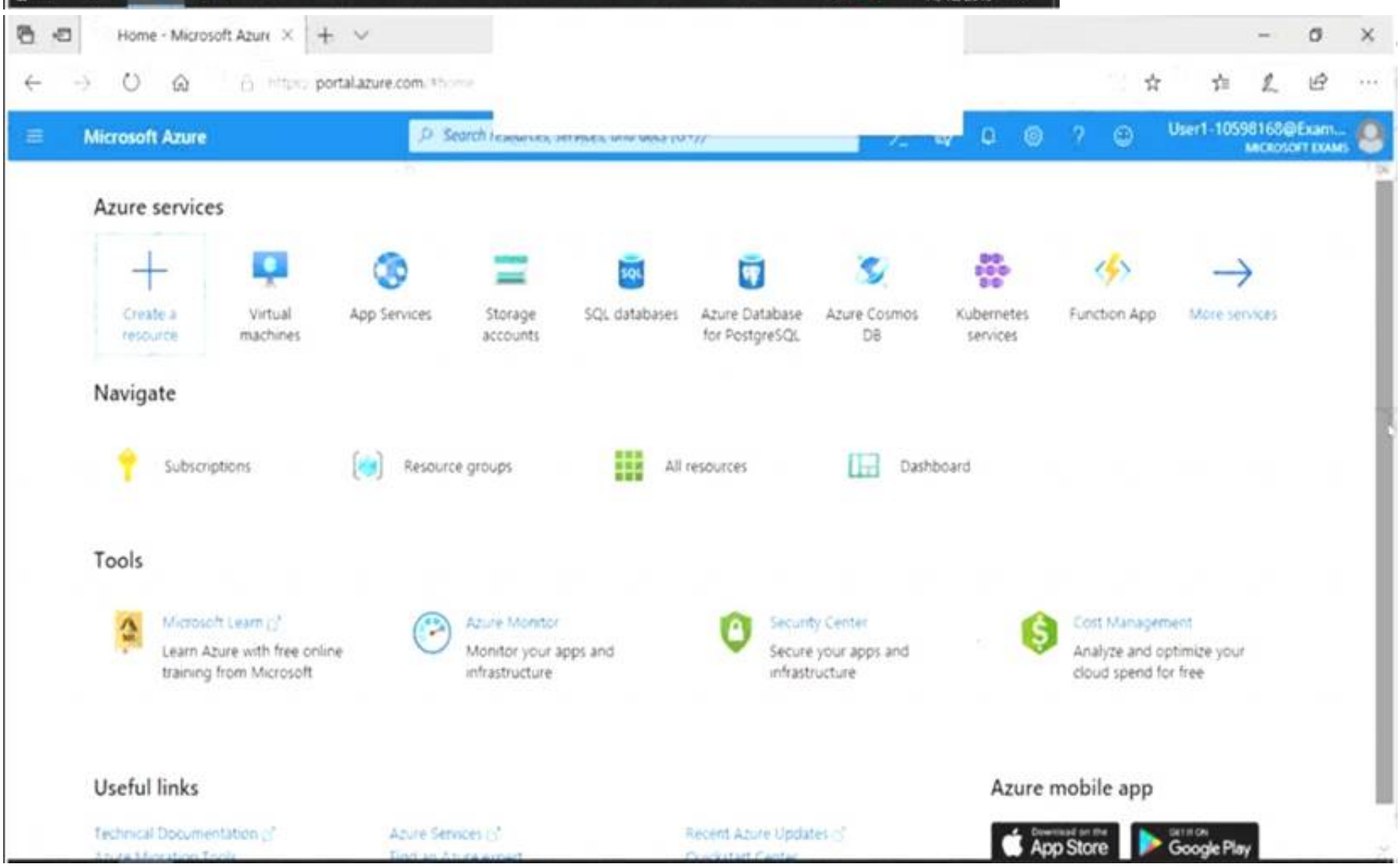
**Answer:** A

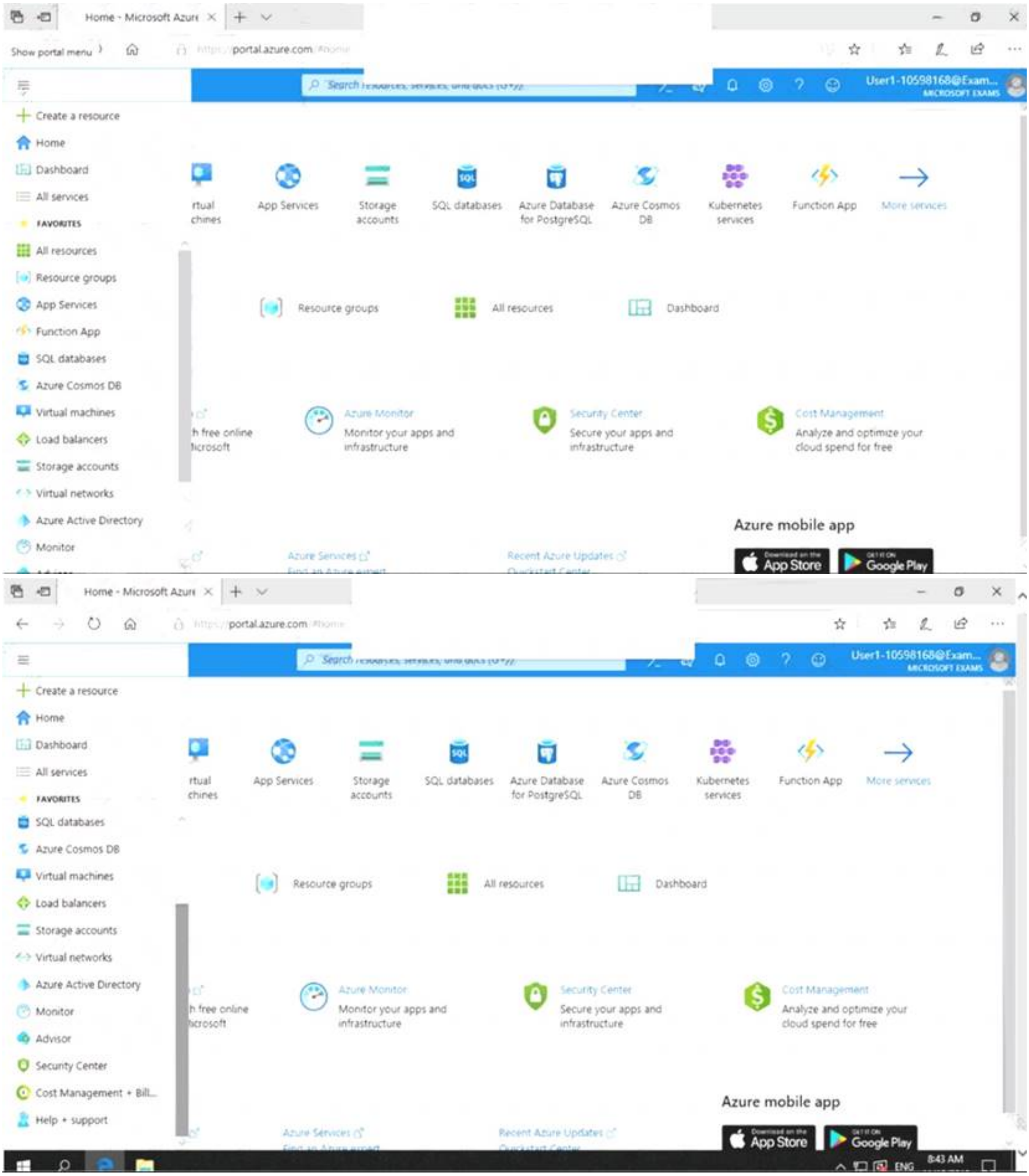
**Explanation:**

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

**NEW QUESTION 89**
- (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


login.microsoftonline.com
This site uses cookies for analytics, personalized content and ads. By
Microsoft Azure
Microsoft
Sign in
to continue to Microsoft Azure
Email, phone, or Skype
No account? Create one!
Can't access your account?
Next
Sign in with GitHub
Terms of use
Privacy & cookies
ENG
8:39 AM
11/15/2019


Home - Microsoft Azure
portal.azure.com
Microsoft Azure
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




You need to ensure that only devices connected to a 131.107.0.0/16 subnet can access data in the rg1lod10598168 Azure Storage account.
To complete this task, sign in to the Azure portal.

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Step 1:
* 1. In Azure portal go to the storage account you want to secure. Here: rg1lod10598168
* 2. Click on the settings menu called Firewalls and virtual networks.
* 3. To deny access by default, choose to allow access from Selected networks. To allow traffic from all networks, choose to allow access from All networks.
* 4. Click Save to apply your changes.
Step 2:
* 1. Go to the storage account you want to secure. Here: rg1lod10598168
* 2. Click on the settings menu called Firewalls and virtual networks.
* 3. Check that you've selected to allow access from Selected networks.
* 4. To grant access to a virtual network with a new network rule, under Virtual networks, click Add existing virtual network, select Virtual networks and Subnets options. Enter the 131.107.0.0/16 subnet and then click Add.
Note: When network rules are configured, only applications requesting data over the specified set of networks can access a storage account. You can limit access to your storage account to requests originating from specified IP addresses, IP ranges or from a list of subnets in an Azure Virtual Network (VNet).
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security

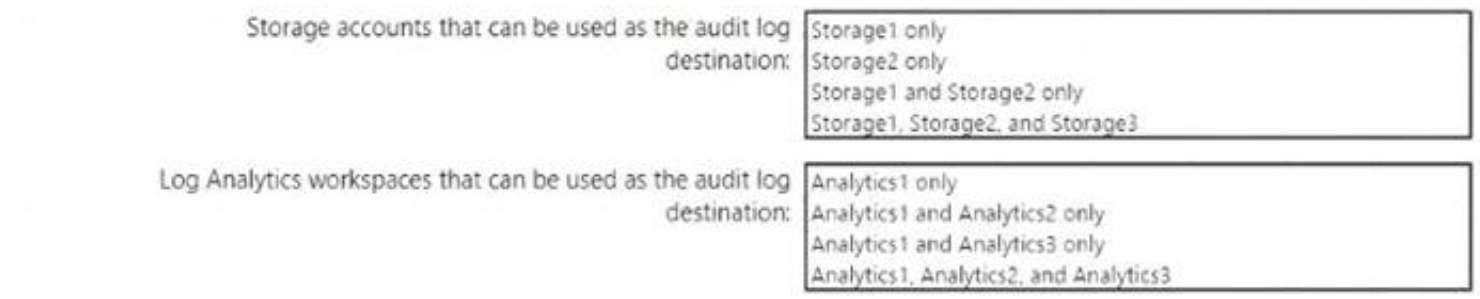
**NEW QUESTION 92**
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.

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

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

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

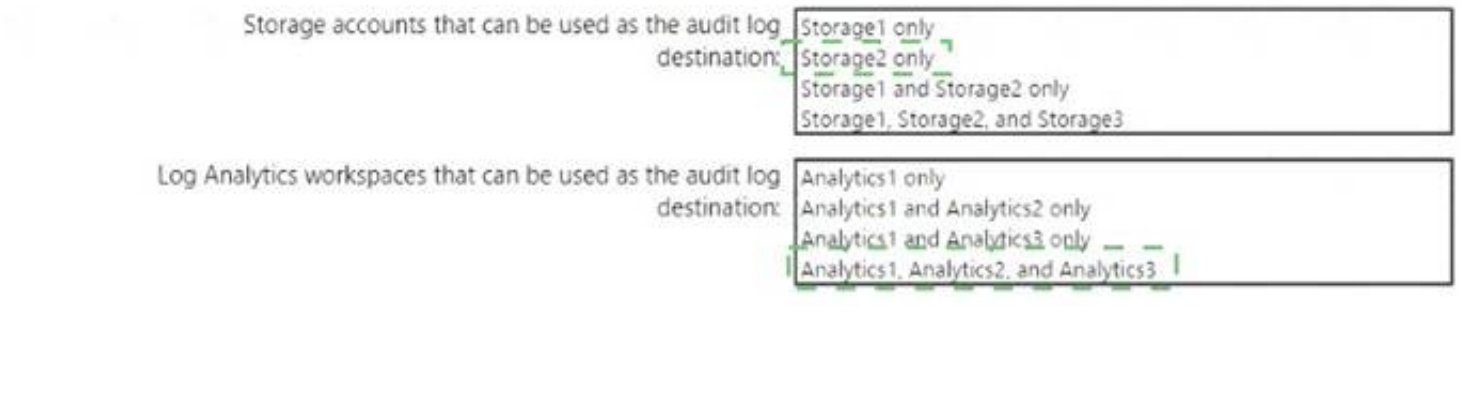
You need to configure auditing for SQL1.
Which storage accounts and Log Analytics workspaces can you use as the audit log destination? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
**Answer Area**




A. Mastered
B. Not Mastered

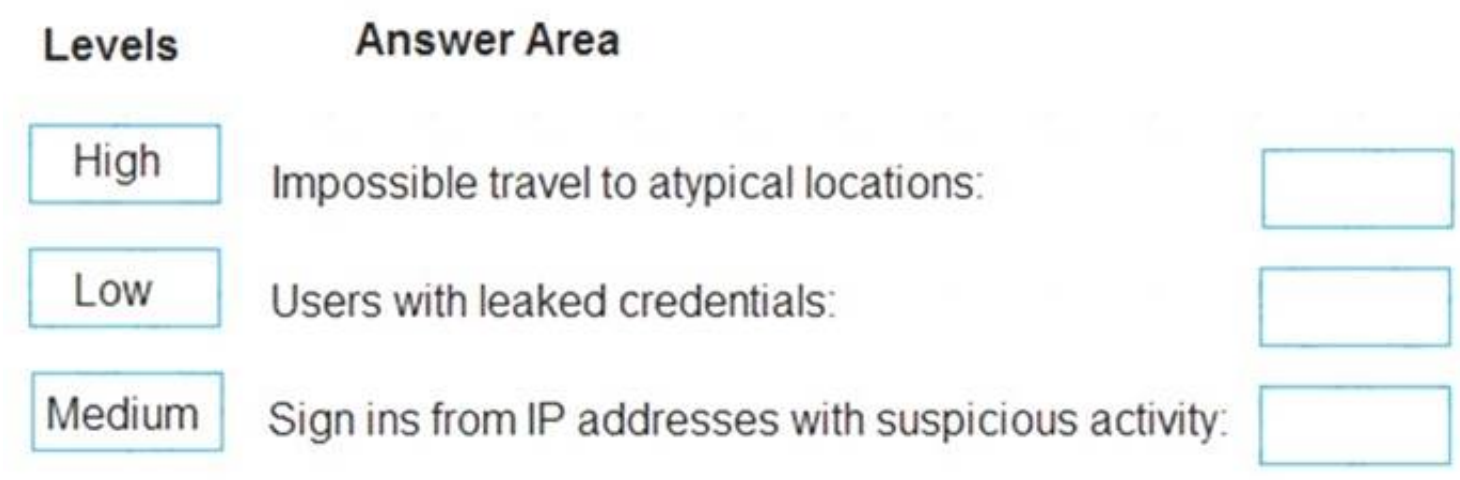
**Answer:** A

**Explanation:**
**Answer Area**




**NEW QUESTION 94**
- (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 96**
- (Exam Topic 4)
You have an Azure Subscription that is linked to an Azure Active Directory (Azure AD). The tenant contains the users shown in the following table.

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

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

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

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

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

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


A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**


**NEW QUESTION 101**

- (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 106**
- (Exam Topic 4)
You have an Azure subscription mat contains a resource group named RG1. RG1 contains a storage account named storage1.
You have two custom Azure rotes named Role1 and Role2 that are scoped to RG1. The permissions for Role1 are shown in the following JSON code.

```
"permissions": [
            {
                "actions": [
                    "Microsoft.Storage/storageAccounts/listKeys/action".

                    ],
                    "notActions": [],
                    "dataActions": [],
                    "notDataActions": []
                }
            ]
```

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

```
"permissions": [
            {
             "actions": [
                 "Microsoft.Storage/storageAccounts/listKeys/action",
               "Microsoft.Storage/storageAccounts/ListAccountSas/action",
                 "Microsoft.Storage/storageAccounts/read"
             ],
             "notActions": [],
             "dataActions": [],
             "notDataActions": []
```

Answer Area

| Statements | Yes | No |
|---|---|---|
| User1 can read data in storage1. | ○ | ○ |
| User2 can read data in storage1. | ○ | ○ |
| User3 can restore storage1 from a backup in Azure Backup. | ○ | ○ |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area

| Statements | Yes | No |
|---|---|---|
| User1 can read data in storage1. | ○ | ○ |
| User2 can read data in storage1. | ○ | ○ |
| User3 can restore storage1 from a backup in Azure Backup. | ○ | ○ |

**NEW QUESTION 108**
- (Exam Topic 4)
You plan to create an Azure Kubernetes Service (AKS) cluster in an Azure subscription. The manifest of the registered server application is shown in the following exhibit.

Save Discard Upload Download

The editor below allows you to update this application by directly modifying its JSON representation. For more details, see: Understanding the Azure Active Directory application manifest.

```
{
    "id": "d6b00db3-7ef4-4f3c-b1e7-8346f0a59546",
    "acceptMappedClaims": null,
    "accessTokenAcceptedVersion": null,
    "addIns": [],
    "allowPublicClient": null,
    "appId": "88137405-6a75-4c20-903a-f7b18ff7d496",
    "appRoles": [],
    "oauth2AllowUrlPathMatching": false,
    "createdDateTime": "2019-07-15T21:09:20Z",
    "groupMembershipClaims": null,
    "identifierUris": [],
    "informationalUrls": {
        "termsOfService": null,
        "support": null,
        "privacy": null,
        "marketing": null
    },
    "keyCredentials": [],
    "knownClientApplications": [],
    "logoUrl": null,
    "logoutUrl": null,
    "name": "AKSAzureADServer",
    "oauth2AllowIdTokenImplicitFlow": false,
    "oauth2AllowImplicitFlow": false,
    "oauth2Permissions": [],
    "oauth2RequirePostResponse": false,
    "optionalClaims": null,
    "orgRestrictions": [],
    "parentalControlSettings": {
```

You need to ensure that the AKS cluster and Azure Active Directory (Azure AD) are integrated. Which property should you modify in the manifest?

A. accessTokenAcceptedVersion
B. keyCredentials
C. groupMembershipClaims
D. acceptMappedClaims

**Answer:** C

**Explanation:**

Reference:
https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli https://www.codeproject.com/Articles/3211864/Operation-and-Maintenance-of-AKS-Applications

**NEW QUESTION 113**
- (Exam Topic 4)
You have a network security group (NSG) bound to an Azure subnet.
You run Get-AzureRmNetworkSecurityRuleConfig and receive the output shown in the following exhibit.

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

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

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

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

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

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

- allowed
- dropped
- forwarded

A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 115**
- (Exam Topic 4)
You have an Azure subscription named Subscription1 that contains a resource group named RG1 and the users shown in the following table.

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

You perform the following tasks:

- Assign User1 the Network Contributor role for Subscription1.
- Assign User2 the Contributor role for RG1.

To Subscription1 and RG1, you assign the following policy definition: External accounts with write permissions should be removed from your subscription.

What is the Compliance State of the policy assignments?

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

**Answer:** A

**NEW QUESTION 116**
- (Exam Topic 4)
You have 10 on-premises servers that run Windows Server 2019.
You plan to implement Azure Security Center vulnerability scanning for the servers. What should you install on the servers first?

A. the Security Events data connector in Azure Sentinel
B. the Microsoft Endpoint Configuration Manager client
C. the Azure Arc enabled servers Connected Machine agent
D. the Microsoft Defender for Endpoint agent

**Answer:** D

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/azure-arc/servers/agent-overview https://docs.microsoft.com/en-us/azure/security-center/deploy-vulnerability-assessment-vm

**NEW QUESTION 120**
- (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 122**
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Security Center for the centralized policy management of three Azure subscriptions. You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create a resource graph and an assignment that is scoped to a management group. Does this meet the goal?

A. Yes
B. No

**Answer:** B

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

**NEW QUESTION 125**
- (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

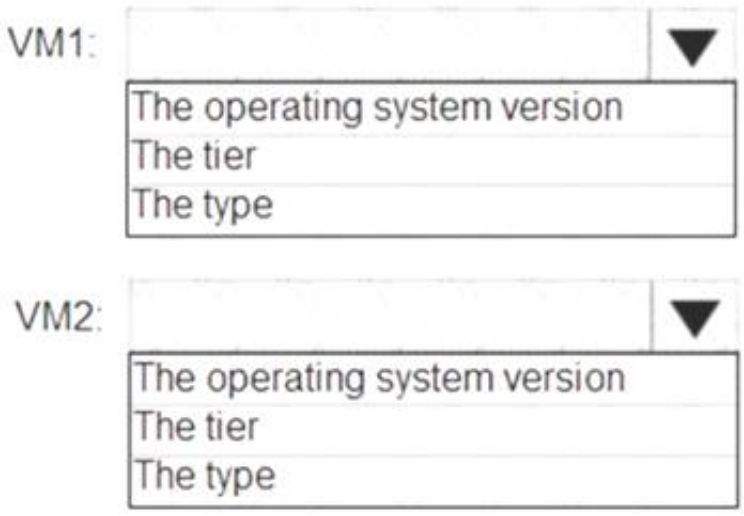
**Answer:** D

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

**NEW QUESTION 128**
- (Exam Topic 4)
You have two Azure virtual machines in the East US2 region as shown in the following table.

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

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




A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 132**
- (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 135**
- (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.

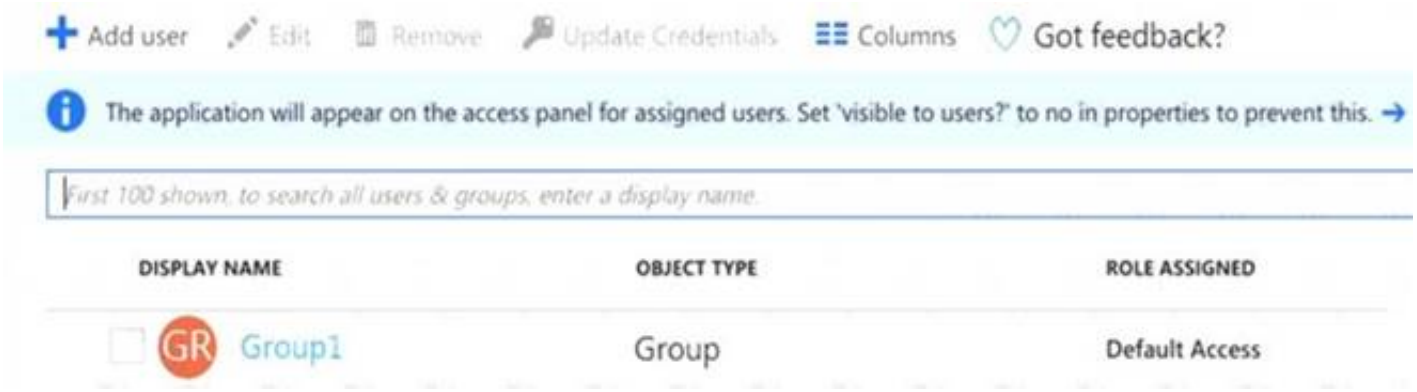
**Answer:** B

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

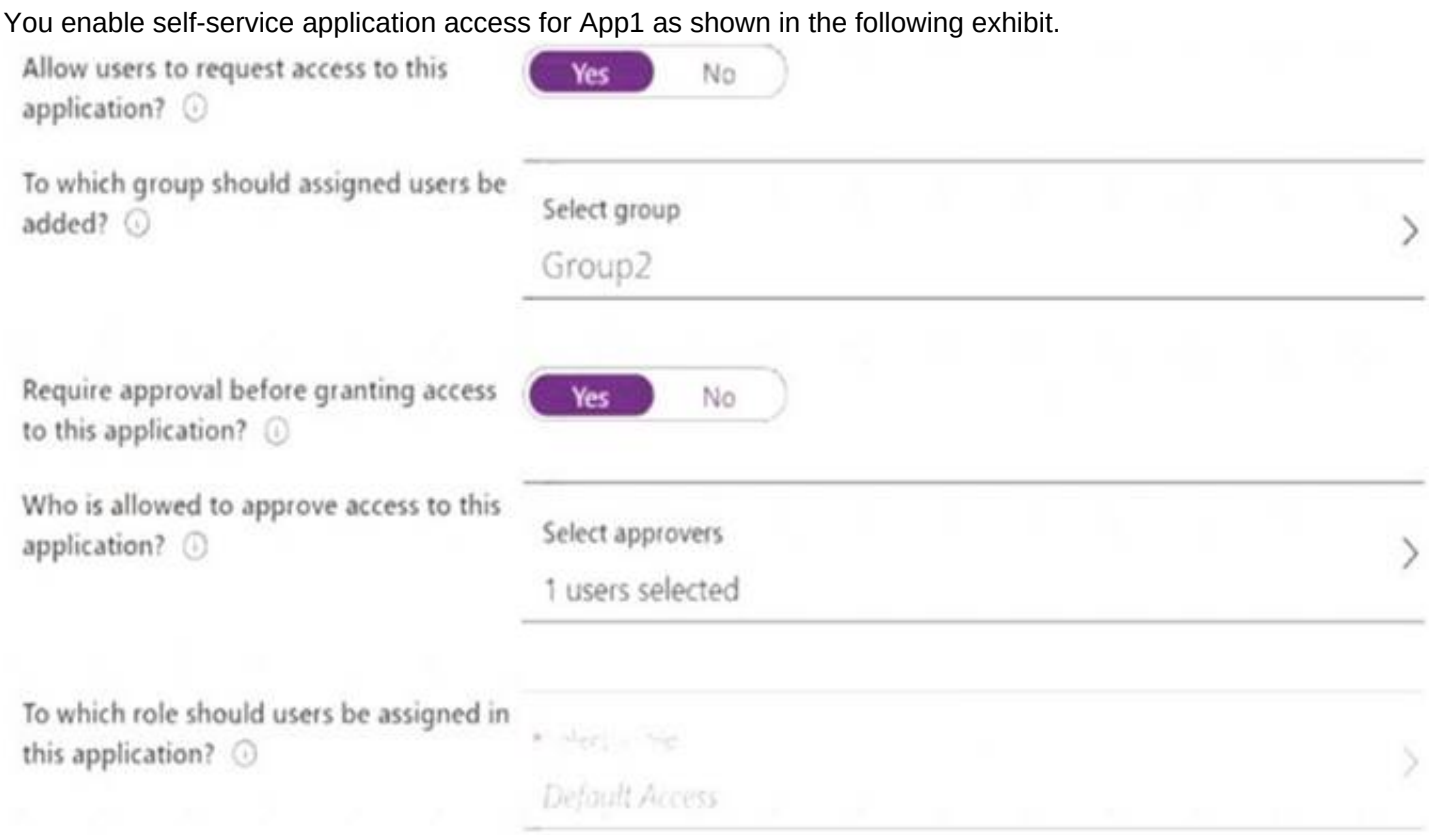
**NEW QUESTION 136**
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains the resources shown in the following table.

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

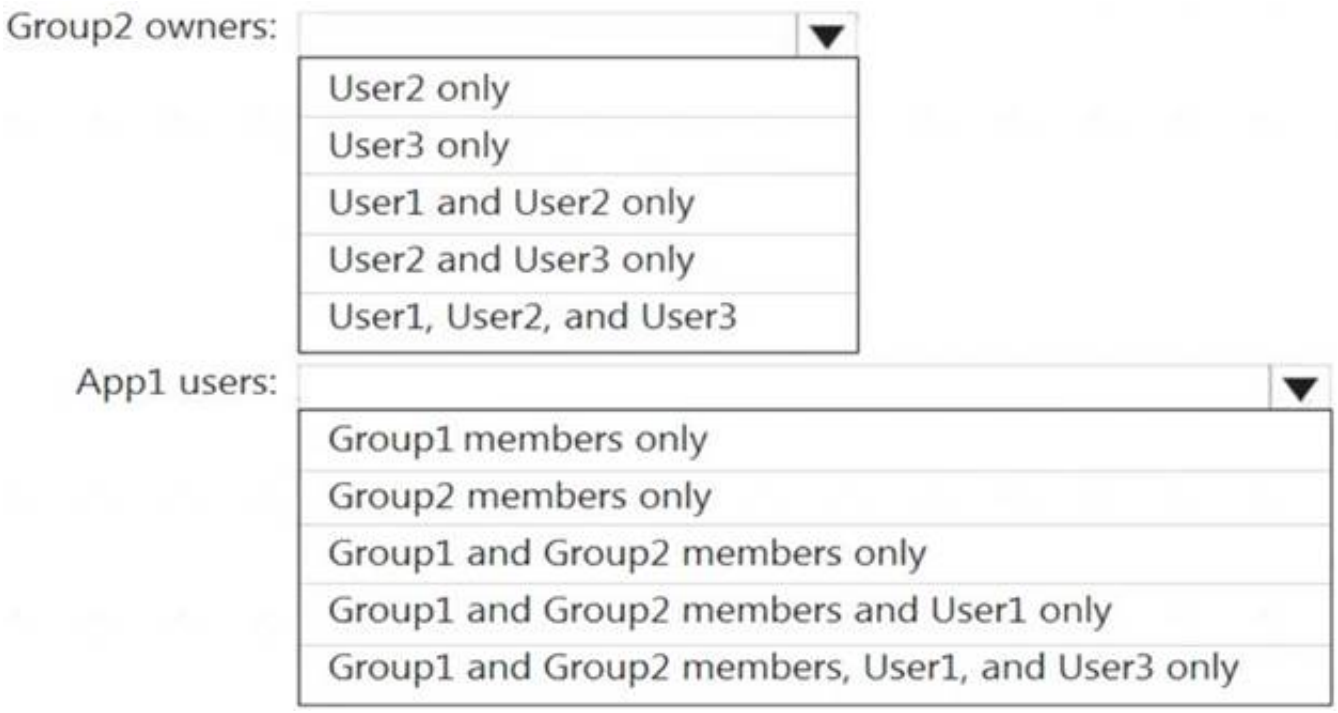
User2 is the owner of Group2.
The user and group settings for App1 are configured as shown in the following exhibit.




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




User3 is configured to approve access to Appl.
You need to identify the owners of Group2 and the users of Appl.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.




A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Reference:

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

**NEW QUESTION 140**
- (Exam Topic 4)
You have an Azure Storage account named storage1 that has a container named container1. You need to prevent the blobs in container1 from being modified.
What should you do?

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

**Answer:** B

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

**NEW QUESTION 145**
- (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 149**
- (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.

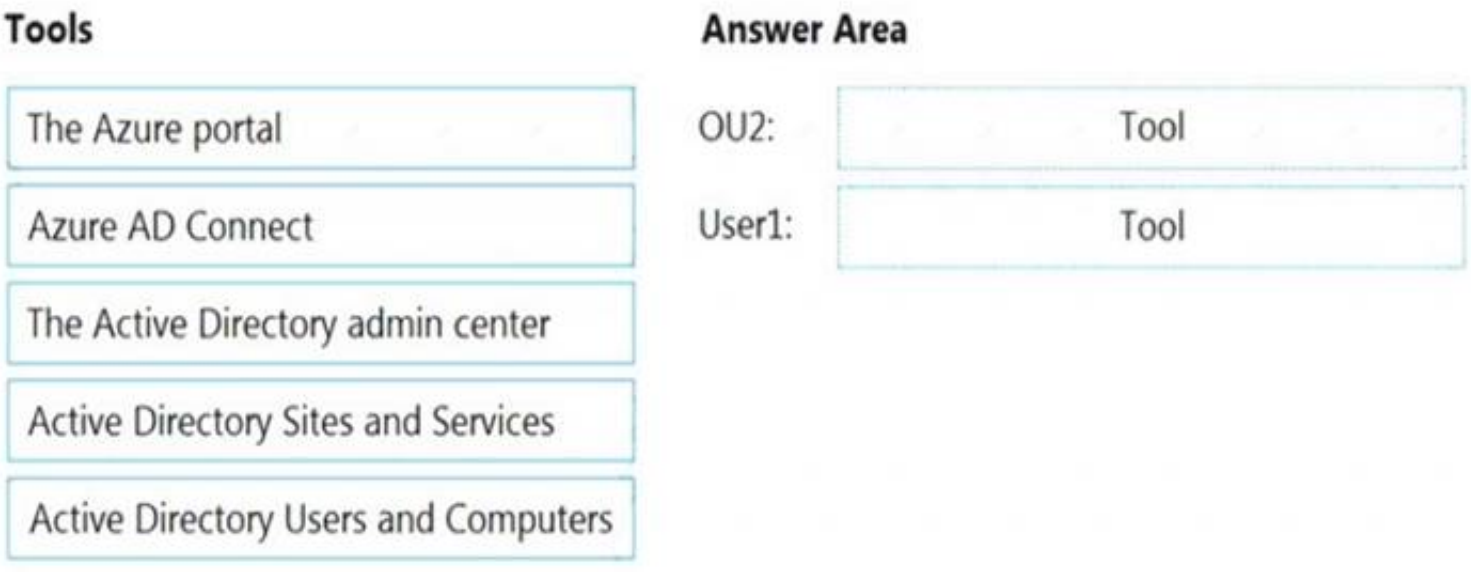
**NEW QUESTION 150**
- (Exam Topic 4)
You have an Azure subscription that contains virtual machines. You enable just in time (JIT) VM access to all the virtual machines.
You need to connect to a virtual machine by using Remote Desktop. What should you do first?

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 153**
- (Exam Topic 3)
You need to perform the planned changes for OU2 and User1.
Which tools should you use? To answer, drag the appropriate tools to the correct resources. Each tool may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.




A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Table Description automatically generated

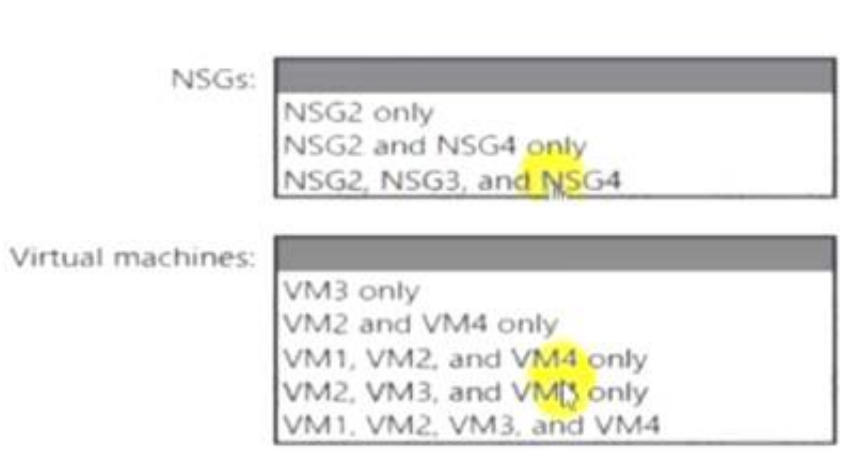
**NEW QUESTION 155**
- (Exam Topic 3)
You need to meet the technical requirements for the finance department users. Which CAPolicy1 settings should you modify?

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 156**
- (Exam Topic 3)
You implement the planned changes for ASG1 and ASG2.
In which NSGs can you use ASG1. and the network interfaces of which virtual machines can you assign to ASG2?




A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Graphical user interface, text, application, chat or text message Description automatically generated

**NEW QUESTION 158**
- (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

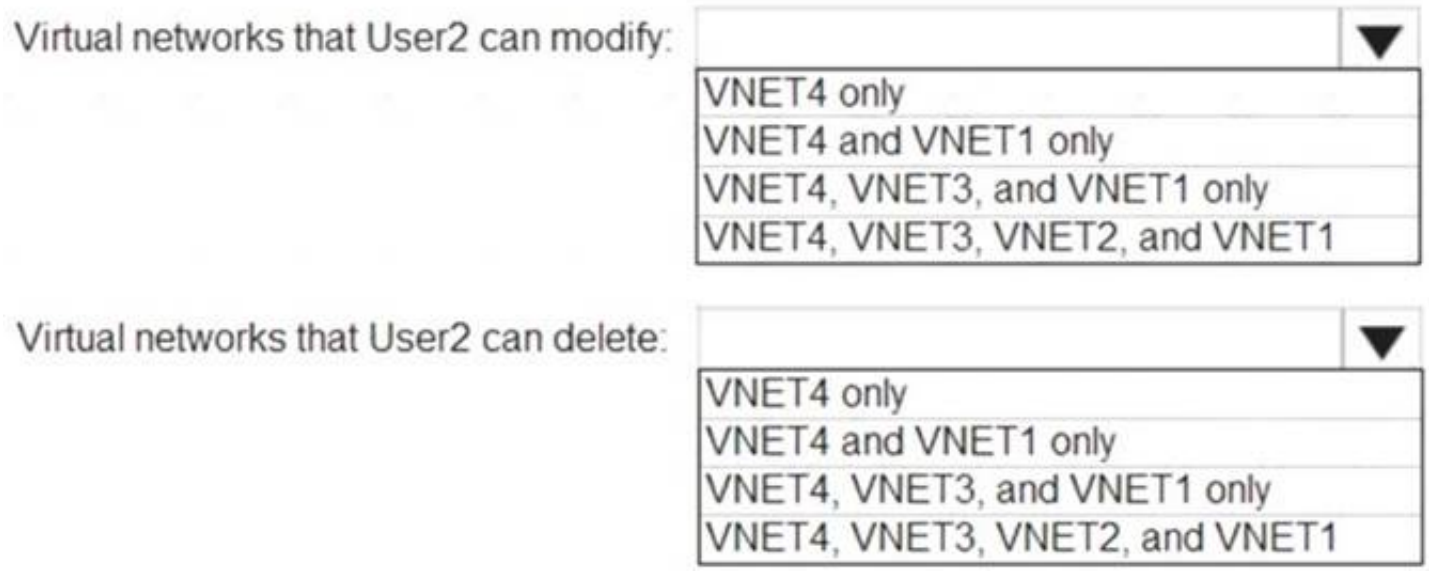
**NEW QUESTION 162**
- (Exam Topic 2)
You need to ensure that User2 can implement PIM. What should you do first?

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 163**
- (Exam Topic 2)
HOTSPOT
Which virtual networks in Sub1 can User2 modify and delete in their current state? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.




A. Mastered
B. Not Mastered

**Answer:** A

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

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

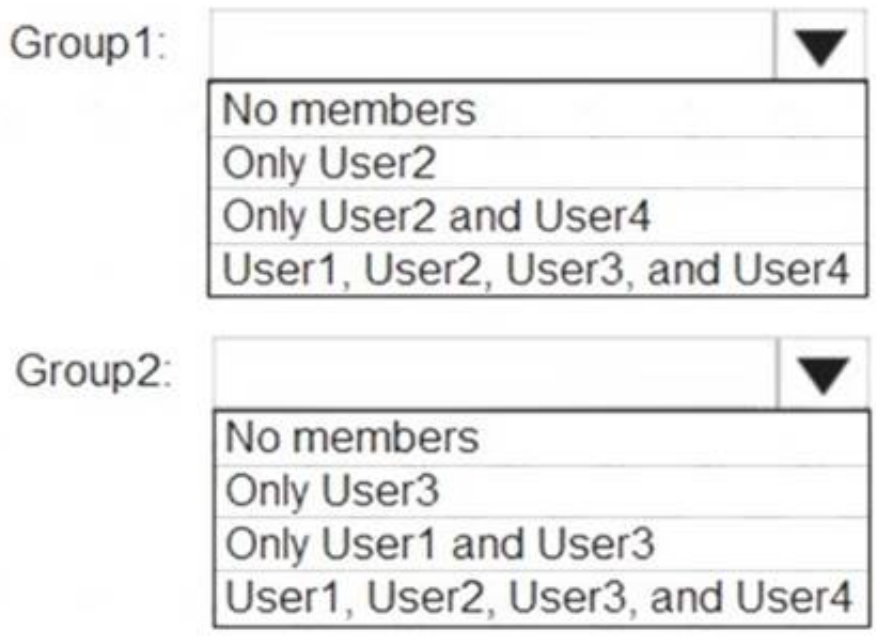
| Name | Resource group |
|---|---|
| VNET1 | RG1 |
| VNET2 | RG2 |
| VNET3 | RG3 |
| VNET4 | RG4 |

Sub1 contains the locks shown in the following table.

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

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

**NEW QUESTION 165**
- (Exam Topic 2)
What is the membership of Group1 and Group2? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

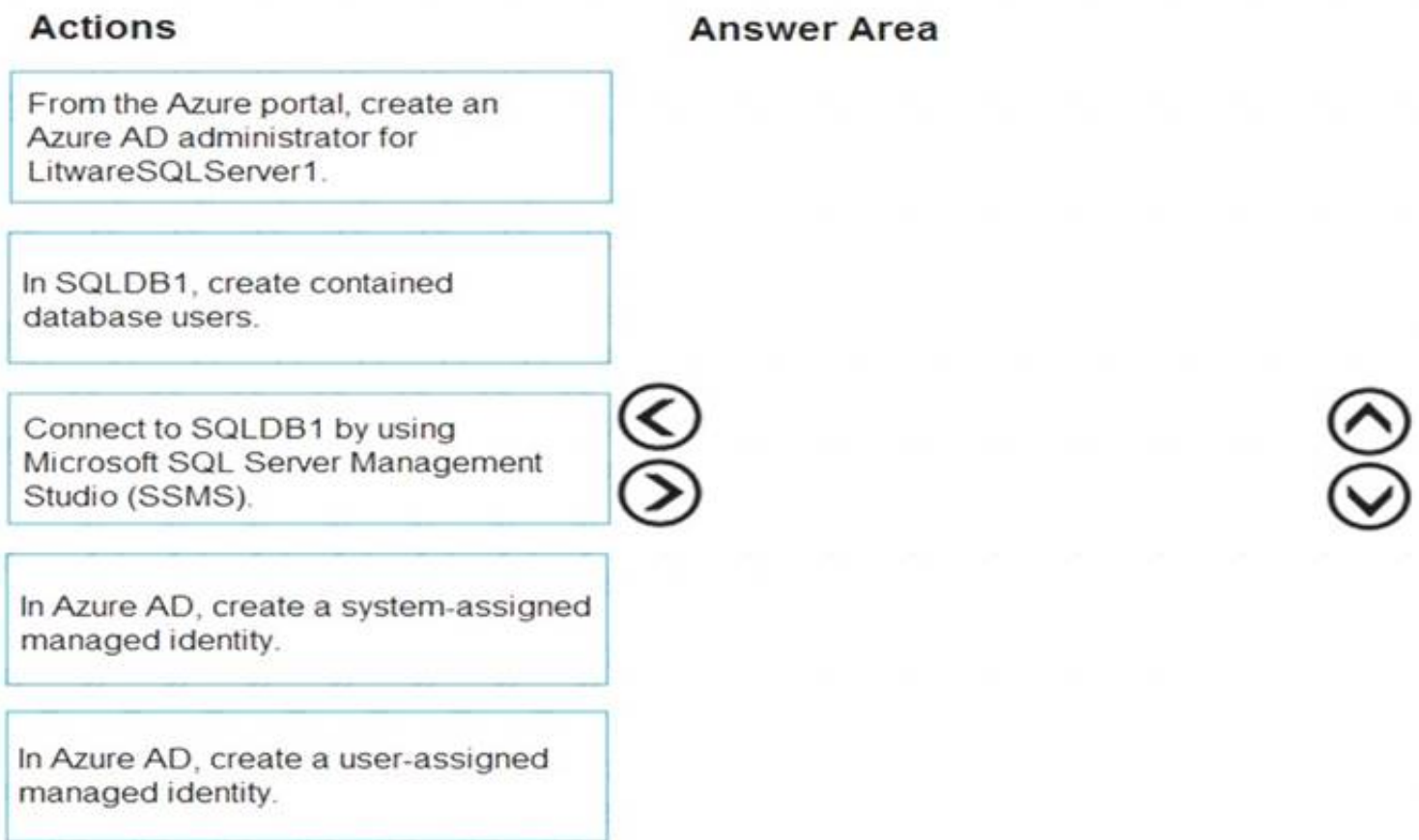



A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Box 1: User1, User2, User3, User4
Contains "ON" is true for Montreal (User1), MONTREAL (User2), London (User 3), and Ontario (User4) as string and regex operations are not case sensitive.
Box 2: User1, User2, User3, User4 References:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership

**NEW QUESTION 170**
- (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 173**
- (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

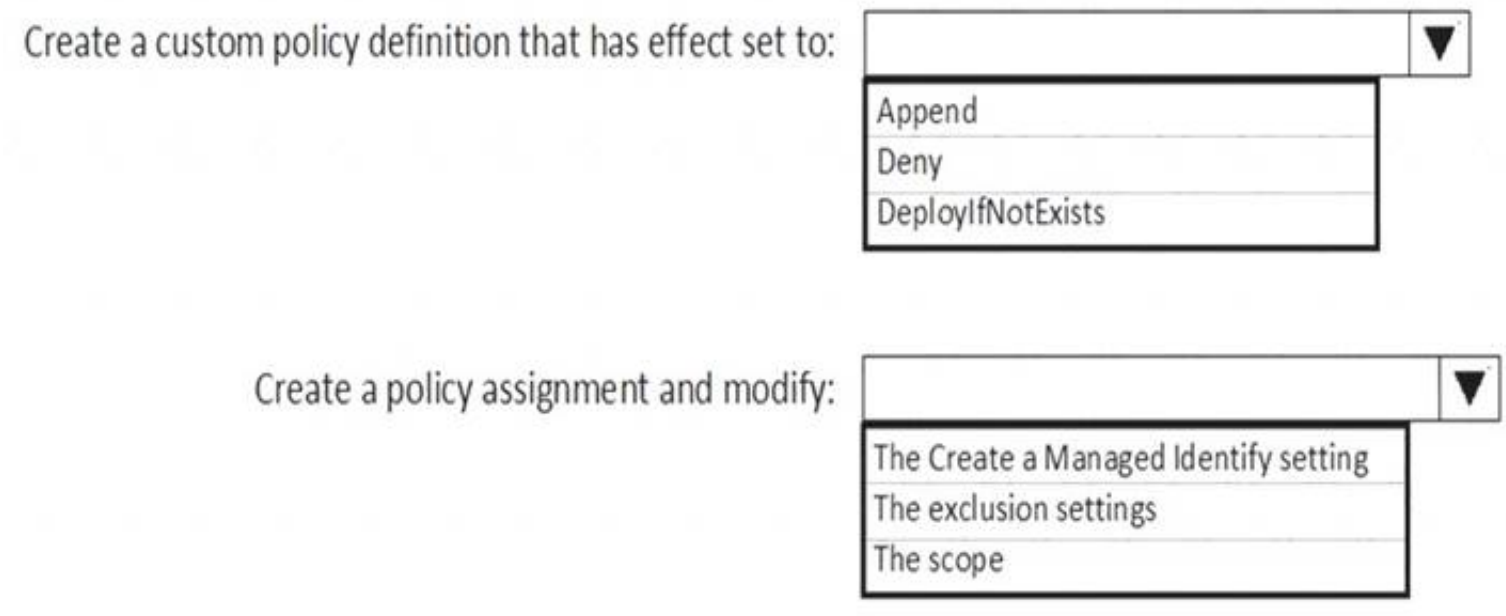
**NEW QUESTION 178**
- (Exam Topic 1)
You need to configure WebApp1 to meet the data and application requirements.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Upload a public certificate.
B. Turn on the HTTPS Only protocol setting.
C. Set the Minimum TLS Version protocol setting to 1.2.
D. Change the pricing tier of the App Service plan.
E. Turn on the Incoming client certificates protocol setting.

**Answer:** BE

**Explanation:**
Refer https://docs.microsoft.com/en-us/azure/app-service/app-service-web-configure-tls-mutual-auth

**NEW QUESTION 183**
- (Exam Topic 1)
You need to deploy Microsoft Antimalware to meet the platform protection requirements. What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.




A. Mastered
B. Not Mastered

**Answer:** A

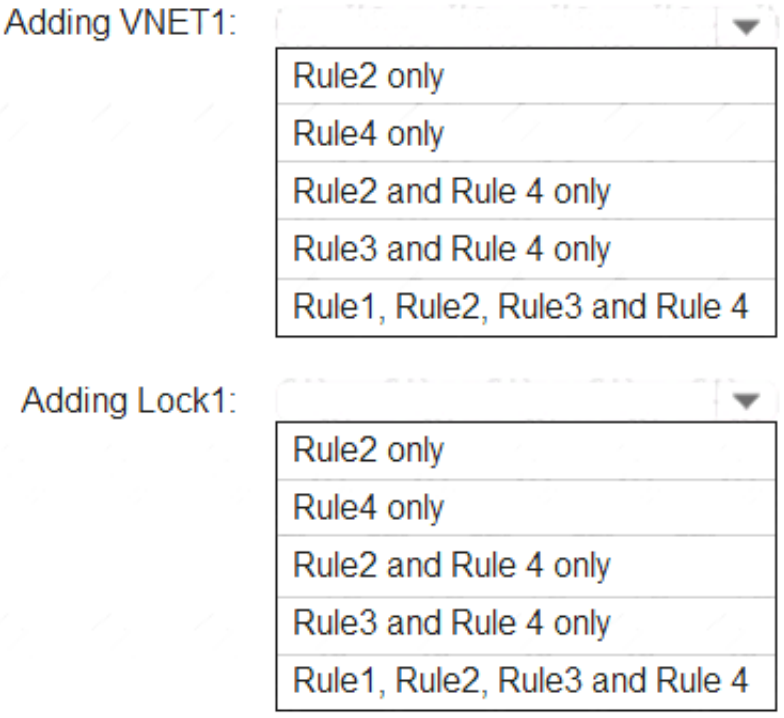
**Explanation:**
* 1. DeployifNotExists
* 2. Scope

**NEW QUESTION 187**
- (Exam Topic 4)
You have an Azure subscription that contains a user named Admin1 and a resource group named RG1. In Azure Monitor, you create the alert rules shown in the following table.

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

Admin1 performs the following actions on RG1:
- Adds a virtual network named VNET1
- Adds a Delete lock named Lock1

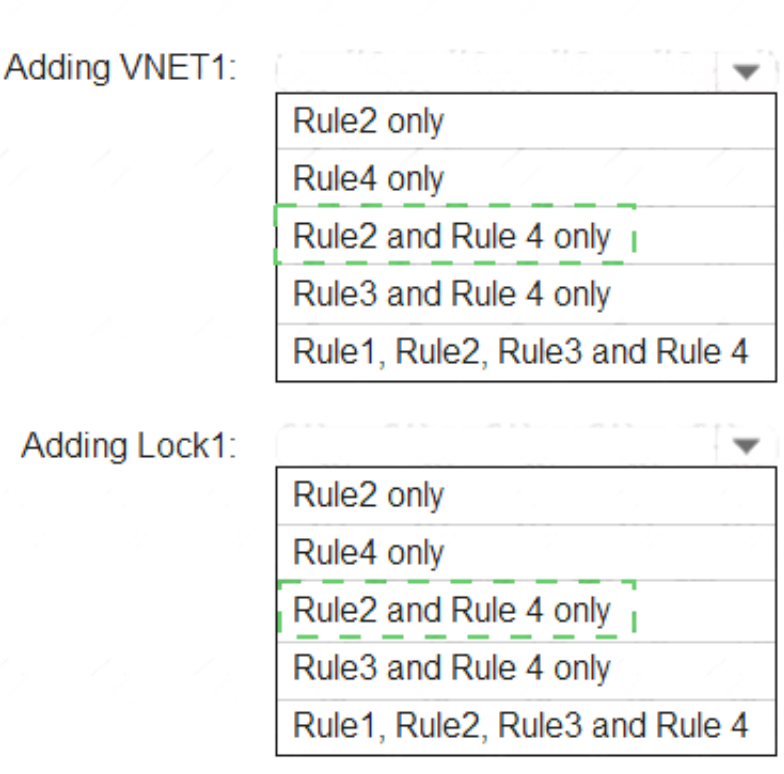
Which rules will trigger an alert as a result of the actions of Admin1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.




A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**




**NEW QUESTION 191**
- (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 195**
- (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

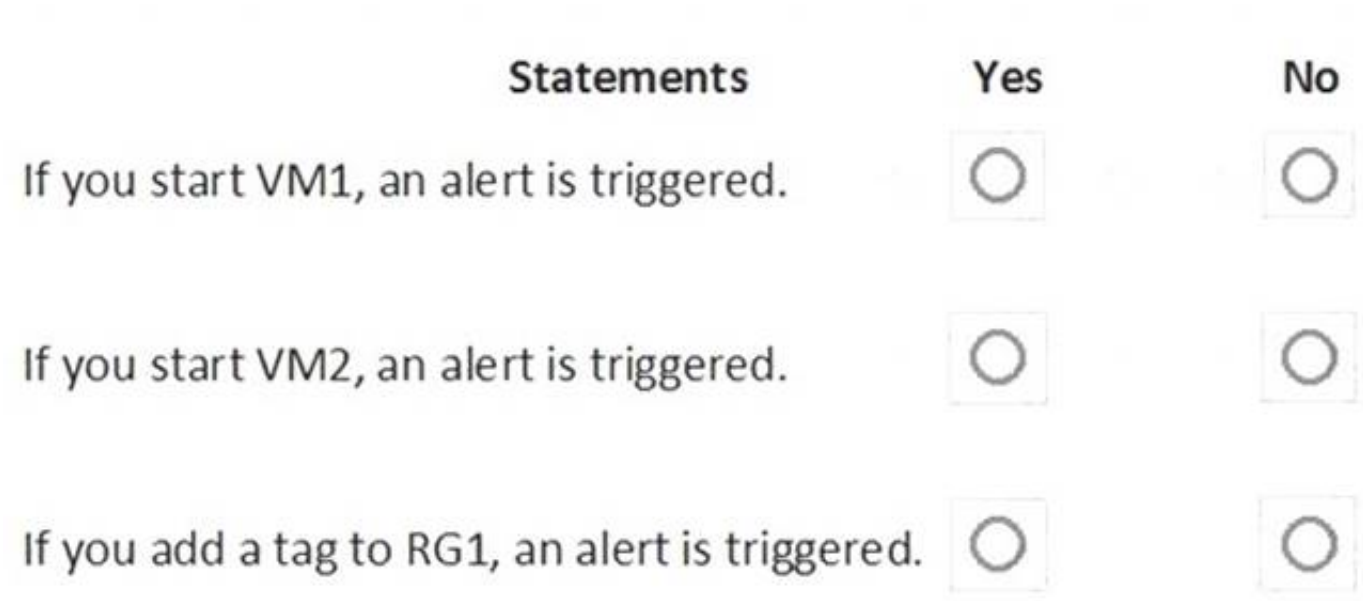
**Answer:** D

**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 196**
- (Exam Topic 4)
You create an alert rule that has the following settings:
- Resource: RG1
- Condition: All Administrative operations
- Actions: Action groups configured for this alert rule: ActionGroup1
- Alert rule name: Alert1

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

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




A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 198**
- (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 202**
- (Exam Topic 4)
You have a web app hosted on an on-premises server that is accessed by using a URL of https://www.contoso.com. You plan to migrate the web app to Azure.
You will continue to use https://www.contoso.com. You need to enable HTTPS for the Azure web app. What should you do first?

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

**Answer:** B

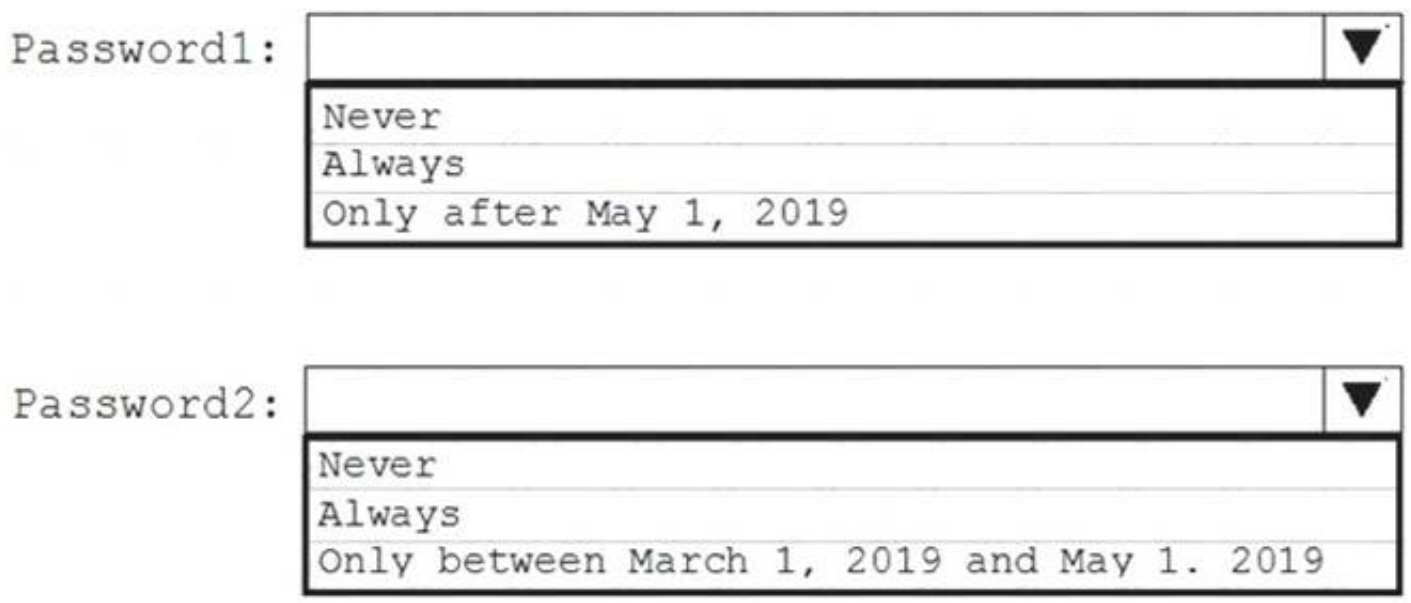
**Explanation:**
https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate#private-certificate-requirements

**NEW QUESTION 205**
- (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 206**
- (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 208**
- (Exam Topic 4)
You have an Azure subscription that contains an app named App1. App1 has the app registration shown in the following table.

| API | Permission | Type | Admin consent required | Status |
|---|---|---|---|---|
| Microsoft.Graph | User.Read | Delegated | No | None |
| Microsoft.Graph | Calendars.Read | Delegated | No | None |

You need to ensure that App1 can read all user calendars and create appointments. The solution must use the principle of least privilege.
What should you do?

A. Add a new Delegated API permission for Microsoft.Graph Calendars.ReadWrite.
B. Add a new Application API permission for Microsoft.Graph Calendars.ReadWrite.
C. Select Grant admin consent.
D. Add a new Delegated API permission for Microsoft.Graph Calendars.ReadWrite.Shared.

**Answer:** A

**Explanation:**
Reference:
https://docs.microsoft.com/en-us/graph/permissions-reference#calendars-permissions

**NEW QUESTION 210**
- (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?

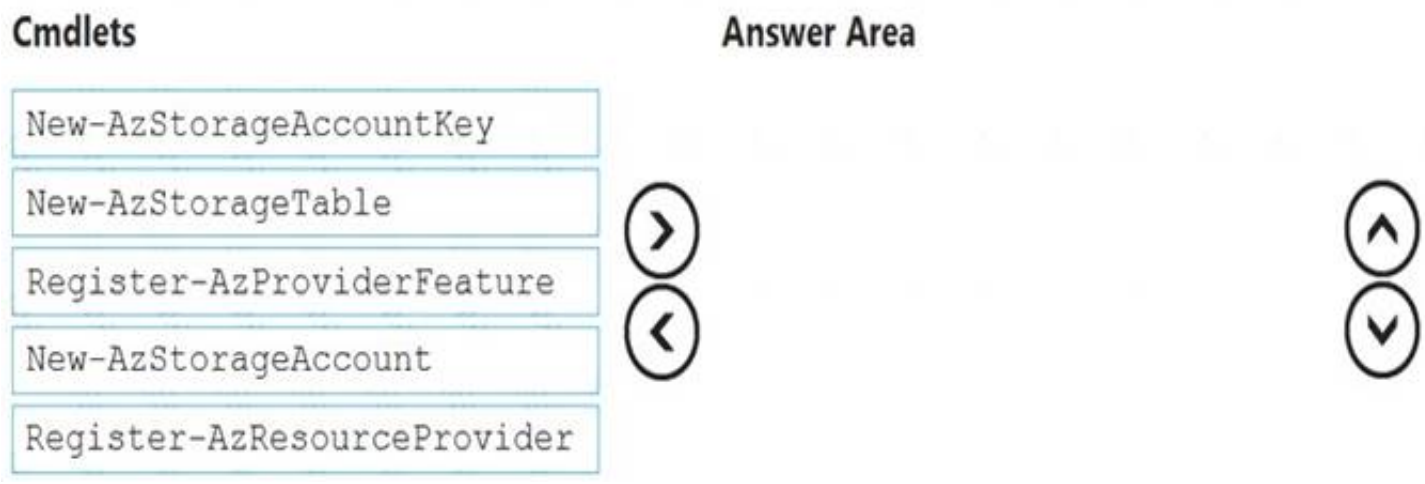
A. Add an Azure Policy definition to the root management group.
B. Modify the role-based access control (RBAC) role assignments for the root management group.

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 211**
- (Exam Topic 4) You have an Azure subscription. You plan to create a storage account.
You need to use customer-managed keys to encrypt the tables in the storage account.
From Azure Cloud Shell, which three cmdlets should you run in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the correct order.




A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 215**
- (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

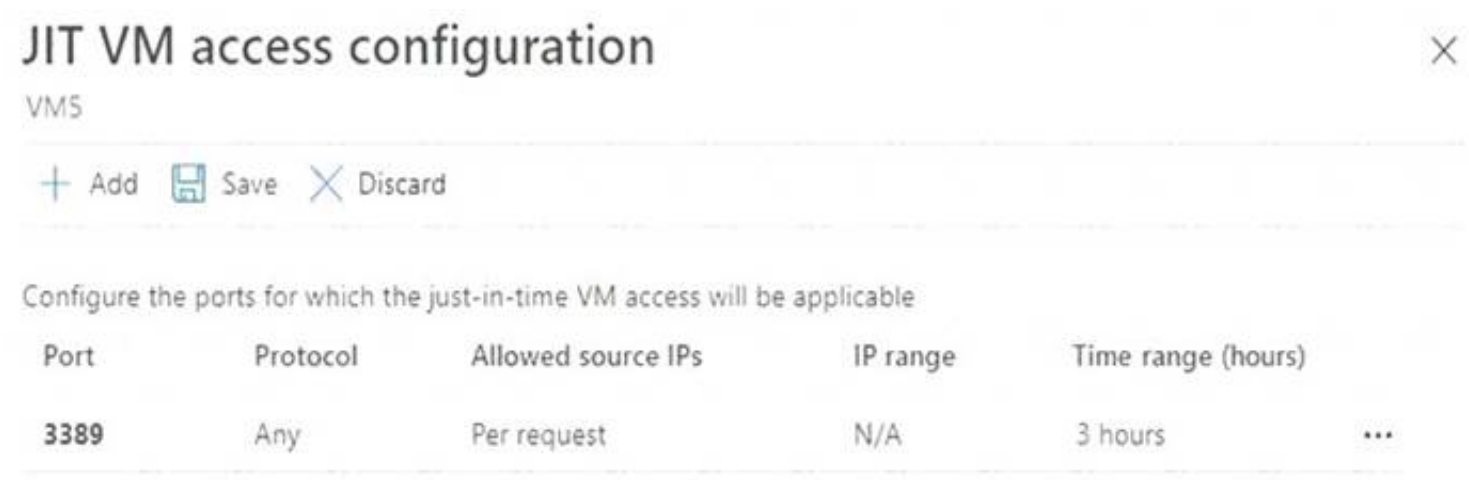
**Answer:** C

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

**NEW QUESTION 218**
- (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 221**
- (Exam Topic 4)
Your company plans to create separate subscriptions for each department. Each subscription will be associated to the same Azure Active Directory (Azure AD) tenant.
You need to configure each subscription to have the same role assignments. What should you use?

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

**Answer:** D

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

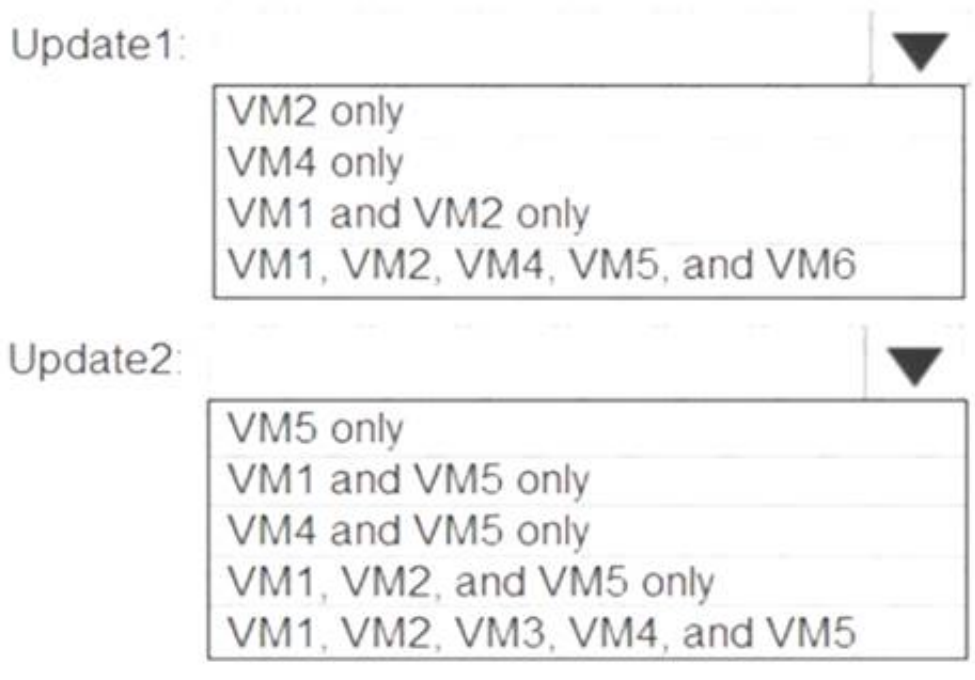
- Role Assignments
- Policy Assignments
- Azure Resource Manager templates
- Resource Groups

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

**NEW QUESTION 224**
- (Exam Topic 4)
You have Azure virtual machines that have Update Management enabled. The virtual machines are configured as shown in the following table.

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

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




A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 228**
- (Exam Topic 4)
You have an Azure environment.
You need to identify any Azure configurations and workloads that are non-compliant with ISO 27001 standards. What should you use?

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

**Answer:** C

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

**NEW QUESTION 232**

- (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.

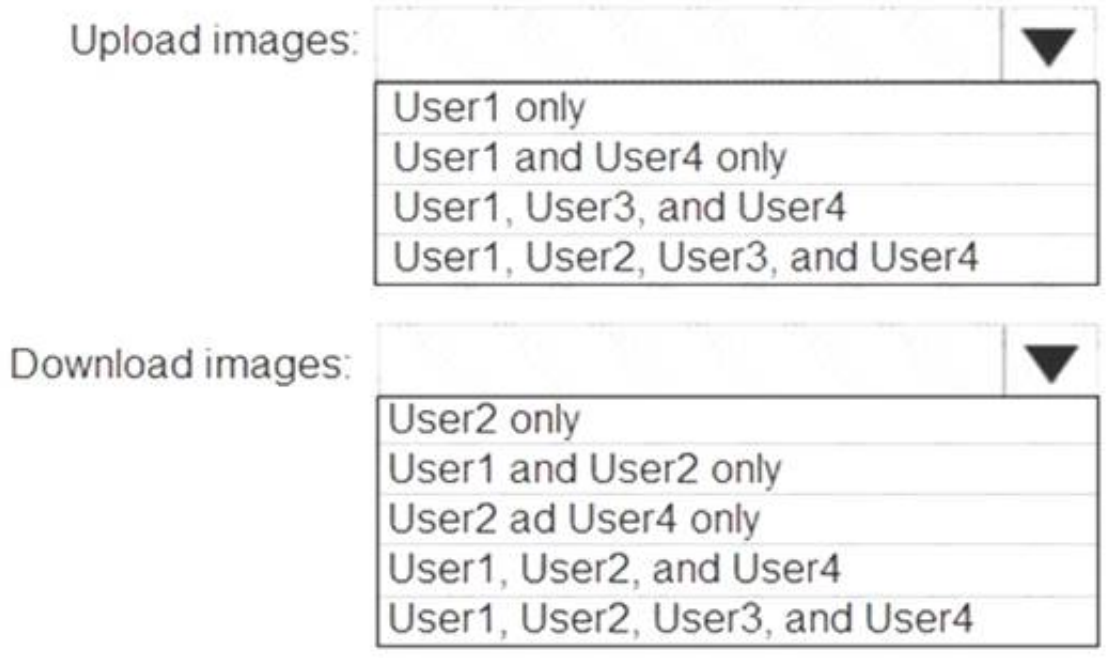
**Answer:** A

**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 234**
- (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 238**
- (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).

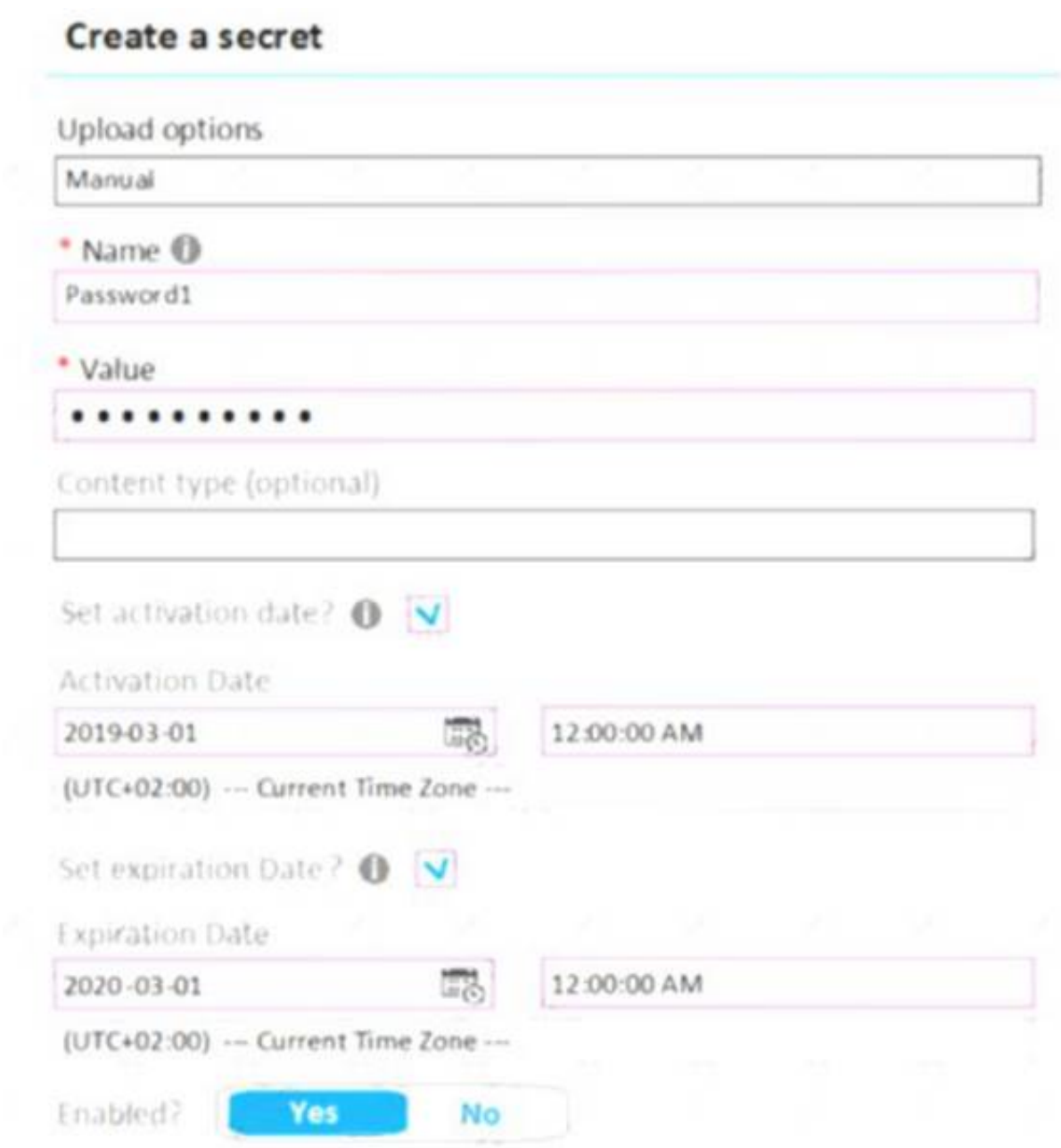
**Answer:** A

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

**NEW QUESTION 240**
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.

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

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




User2 is assigned an access policy to Vault1. The policy has the following configurations:

- Key Management Operations: Get, List, and Restore
- Cryptographic Operations: Decrypt and Unwrap Key
- Secret Management Operations: Get, List, and Restore

Group1 is assigned an access to Vault1. The policy has the following configurations:

- Key Management Operations: Get and Recover
- Secret Management Operations: List, Backup, and Recover

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

| Statements | Yes | No |
|---|---|---|
| On January 1, 2019, User1 can view the value of Password1. | ○ | ○ |
| On June 1, 2019, User2 can view the value of Password1. | ○ | ○ |
| On June 1, 2019, User1 can view the value of Password1. | ○ | ○ |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

| Statements | Yes | No |
|---|---|---|
| On January 1, 2019, User1 can view the value of Password1. | ○ | ○ |
| On June 1, 2019, User2 can view the value of Password1. | ○ | ○ |
| On June 1, 2019, User1 can view the value of Password1. | ○ | ○ |

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

| Name | Role |
|---|---|
| Admin1 | Global administrator |
| Admin2 | Group administrator |
| Admin3 | User administrator |

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

Users who can create a security group named Contoso Sales:

- Admin1 only
- Admin1 and Admin2 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3

Users who can create an Office 365 group named Contoso Sales:

- Admin1 only
- Admin1 and Admin2 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3

A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 246**
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Security Center for the centralized policy management of three Azure subscriptions. You use several policy definitions to manage the security of the subscriptions.
You need to deploy the policy definitions as a group to all three subscriptions.
Solution: You create an initiative and an assignment that is scoped to the Tenant Root Group management group.
Does this meet the goal?

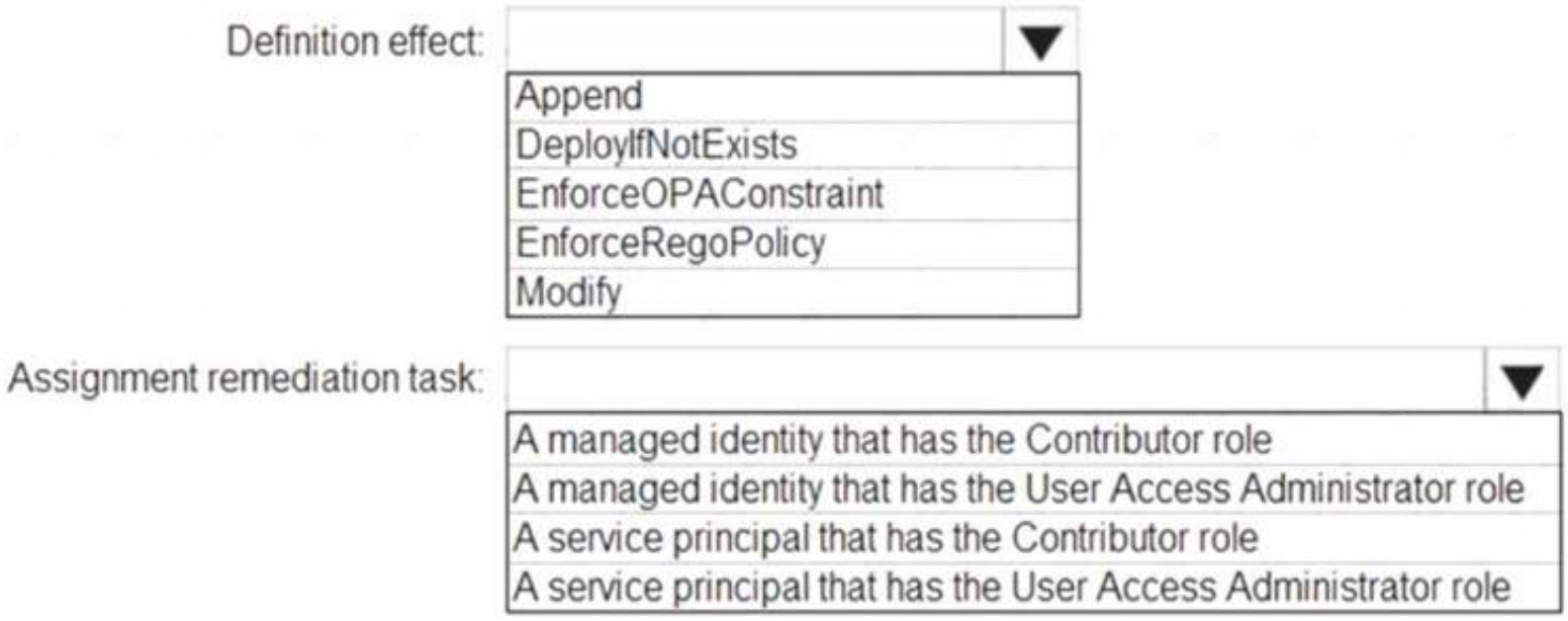
A. Yes
B. No

**Answer:** A

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

**NEW QUESTION 251**
- (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 256**
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Subscription named Sub1.
You have an Azure Storage account named Sa1 in a resource group named RG1.
Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.
You discover that unauthorized users accessed both the file service and the blob service. You need to revoke all access to Sa1.
Solution: You generate new SASs. Does this meet the goal?

A. Yes
B. No

**Answer:** B

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

**NEW QUESTION 259**
- (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 264**
- (Exam Topic 4)
You need to ensure that web11597200 is protected from malware by using Microsoft Antimalware for Virtual Machines and is scanned every Friday at 01:00. To complete this task, sign in to the Azure portal.

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
You need to install and configure the Microsoft Antimalware extension on the virtual machine named web11597200.

- In the Azure portal, type Virtual Machines in the search box, select Virtual Machines from the search results then select web11597200. Alternatively, browse to Virtual Machines in the left navigation pane.
- In the properties of web11597200, click on Extensions.
- Click the Add button to add an Extension.
- Scroll down the list of extensions and select Microsoft Antimalware.
- Click the Create button. This will open the settings pane for the Microsoft Antimalware Extension.
- In the Scan day field, select Friday.
- In the Scan time field, enter 60. The scan time is measured in minutes after midnight so 60 would be 01:00, 120 would be 02:00 etc.
- Click the OK button to save the configuration and install the extension.

**NEW QUESTION 269**
- (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 274**
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant named contoso.com
You need to configure diagnostic settings for contoso.com. The solution must meet the following requirements:
• Retain loqs for two years.
• Query logs by using the Kusto query language
• Minimize administrative effort. Where should you store the logs?

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

**Answer:** A

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

**NEW QUESTION 276**
- (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 280**
- (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 282**
- (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

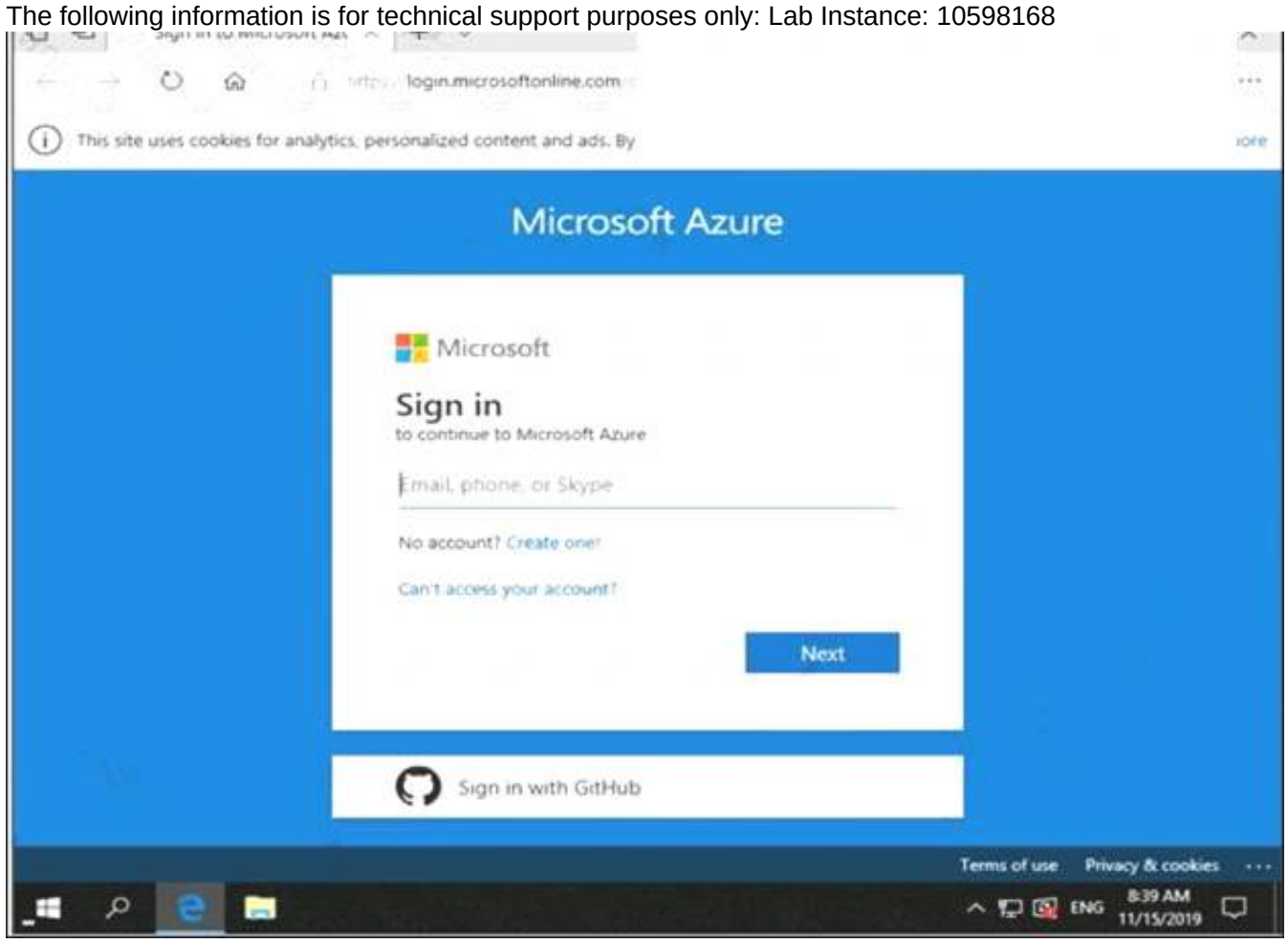
**Explanation:**
Reference:
https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity?tabs=dotnet

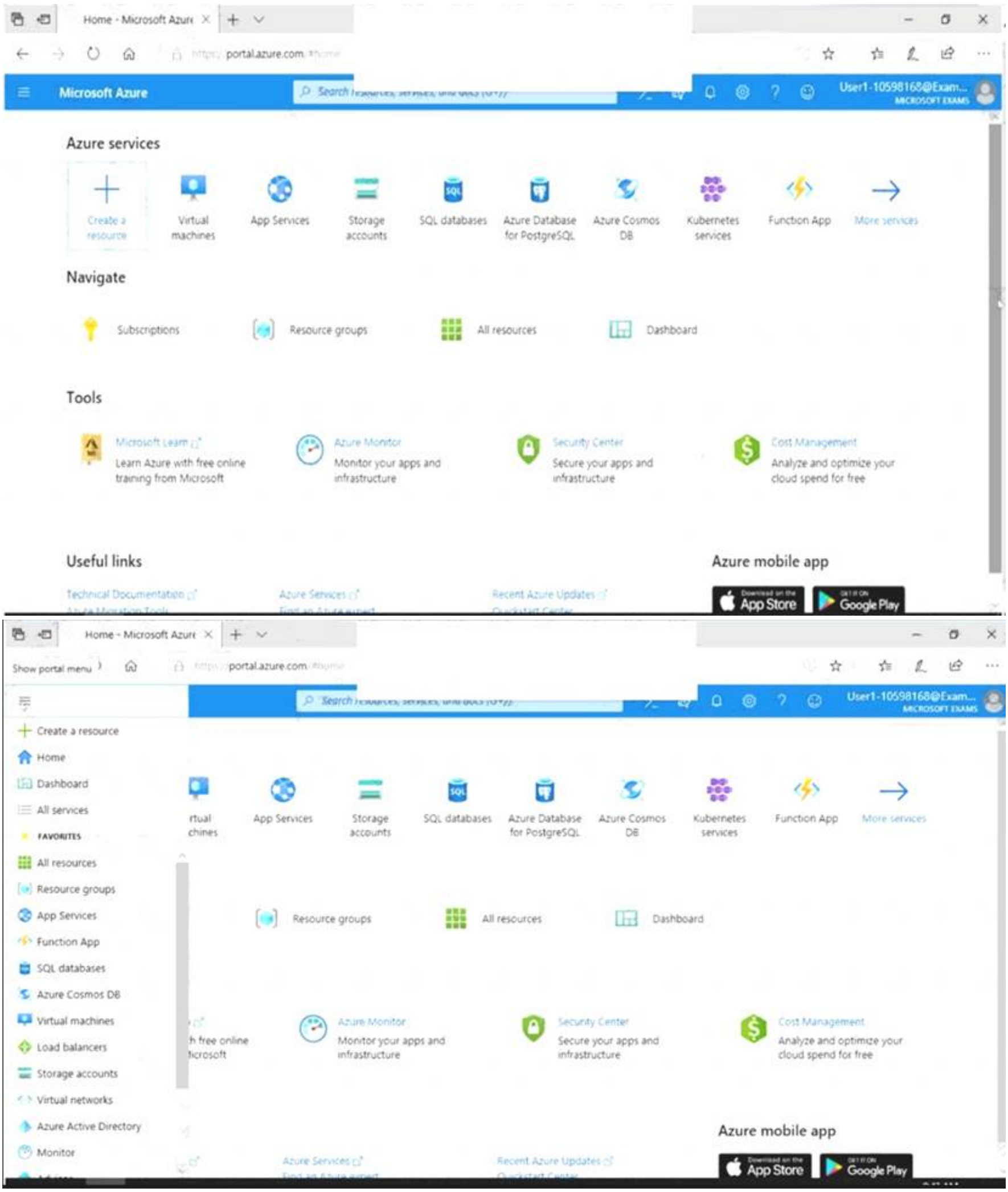
**NEW QUESTION 286**
- (Exam Topic 4)
You have an Azure subscription that uses Azure Active Directory (Azure AD) Privileged Identity Management (PIM).
A PIM user that is assigned the User Access Administrator role reports receiving an authorization error when performing a role assignment or viewing the list of assignments.
You need to resolve the issue by ensuring that the PIM service principal has the correct permissions for the subscription. The solution must use the principle of least privilege.
Which role should you assign to the PIM service principle?

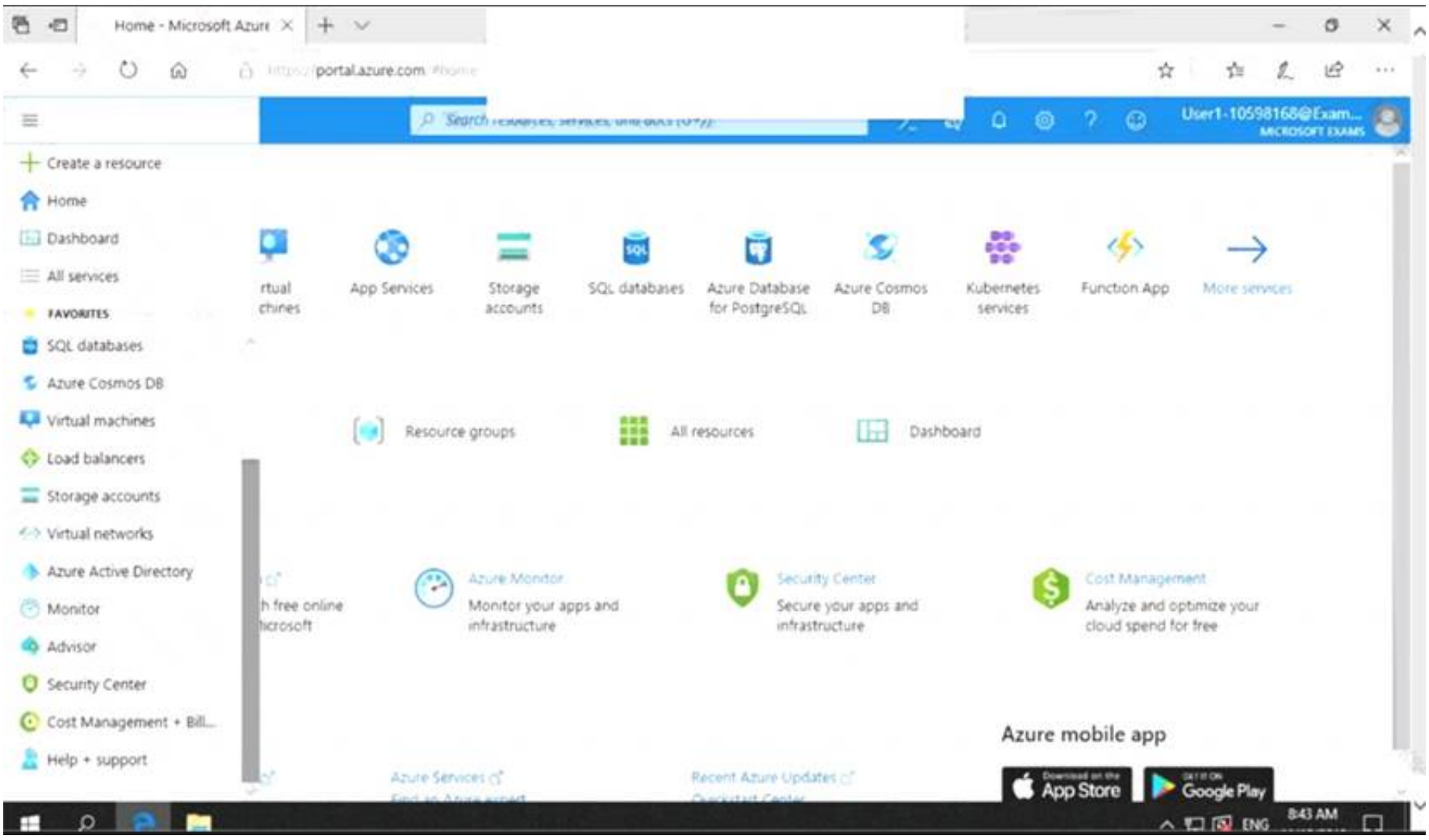
A. Contributor
B. User Access Administrator
C. Managed Application Operator
D. Resource Policy Contributor

**Answer:** B

**NEW QUESTION 290**
- (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

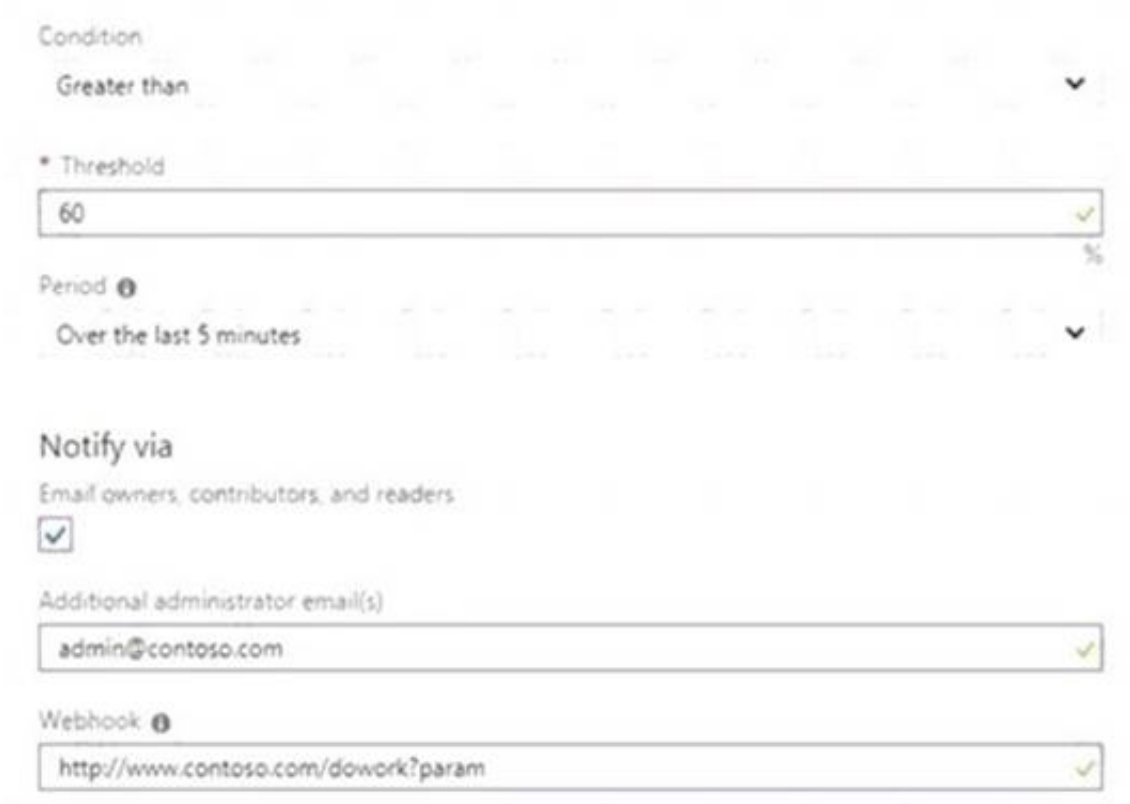



You need to email an alert to a user named admin1@contoso.com if the average CPU usage of a virtual machine named VM1 is greater than 70 percent for a period of 15 minutes.
To complete this task, sign in to the Azure portal.

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Create an alert rule on a metric with the Azure portal
* 1. In the portal, locate the resource, here VM1, you are interested in monitoring and select it.
* 2. Select Alerts (Classic) under the MONITORING section. The text and icon may vary slightly for different resources.
* 3. Select the Add metric alert (classic) button and fill in the fields as per below, and click OK. Metric: CPU Percentage
Condition: Greater than Period: Over last 15 minutes Notify via: email
Additional administrator email(s): admin1@contoso.com




Reference:
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-insights-alerts-portal

**NEW QUESTION 292**
- (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 296**
- (Exam Topic 4)
You have an Azure Sentinel workspace that contains an Azure Active Directory (Azure AD) connector, an Azure Log Analytics query named Query1 and a playbook named Playbook1.
Query1 returns a subset of security events generated by Azure AD.
You plan to create an Azure Sentinel analytic rule based on Query1 that will trigger Playbook1. You need to ensure that you can add Playbook1 to the new rule.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Create the rule and set the type to: [ ]
- Fusion
- Microsoft Security incident creation
- Scheduled

Configure the playbook to include: [ ]
- A managed connector
- A system-assigned managed identity
- A trigger
- Diagnostic settings

A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 298**
- (Exam Topic 4)
Your network contains an Active Directory forest named contoso.com. You have an Azure Directory (Azure AD) tenant named contoso.com.
You plan to configure synchronization by using the Express Settings installation option in Azure AD Connect. You need to identify which roles and groups are required to perform the planned configurations. The solution must use the principle of least privilege.
Which two roles and groups should you identify? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

**Answer:** CE

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

**NEW QUESTION 301**
- (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

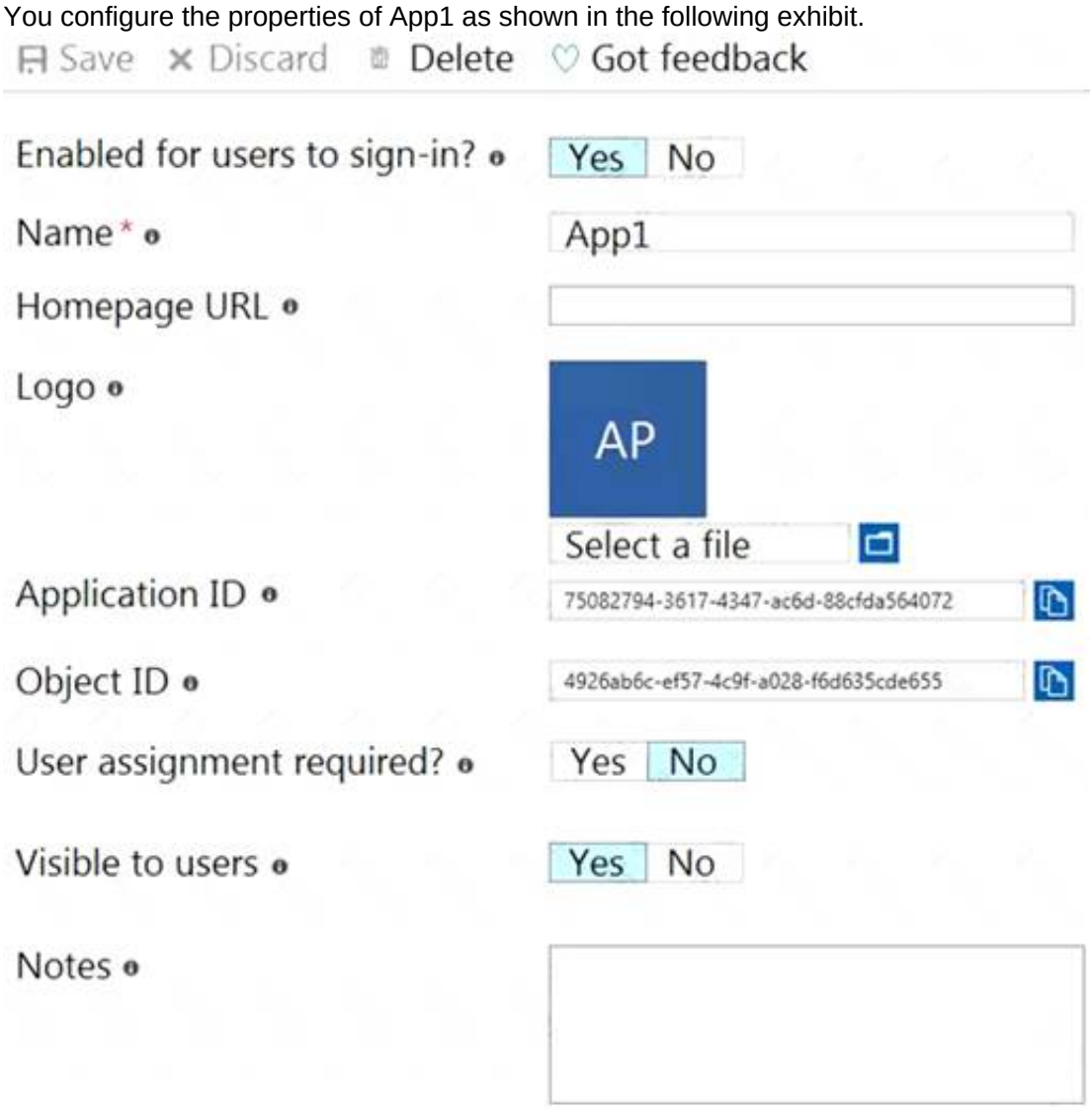
**Explanation:**
References:
https://docs.microsoft.com/en-us/azure/governance/policy/overview

**NEW QUESTION 302**
- (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 307**
- (Exam Topic 4)
You have an Azure subscription named Subcription1 that contains an Azure Active Directory (Azure AD) tenant named contosos.com and a resource group named RG1.
You create a custom role named Role1 for contoso.com.
You need to identify where you can use Role1 for permission delegation. What should you identify?

A. contoso.com only
B. contoso.com and RGT only
C. contoso.com and Subscription1 only
D. contoso.com, RG1, and Subcription1

**Answer:** A

**Explanation:**
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles

**NEW QUESTION 311**
- (Exam Topic 4)
You create resources in an Azure subscription as shown in the following table.

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

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

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

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

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

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


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

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

PS C:\>_
```

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

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

A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 314**
- (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 319**
- (Exam Topic 4)
You have 15 Azure virtual machines in a resource group named RG1. All virtual machines run identical applications.
You need to prevent unauthorized applications and malware from running on the virtual machines. What should you do?

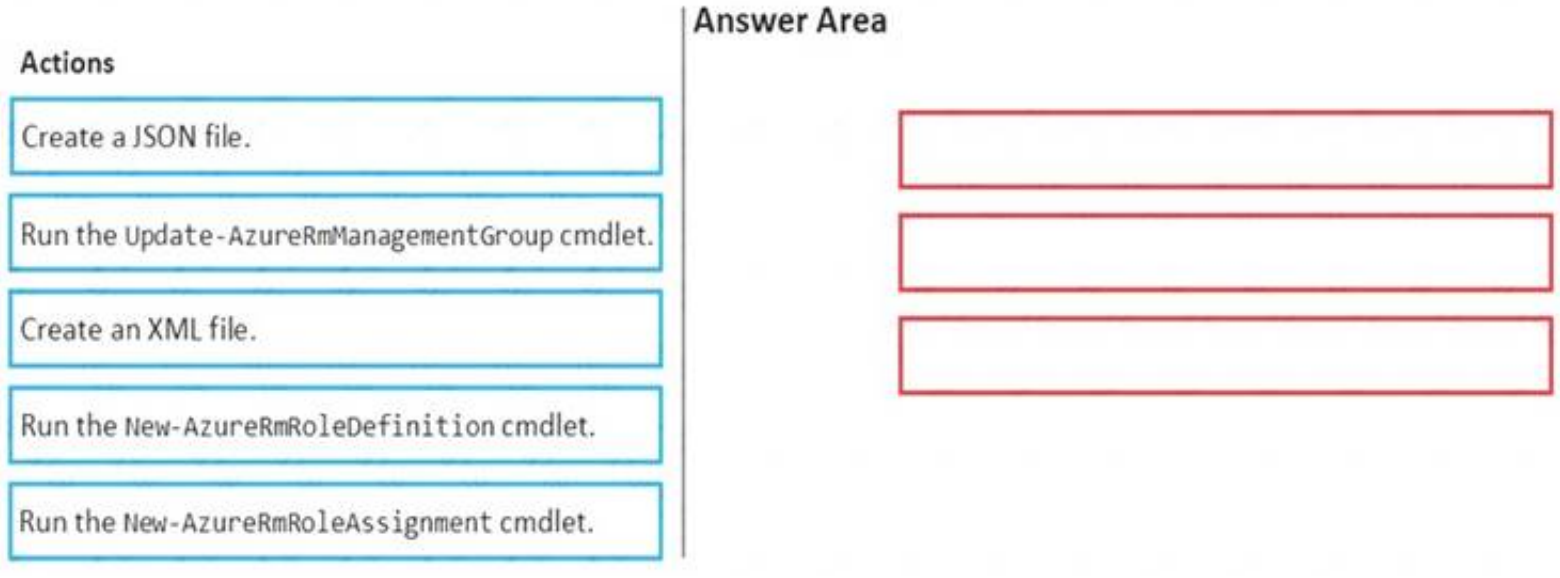
A. Apply an Azure policy to RG1.
B. From Azure Security Center, configure adaptive application controls.
C. Configure Azure Active Directory (Azure AD) Identity Protection.
D. Apply a resource lock to RG1.

**Answer:** B

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

**NEW QUESTION 324**
- (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.

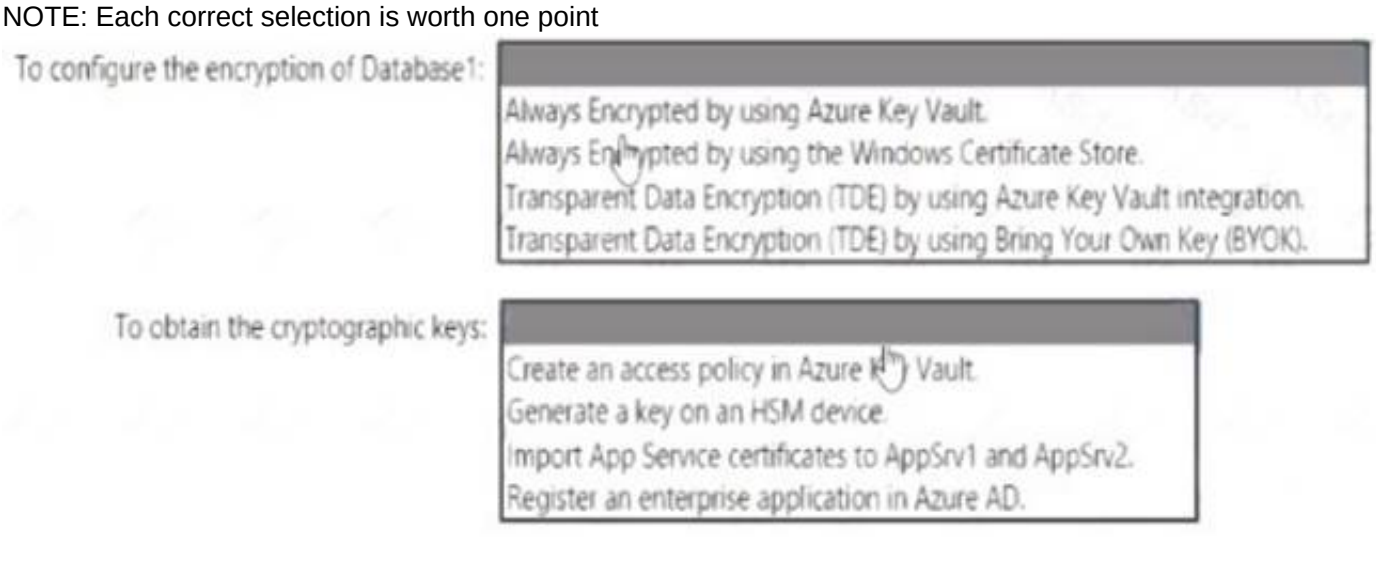



A. Mastered
B. Not Mastered

**Answer:** A

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

**NEW QUESTION 327**
- (Exam Topic 4)
You have an Azure subscription that contains the following resources:
• An Azure key vault
• An Azure SQL database named Database1
• Two Azure App Service web apps named AppSrv1 and AppSrv2 that are configured to use system-assigned managed identities and access Database1
You need to implement an encryption solution for Database1 that meets the following requirements:
• The data in a column named Discount in Database1 must be encrypted so that only AppSrv1 can decrypt the data.
• AppSrv1 and AppSrv2 must be authorized by using managed identities to obtain cryptographic keys. How should you configure the encryption settings fa Database1 To answer, select the appropriate options in
the answer area.
NOTE: Each correct selection is worth one point

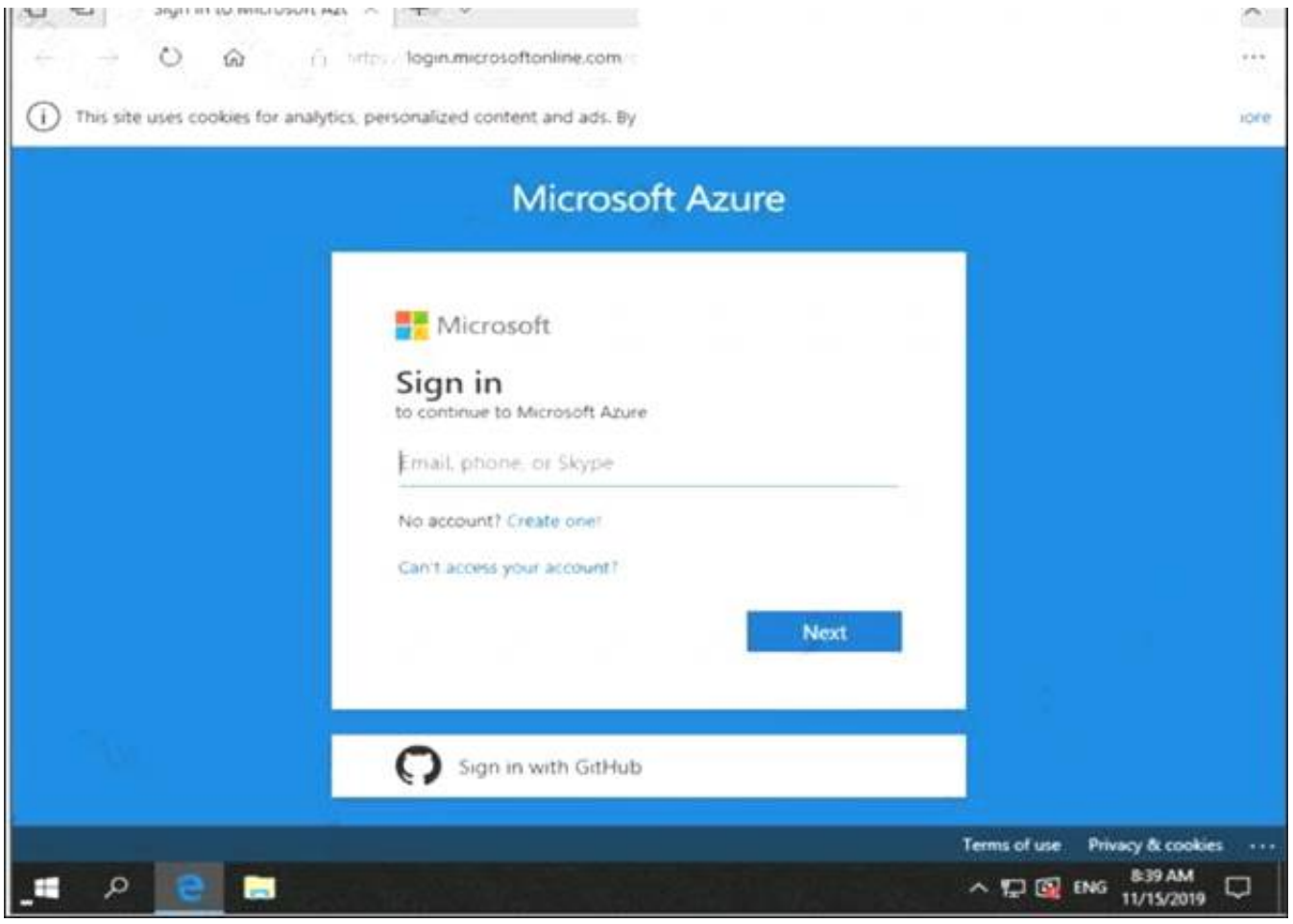


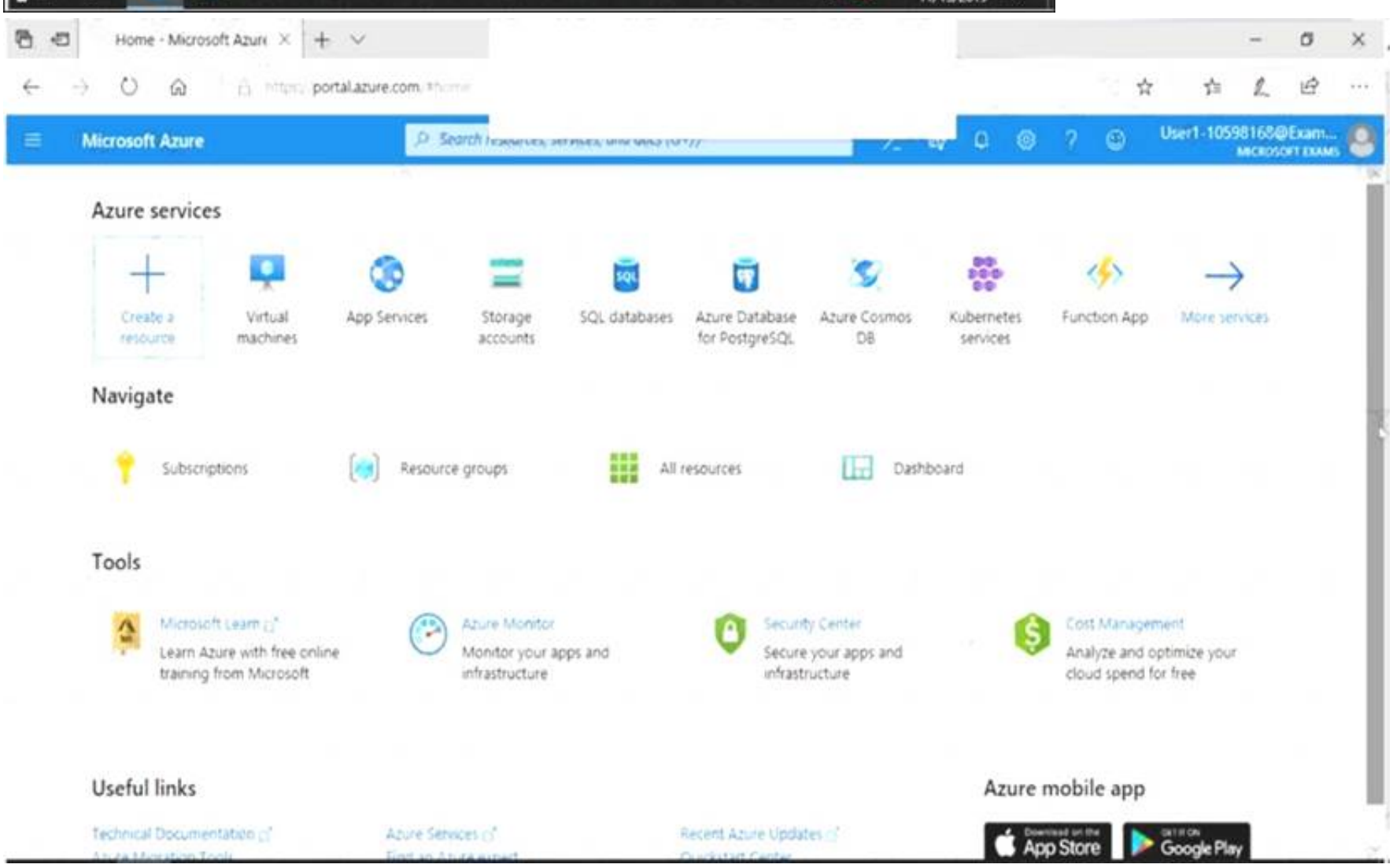

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Text Description automatically generated with medium confidence
Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/database/always-encrypted-azure-key-vault-configure?tabs=az

**NEW QUESTION 332**
- (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


login.microsoftonline.com
This site uses cookies for analytics, personalized content and ads. By
Microsoft Azure
Microsoft
Sign in
to continue to Microsoft Azure
Email, phone, or Skype
No account? Create one!
Can't access your account?
Next
Sign in with GitHub
Terms of use
Privacy & cookies
ENG
8:39 AM
11/15/2019

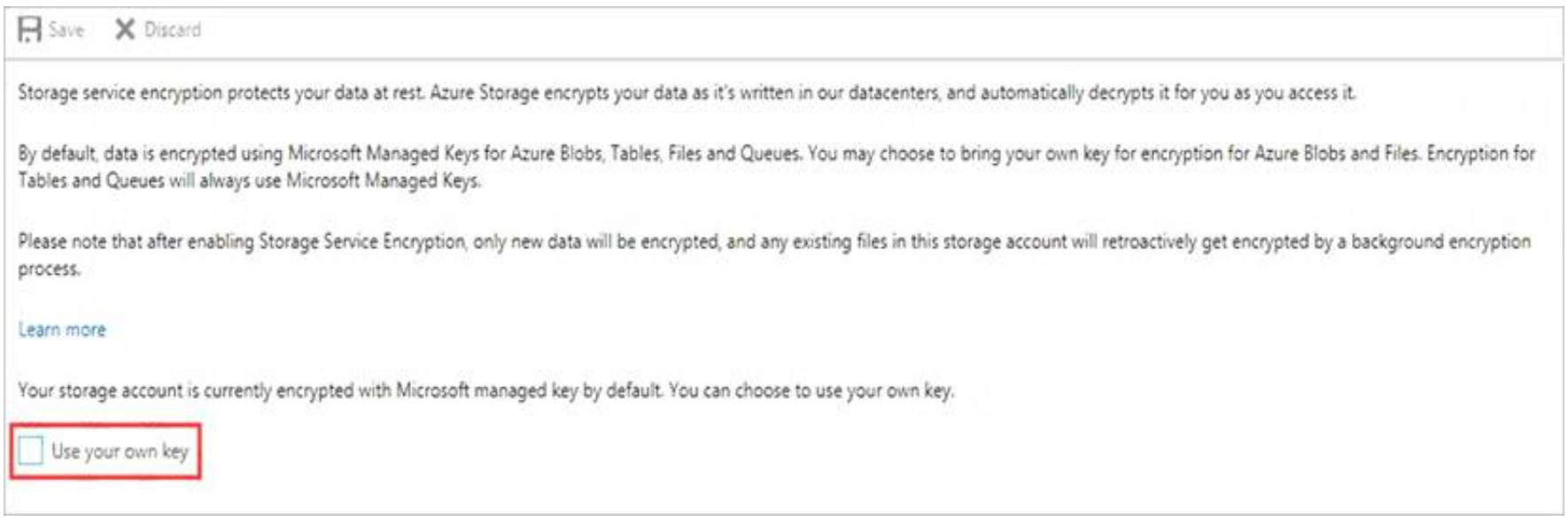

Home - Microsoft Azure
portal.azure.com
Microsoft Azure
User1-10598160@Exam...
MICROSOFT EXAMS
Azure services
Create a resource
Virtual machines
App Services
Storage accounts
SQL databases
Azure Database for PostgreSQL
Azure Cosmos DB
Kubernetes services
Function App
More services
Navigate
Subscriptions
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

You need to ensure that the rg1lod10598168n1 Azure Storage account is encrypted by using a key stored in the KeyVault10598168 Azure key vault.
To complete this task, sign in to the Azure portal.

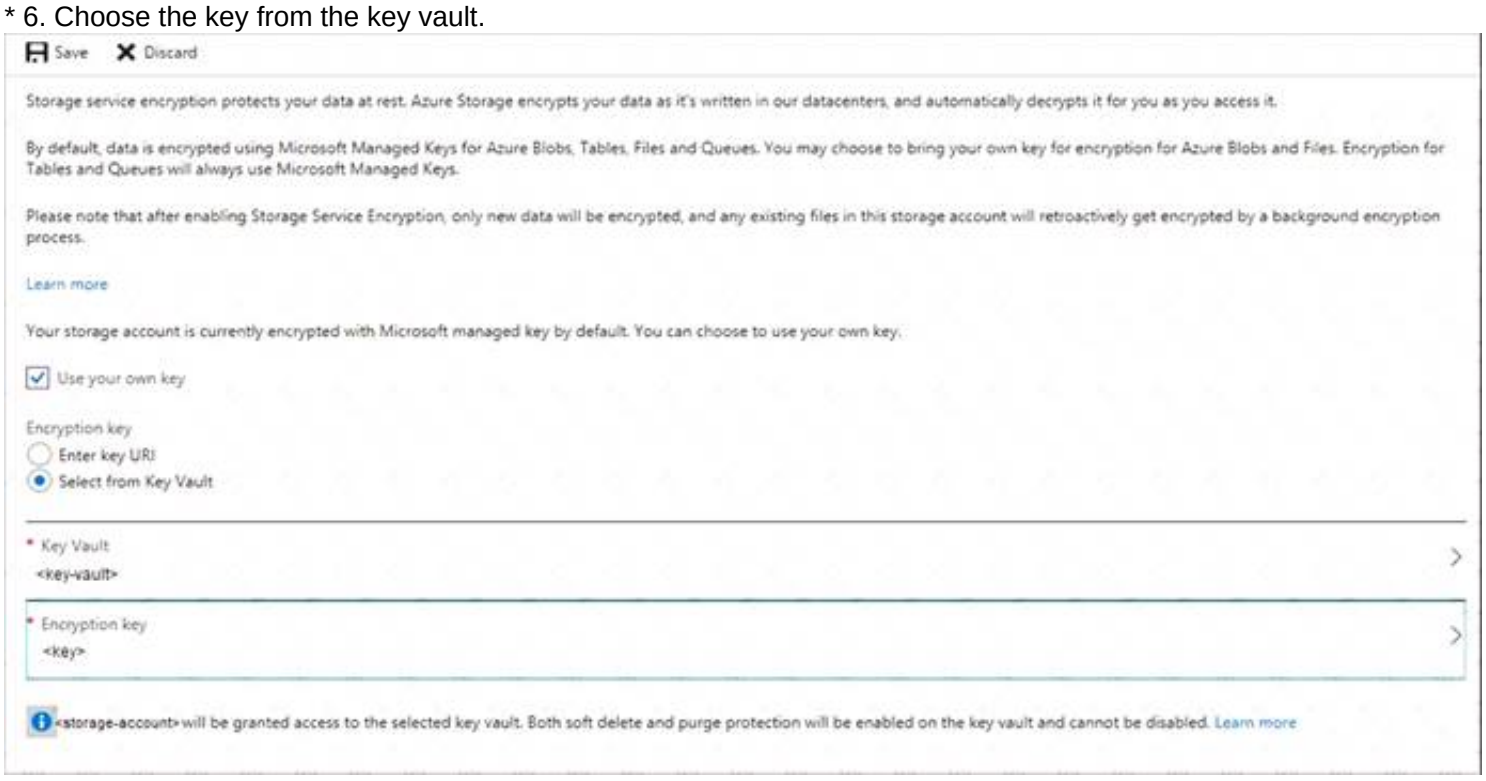
A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Step 1: To enable customer-managed keys in the Azure portal, follow these steps:
* 1. Navigate to your storage account rg1lod10598168n1
* 2. On the Settings blade for the storage account, click Encryption. Select the Use your own key option, as shown in the following figure.




Step 2: Specify a key from a key vault
To specify a key from a key vault, first make sure that you have a key vault that contains a key. To specify a key from a key vault, follow these steps:
* 4. Choose the Select from Key Vault option.
* 5. Choose the key vault KeyVault10598168 containing the key you want to use.
* 6. Choose the key from the key vault.




Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-encryption-keys-portal

**NEW QUESTION 335**
- (Exam Topic 4)
You have an Azure subscription that contains the custom roles shown in the following table.

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

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

| Name | Type |
|---|---|
| Role3 | Azure AD |
| Role4 | Azure subscription |

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

Role3:
- Role1 only
- Built-in Azure AD roles only
- Role1 and built-in Azure AD roles only
- Role1, built-in Azure AD roles, and built-in Azure subscription roles

Role4:
- Role2 only
- Built-in Azure AD roles only
- Role2 and built-in Azure subscription roles only
- Role2, built-in Azure subscription roles, and built-in Azure AD roles

A. Mastered
B. Not Mastered

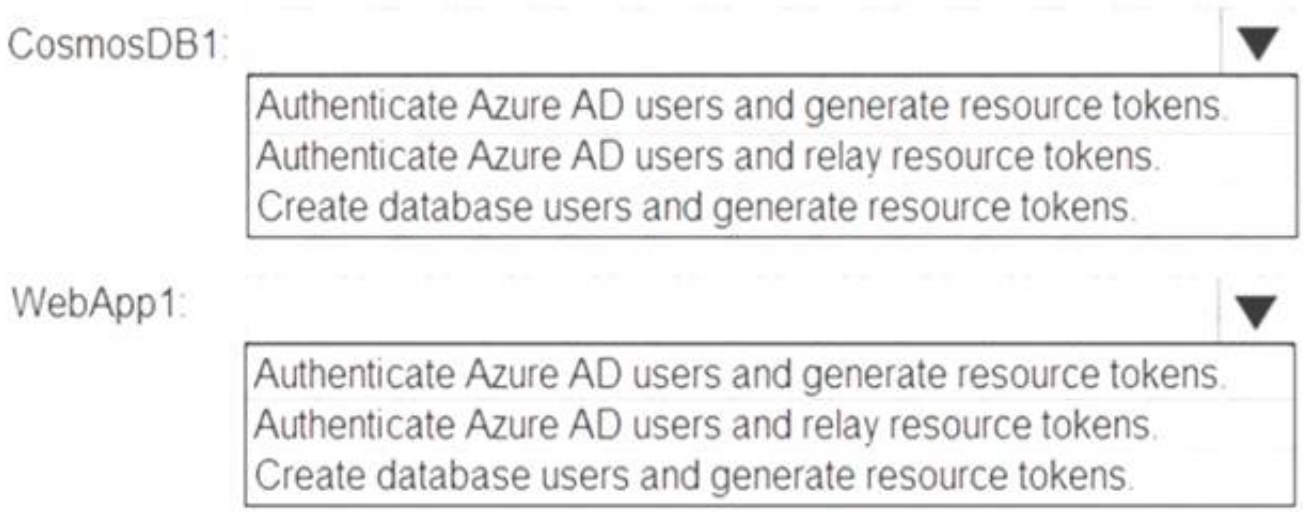
**Answer:** A

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

**NEW QUESTION 337**
- (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 plan to implement an application that will consist of the resources shown in the following table.

| Name | Type | Description |
|---|---|---|
| CosmosDBAccount1 | Azure Cosmos DB account | A Cosmos DB account containing a database Named CosmosDB1 that serves as a back-end tier of the application |
| WebApp1 | Azure web app | A web app configured to serve as the middle tier of the application |

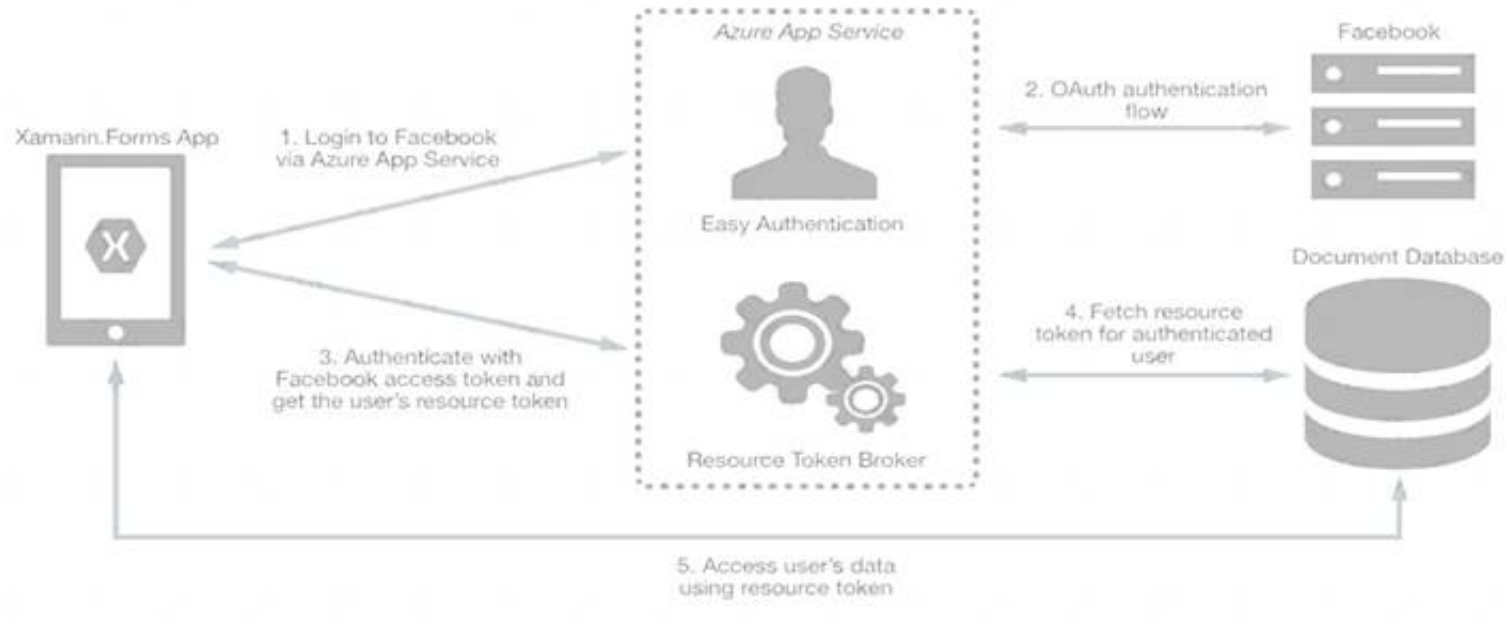
Users will authenticate by using their Azure AD user account and access the Cosmos DB account by using resource tokens.
You need to identify which tasks will be implemented in CosmosDB1 and WebApp1.
Which task should you identify for each resource? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.




A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
CosmosDB1: Create database users and generate resource tokens.
Azure Cosmos DB resource tokens provide a safe mechanism for allowing clients to read, write, and delete specific resources in an Azure Cosmos DB account according to the granted permissions.
WebApp1: Authenticate Azure AD users and relay resource tokens
A typical approach to requesting, generating, and delivering resource tokens to a mobile application is to use a resource token broker. The following diagram shows a high-level overview of how the sample application uses a resource token broker to manage access to the document database data:




References:
https://docs.microsoft.com/en-us/xamarin/xamarin-forms/data-cloud/cosmosdb/authentication

**NEW QUESTION 341**
- (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 344**
- (Exam Topic 4)
You have an app that uses an Azure SQL database.
You need to be notified if a SQL injection attack is launched against the database. What should you do?

A. Modify the Diagnostics settings for the database.
B. Deploy the SQL Health Check solution in Azure Monitor.
C. Enable Azure Defender for SQL for the database.
D. Enable server-level auditing for the database.

**Answer:** C

**NEW QUESTION 348**
.....

# THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual az-500 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the az-500 Product From:

**https://www.2passeasy.com/dumps/az-500/**

## Money Back Guarantee

### 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