az-500 Dumps

Microsoft Azure Security Technologies

https://www.certleader.com/az-500-dumps.html
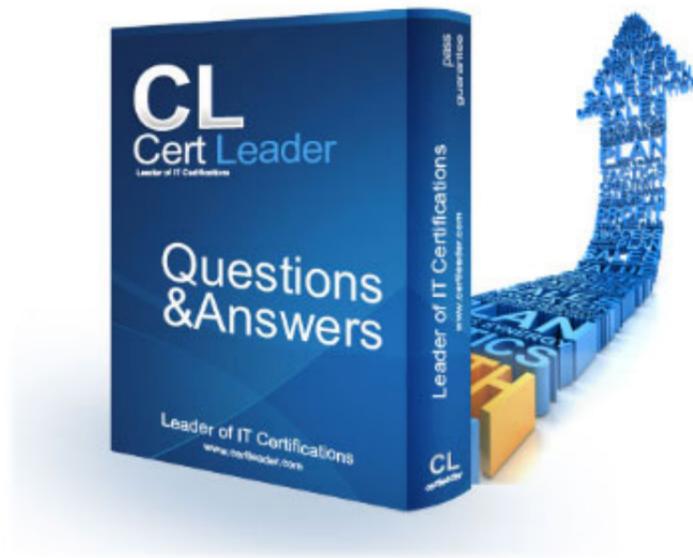
NEW QUESTION 1
- (Exam Topic 4)
You plan to deploy Azure container instances.
You have a containerized application that validates credit cards. The application is comprised of two containers: an application container and a validation container.
The application container is monitored by the validation container. The validation container performs security checks by making requests to the application container and waiting for responses after every transaction.
You need to ensure that the application container and the validation container are scheduled to be deployedtogether. The containers must communicate to each other only on ports that are not externally exposed.
What should you include in the deployment?

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

Answer: D

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


NEW QUESTION 2
- (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
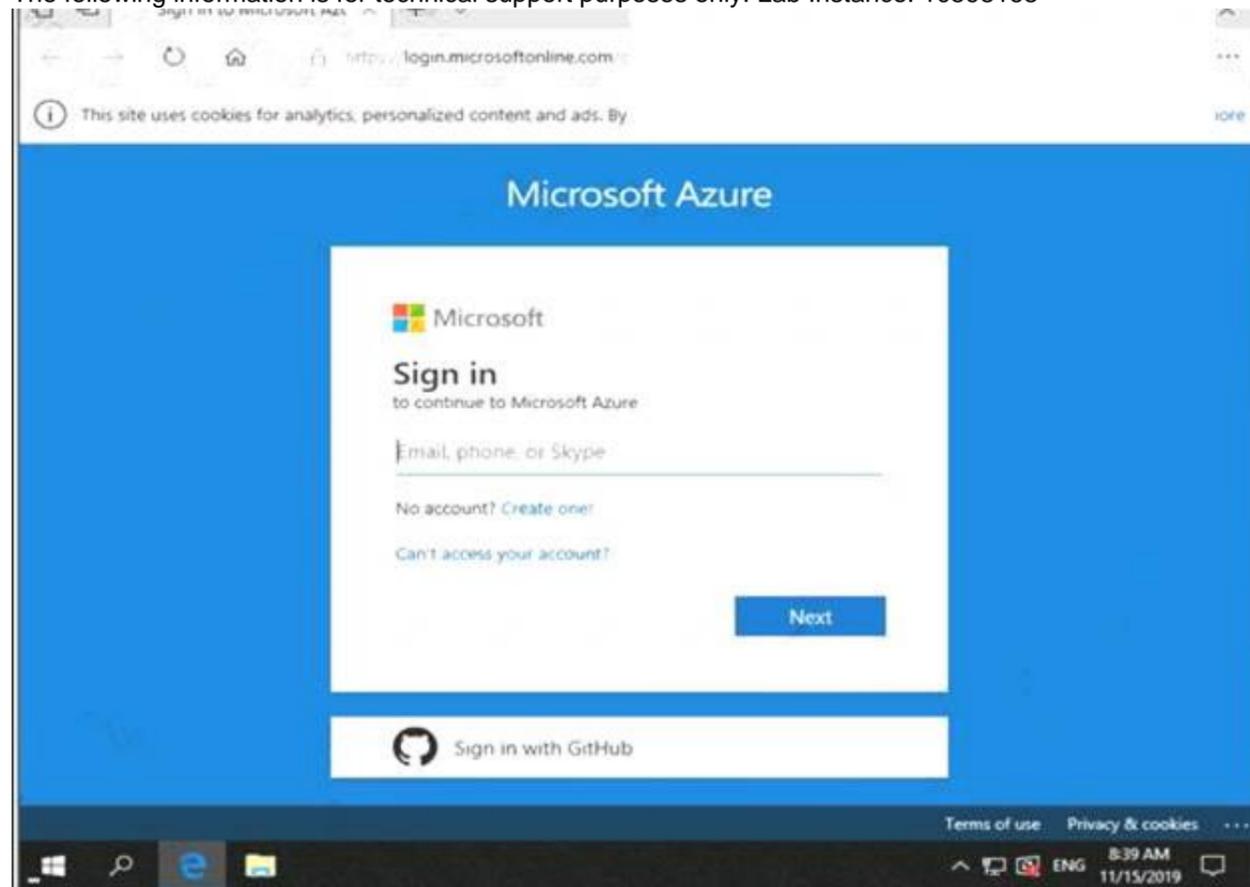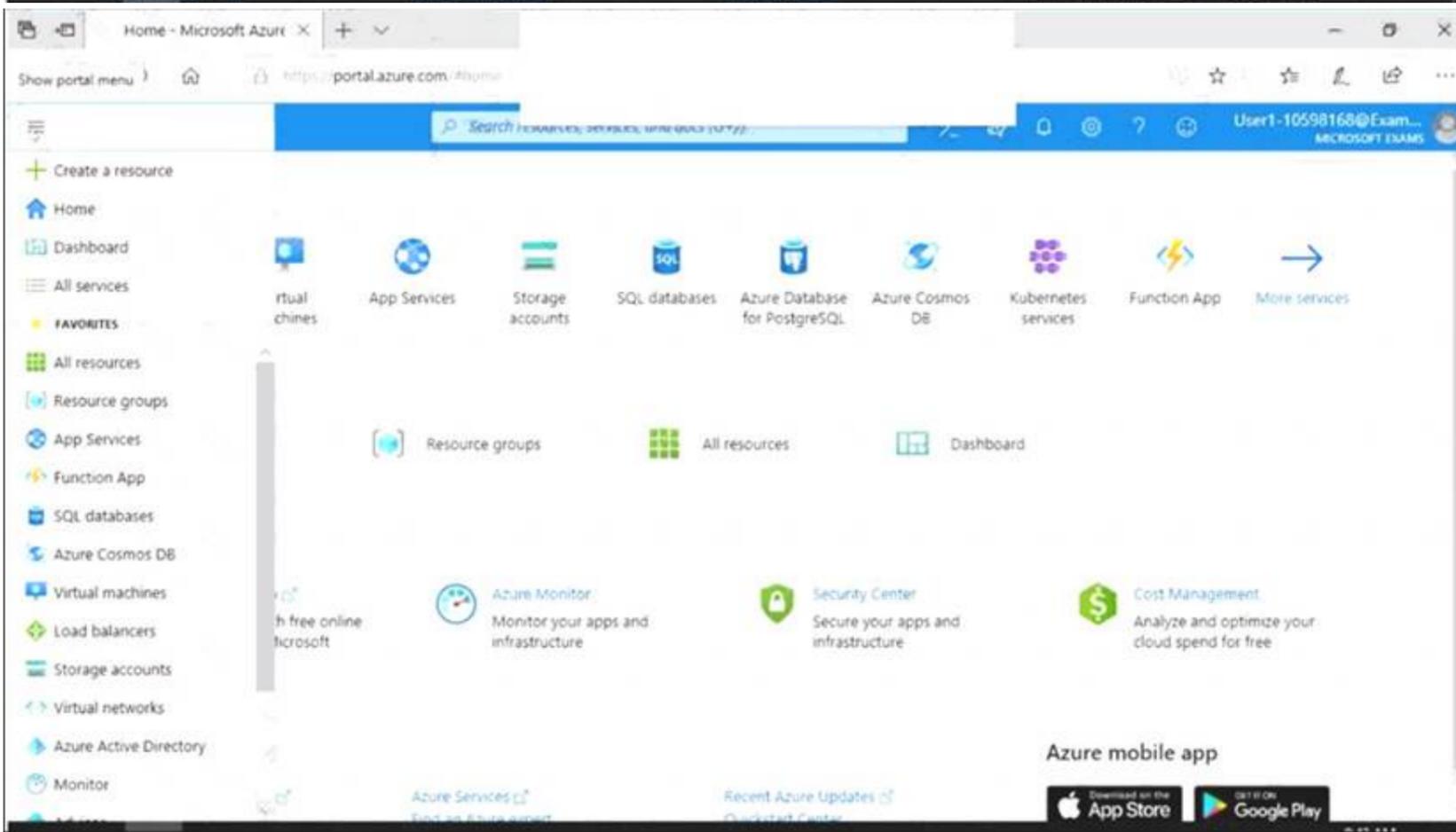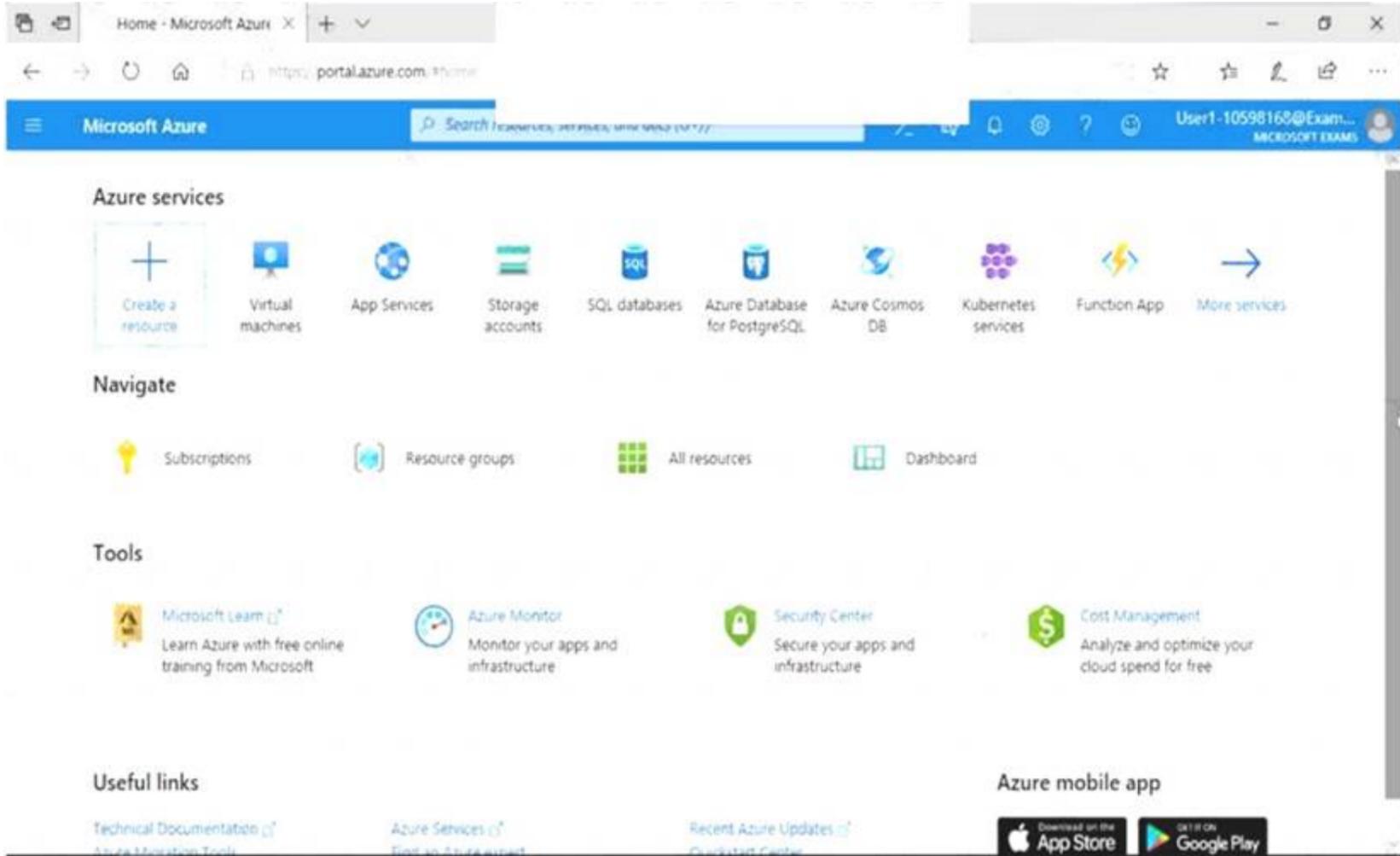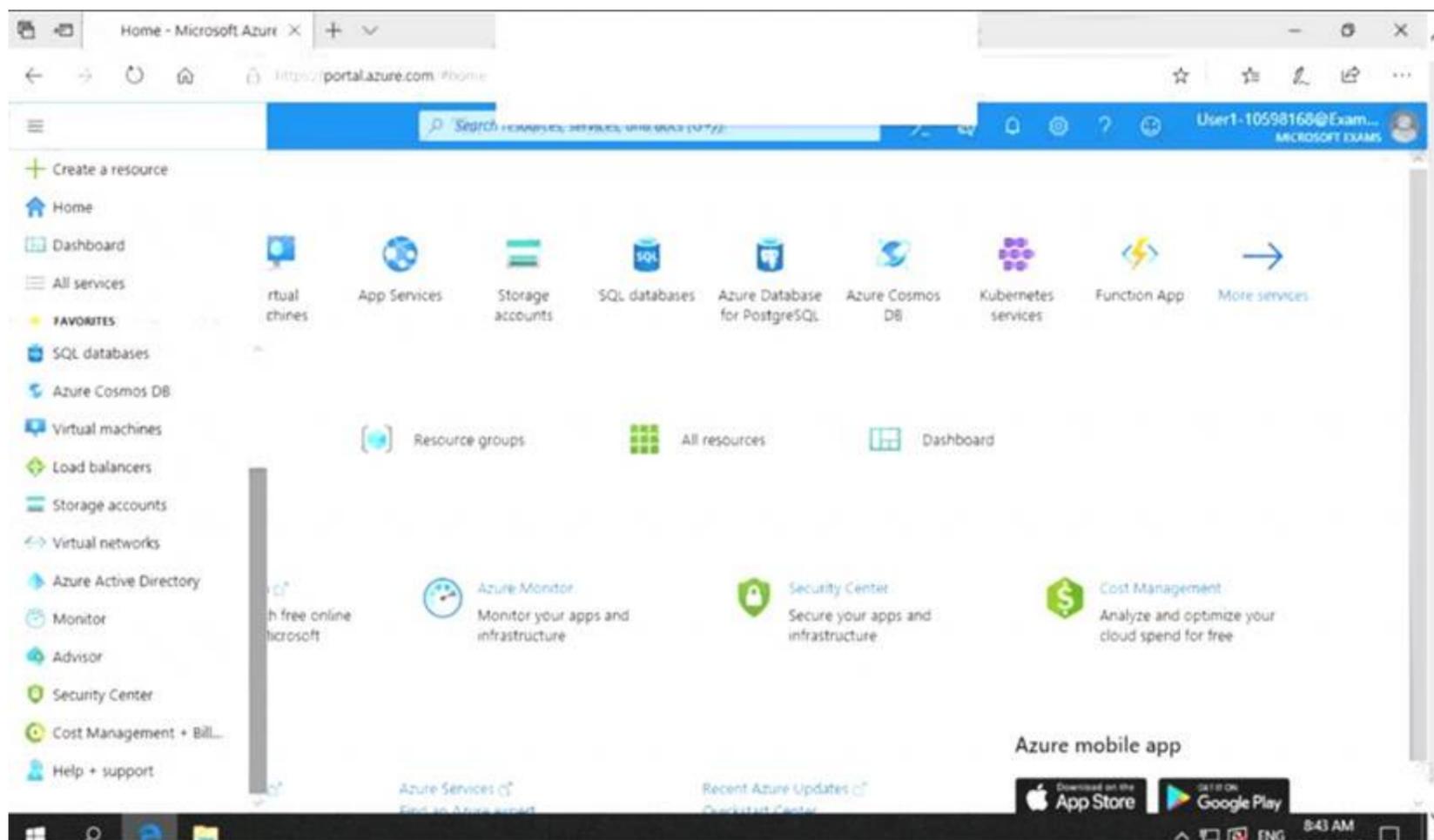
You need to prevent HTTP connections to the rg1lod10598168n1 Azure Storage account. To complete this task, sign in to the Azure portal.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
The "Secure transfer required" feature is now supported in Azure Storage account. This feature enhances the security of your storage account by enforcing all requests to your account through a secure connection. This feature is disabled by default.
* 1. In Azure Portal select you Azure Storage account rg1lod10598168n1.
* 2. Select Configuration, and Secure Transfer required.

Reference:
https://techcommunity.microsoft.com/t5/Azure/quot-Secure-transfer-required-quot-is-available-in-Azure-Storag
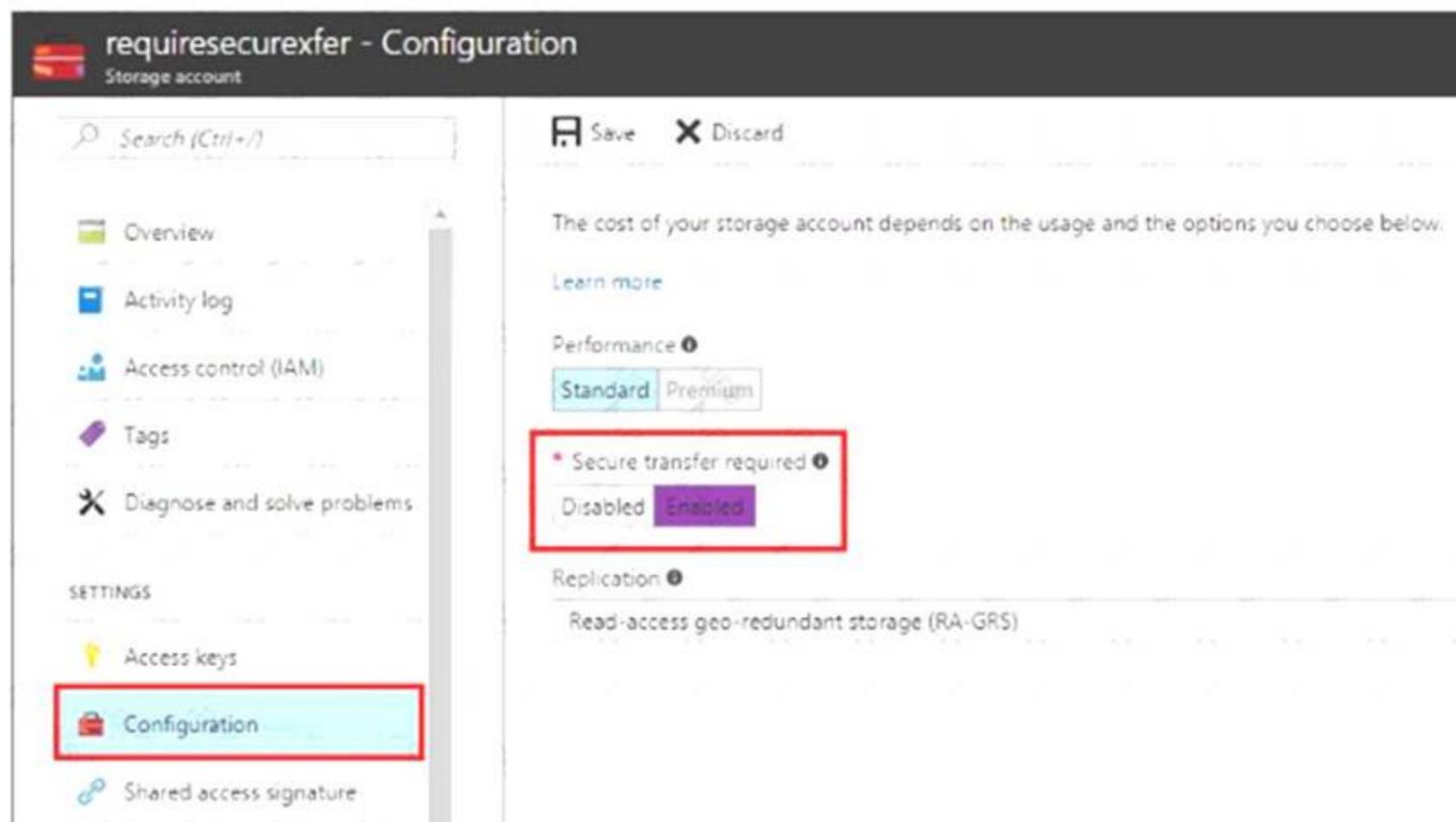
NEW QUESTION 3
- (Exam Topic 4)
Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD).
The Azure AD tenant contains the users shown in the following table.

Name	Source	Password
User1	Azure AD	Adatum123
User2	Azure AD	N3w3rT0Gue33
User3	On-premises Active Directory	ComplexPassword33

You configure the Authentication methods – Password Protection settings for adatum.com as shown in the following exhibit.

Custom smart lockout

Lockout threshold ❶   10   ✓

Lockout duration in seconds ❶   60   ✓

Custom banned passwords

Enforce custom list ❶ | **Yes** | No |

Adatum   ✓

Custom banned password list ❶

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ❶ | **Yes** | No |

Mode ❶ | Enforced | **Audit** |

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 will be prompted to change the password on the next sign-in.	○	○
User2 can change the password to @d@tum_C0mpleX123.	○	○
User3 can change the password to Adatum123!.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Text Description automatically generated
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-de https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad

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

≫ Identify the user who deleted a virtual machine three weeks ago.

≫ Query the security events of a virtual machine that runs Windows Server 2016.

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

Settings	Answer Area
Activity log	
Logs	Identify the user who deleted a virtual machine three weeks ago: [ ]
Metrics	Query the security events of a virtual machine that runs Windows Server 2016: [ ]
Service Health	

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 5
- (Exam Topic 4)
You have an Azure Active Din-dory (Azure AD) tenant named contoso.com that contains a user named User1. You plan to publish several apps in the tenant.
You need to ensure that User1 can grant admin consent for the published apps.
Which two possible user roles can you assign to User! to achieve this goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

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

Answer: CE

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

NEW QUESTION 6
- (Exam Topic 4)
You have an Azure subscription that contains an Azure key vault and an Azure Storage account. The key vault contains customer-managed keys. The storage account is configured to use the customer-managed keys stored In the key vault.
You plan to store data in Azure by using the following services:
* Azure Files
* Azure Blob storage
* Azure Log Analytics
* Azure Table storage
* Azure Queue storage
Which two services data encryption by using the keys stored in the key vault? Each correct answer present a complete solution.
NOTE: Each correct selection is worth one point.

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

Answer: AC

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

NEW QUESTION 7
- (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
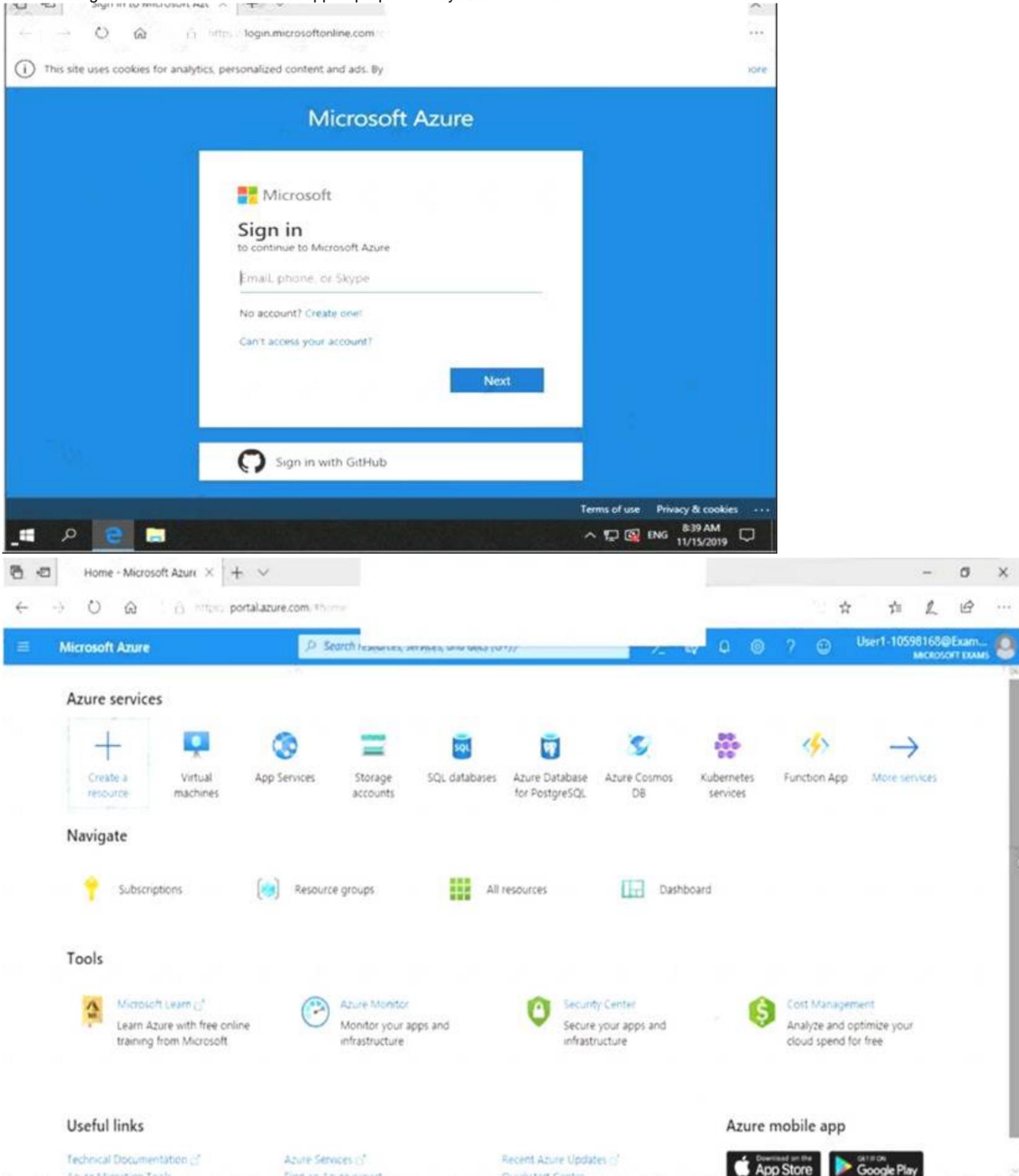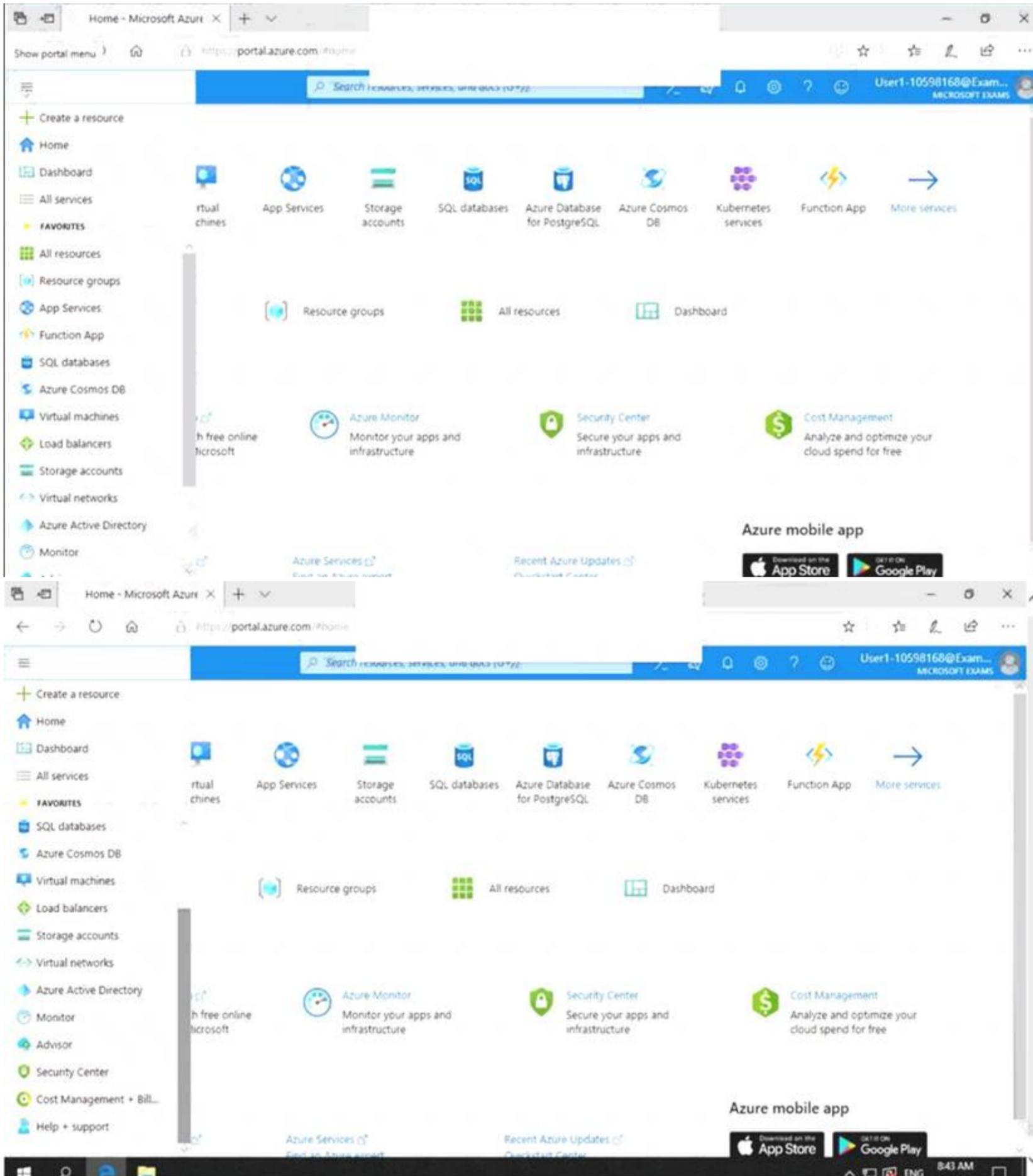
You need to perform a full malware scan every Sunday at 02:00 on a virtual machine named VM1 by using Microsoft Antimalware for Virtual Machines.
To complete this task, sign in to the Azure portal.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Deploy the Microsoft Antimalware Extension using the Azure Portal for single VM deployment
* 1. In Azure Portal, go to the Azure VM1's blade, navigate to the Extensions section and press Add.

Dashboard > Virtual machines > devrgvm > devrg > devrgvm - Extensions

devrgvm - Extensions
Virtual machine

Search (Ctrl+/)

+ Add

Search to filter items...

NAME ↑	TYPE
CustomScriptExtension	Microsoft.Compute.CustomScriptEx
DependencyAgentWindows	Microsoft.Azure.Monitoring.Depend
enablevmaccess	Microsoft.Compute.VMAccessAgen
IaaSDiagnostics	Microsoft.Azure.Diagnostics.IaaSDi
MicrosoftMonitoringAgent	Microsoft.EnterpriseCloud.Monitori
SiteRecovery-Windows	Microsoft.Azure.RecoveryServices.S

Left navigation:
- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings
- Networking
- Disks
- Size
- Security
- **Extensions**

* 2. Select the Microsoft Antimalware extension and press Create.
* 3. Fill the "Install extension" form as desired and press OK. Scheduled: EnableScan type: FullScan day: Sunday

Dashboard > Virtual machines > devrgvm > devrg > devrgvm - Extensions > New resource

Install extension

Excluded files and locations ⓘ

Excluded file extensions ⓘ

Excluded processes ⓘ

Real-time protection ⓘ

| Enable | Disable |

Run a scheduled scan ⓘ

| Enable | Disable |

Scan type ⓘ

| Quick | Full |

Scan day ⓘ

Saturday ⌄

Scan time ⓘ

120

OK

Reference:
https://www.e-apostolidis.gr/microsoft/azure/azure-vm-antimalware-extension-management/

NEW QUESTION 8
- (Exam Topic 4)
You have an Azure subscription linked to an Azure Active Directory Premium Plan 1 tenant. You plan to implement Azure Active Directory (Azure AD) Identity Protection.
You need to ensure that you can configure a user risk policy and a sign-in risk policy. What should you do first?

A. Purchase Azure Active Directory Premium Plan 2 licenses for all users.
B. Register all users for Azure Multi-Factor Authentication (MFA).
C. Enable security defaults for Azure AD.
D. Upgrade Azure Security Center to the standard tier.

Answer: A

Explanation:
Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa

NEW QUESTION 9
- (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
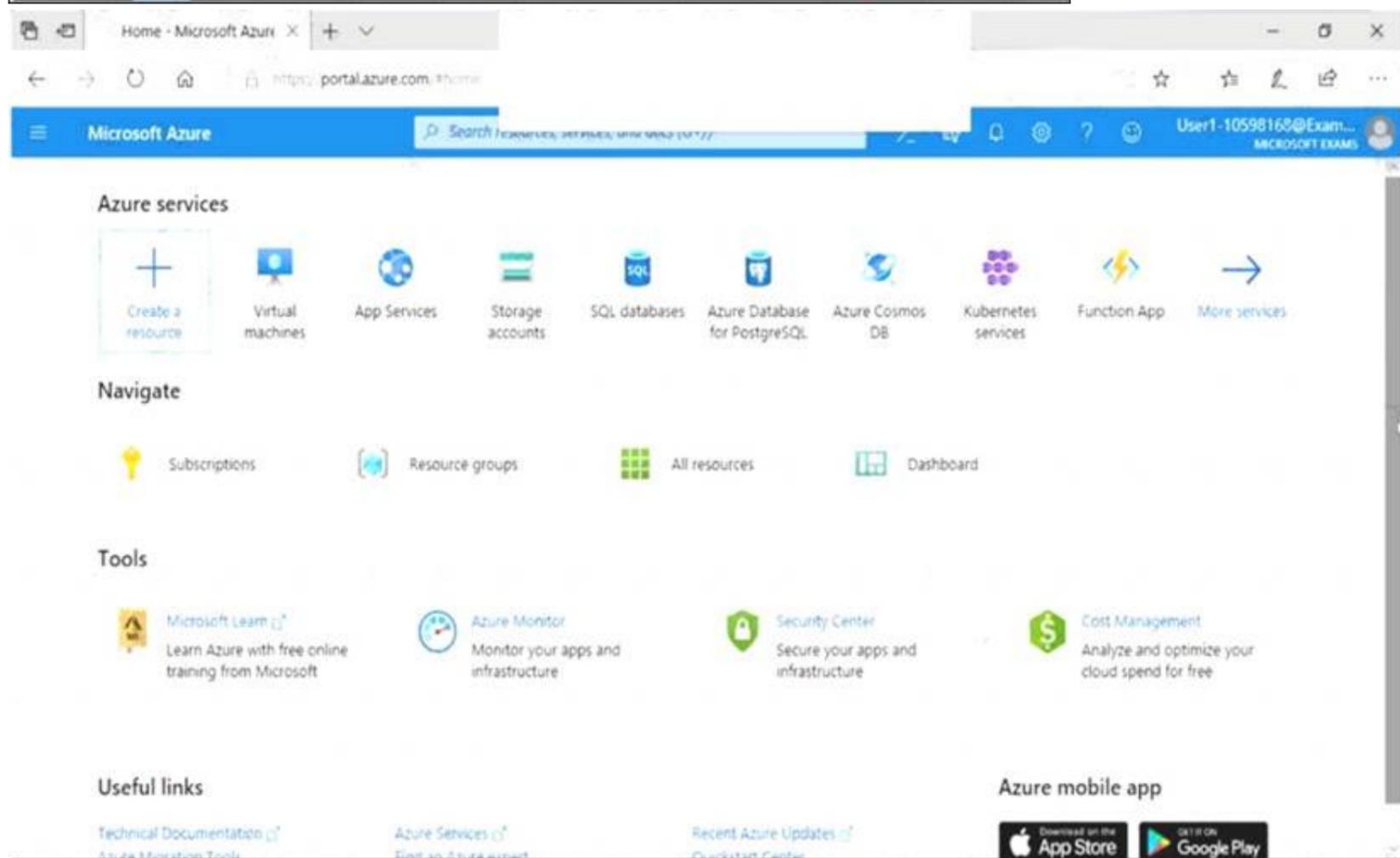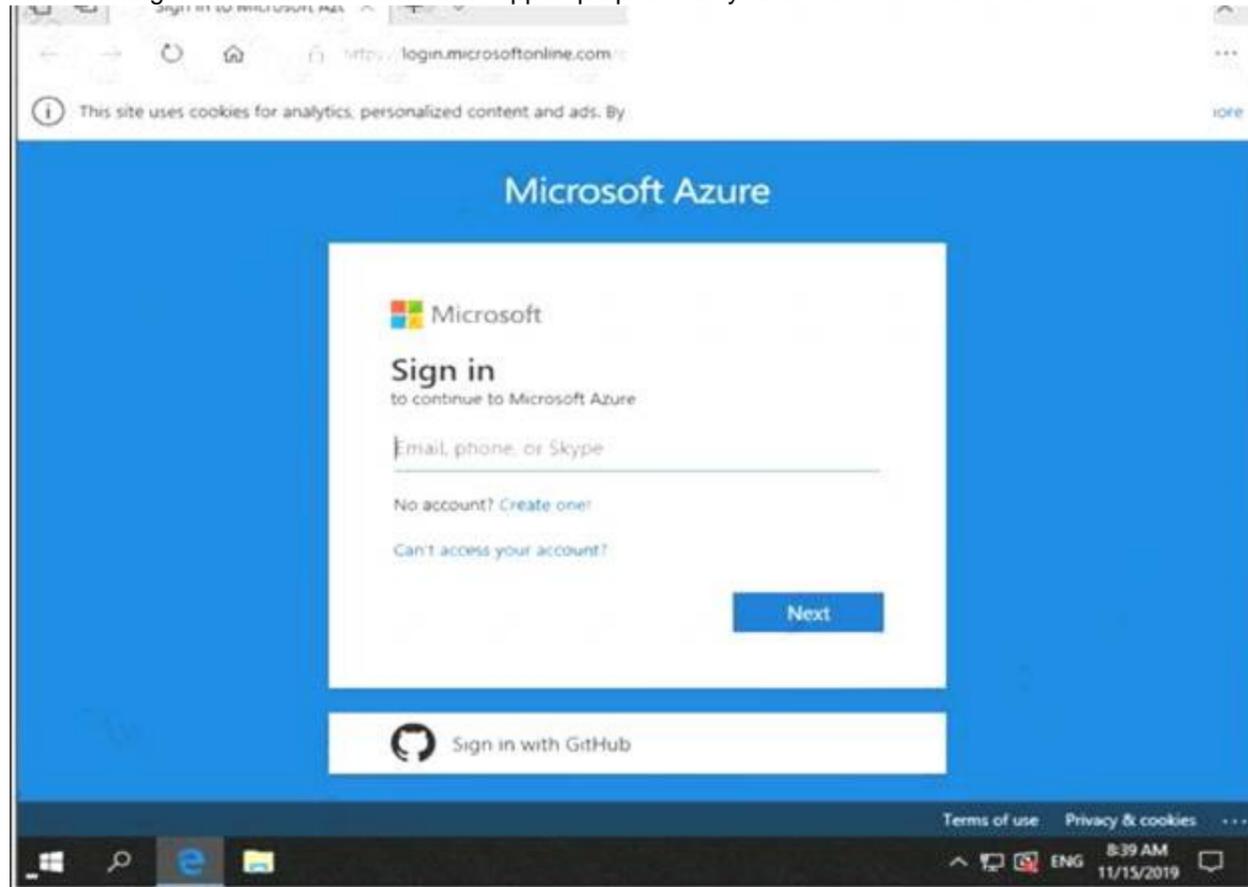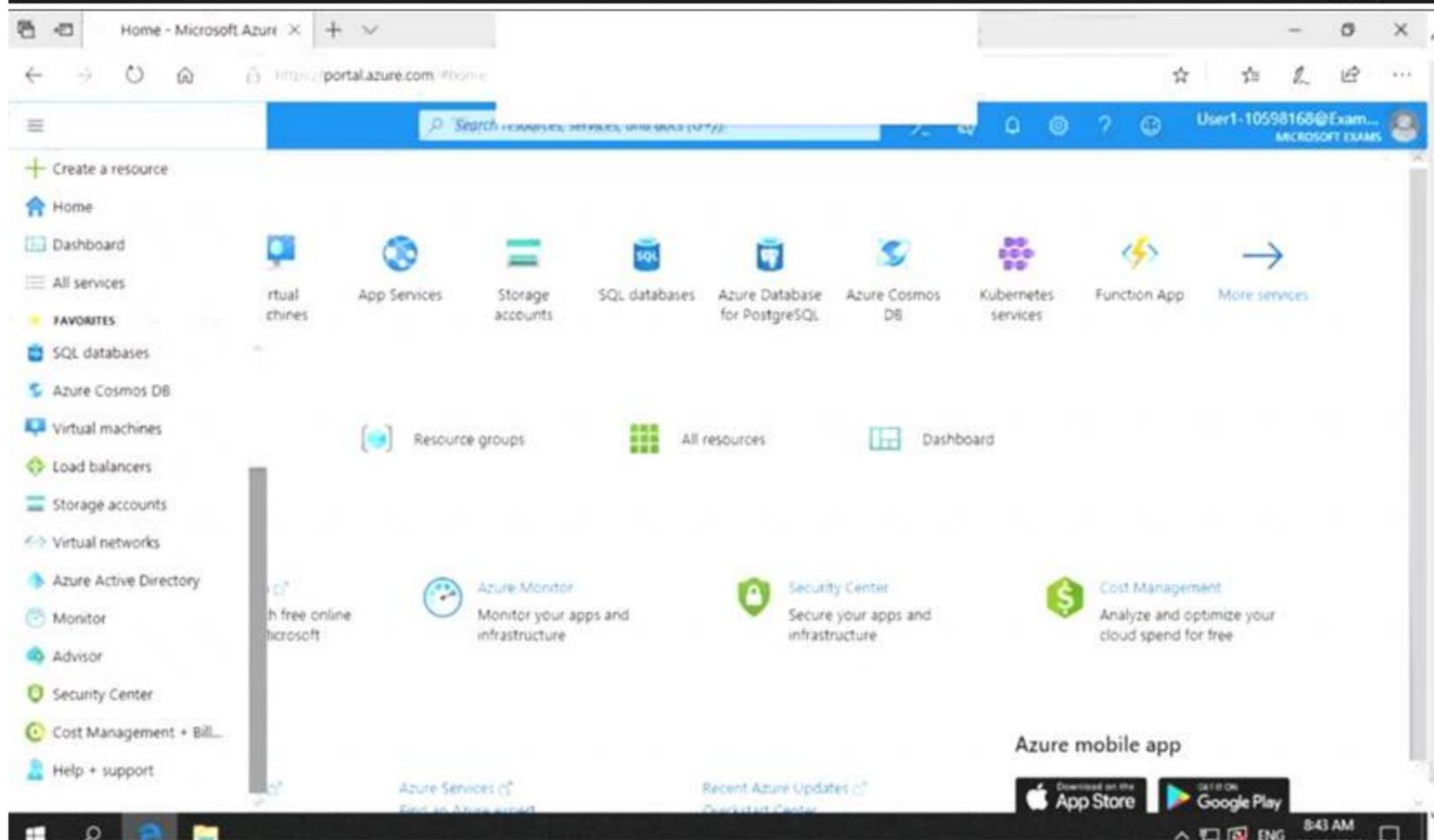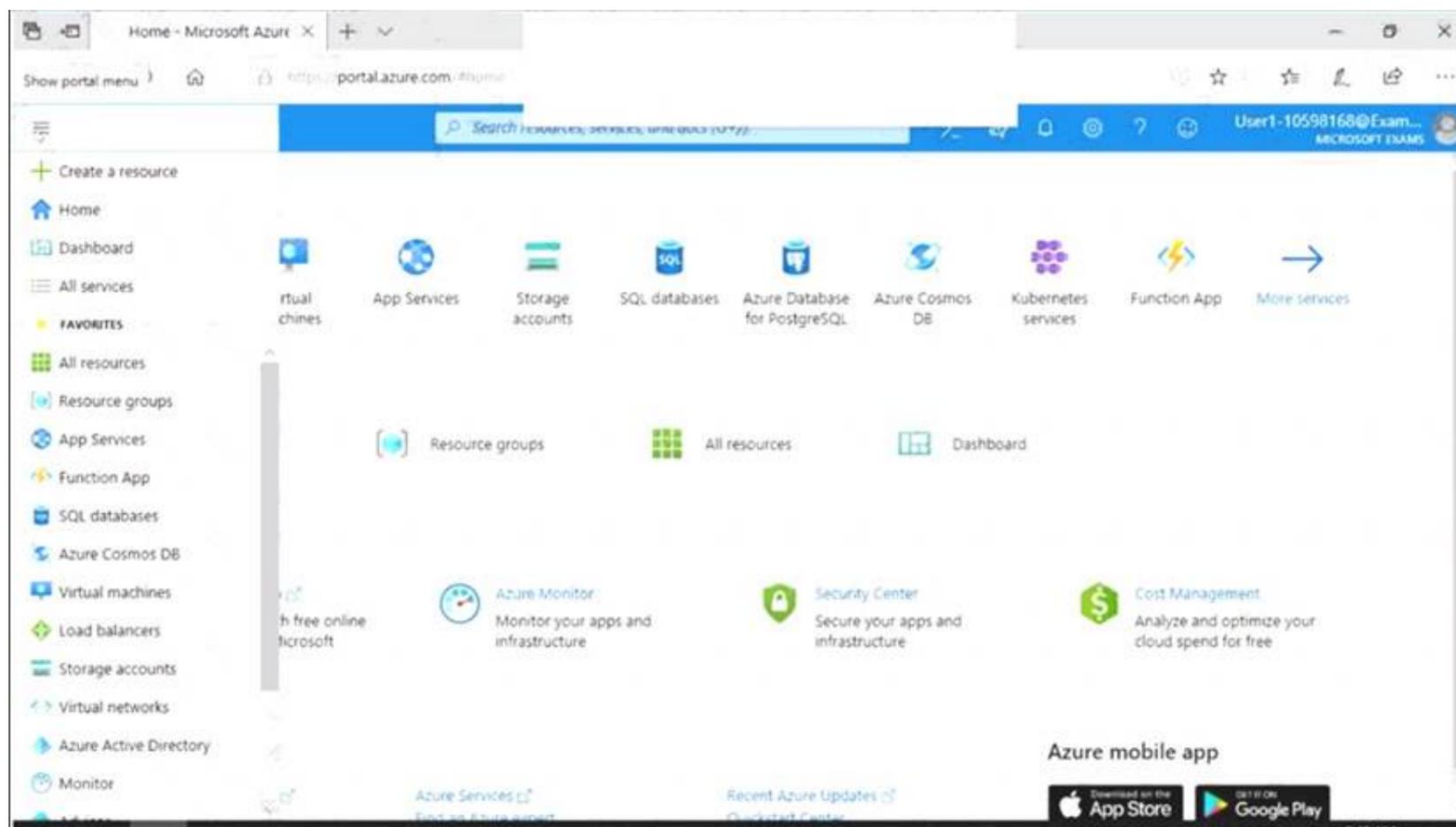
You need to add the network interface of a virtual machine named VM1 to an application security group named ASG1.
To complete this task, sign in to the Azure portal.

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 10
- (Exam Topic 4)
You have a file named File1.yaml that contains the following contents.

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

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

Variable1: ▼

Cannot be accessed
Can be accessed from the Azure portal only
Can be accessed from inside container1 only
Can be accessed from inside container1 and the Azure portal

Variable2: ▼

Cannot be accessed
Can be accessed from the Azure portal only
Can be accessed from inside container1 only
Can be accessed from inside container1 and the Azure portal

A. Mastered
B. Not Mastered

Answer: A

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

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.
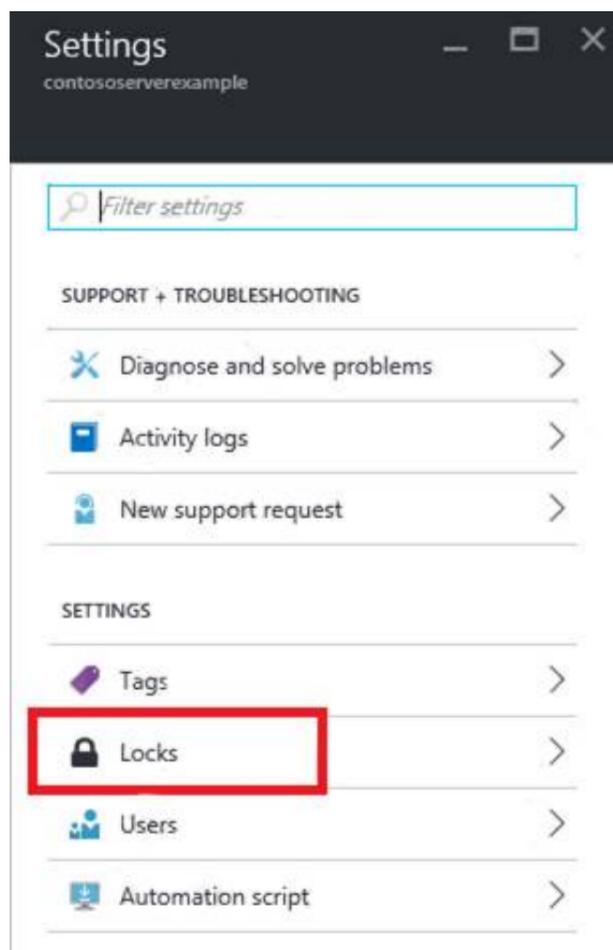
* 3. To add a lock, select Add.

* 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
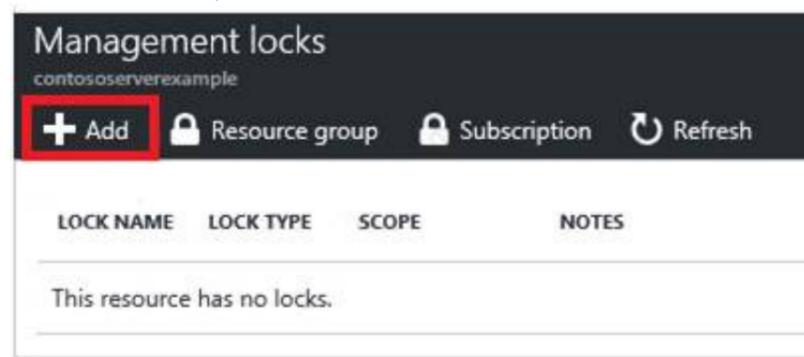
NEW QUESTION 14
- (Exam Topic 4)
You have Azure Resource Manager templates that you use to deploy Azure virtual machines.
You need to disable unused Windows features automatically as instances of the virtual machines are provisioned.
What should you use?

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

Answer: B

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

NEW QUESTION 19
- (Exam Topic 4)
You have an Azure resource group that contains 100 virtual machines.
You have an initiative named Initiative1 that contains multiple policy definitions. Initiative1 is assigned to the resource group.
You need to identify which resources do NOT match the policy definitions.
What should you do?

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

Answer: A

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

NEW QUESTION 23
- (Exam Topic 4)
You have an Azure subscription that contains a virtual machine named VM1. You create an Azure key vault that has the following configurations:

» Name: Vault5
» Region: West US
» Resource group: RG1

You need to use Vault5 to enable Azure Disk Encryption on VM1. The solution must support backing up VM1 by using Azure Backup.
Which key vault settings should you configure?

A. Access policies
B. Secrets
C. Keys
D. Locks

Answer: A

Explanation:

References:
https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

NEW QUESTION 28
- (Exam Topic 4)
You have the Azure resource shown in the following table.

Name	Type	Parent
Management1	Management group	Tenant Root Group
Subscription1	Subscription	Management1
RG1	Resource group	Subscription1
RG2	Resource group	Subscription1
VM1	Virtual machine	RG1
VM2	Virtual machine	RG2

You need to meet the following requirements:
* Internet-facing virtual machines must be protected by using network security groups (NSGs).
* All the virtual machines must have disk encryption enabled.
What is the minimum number of security that you should create in Azure Security Center?

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

Answer: D

NEW QUESTION 32
- (Exam Topic 4)
You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant and a user named User1.
The App registrations settings for the tenant are configured as shown in the following exhibit.

App registrations

Users can register applications ⓘ

| Yes | **No** |
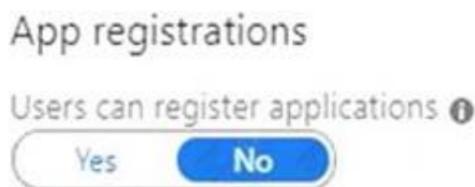
You plan to deploy an app named App1.
You need to ensure that User1 can register App1 in Azure AD. The solution must use the principle of least privilege.
Which role should you assign to User1?

A. App Configuration Data Owner for the subscription
B. Managed Application Contributor for the subscription
C. Cloud application administrator in Azure AD
D. Application developer in Azure AD.

Answer: D

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task

NEW QUESTION 34
- (Exam Topic 4)
You have an Azure subscription named Sub1. Sub1 contains a virtual network named VNet1 that contains one subnet named Subnet1.

You create a service endpoint for Subnet1.
Subnet1 contains an Azure virtual machine named VM1 that runs Ubuntu Server 18.04.
You need to deploy Docker containers to VM1. The containers must be able to access Azure Storage resources and Azure SQL databases by using the service endpoint.

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

Answer: C

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

References:
https://docs.microsoft.com/en-us/azure/virtual-network/container-networking-overview
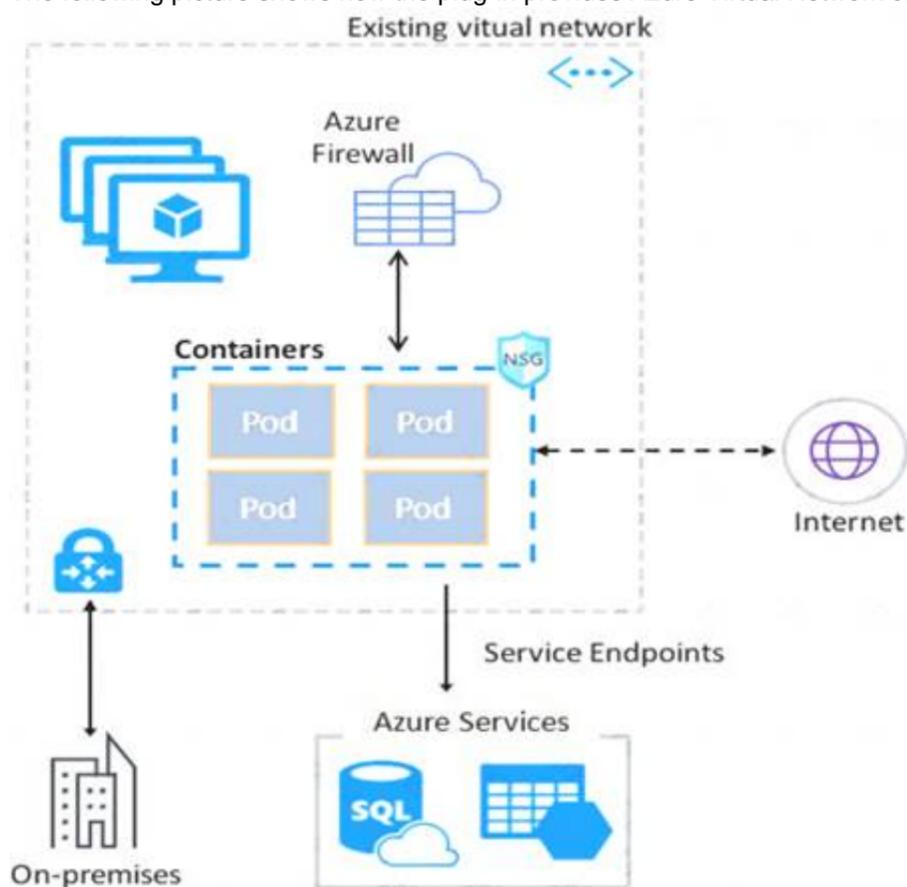
NEW QUESTION 38
- (Exam Topic 4)
You have an Azure environment.
You need to identify any Azure configurations and workloads that are non-compliant with ISO 27001:2013 standards.
What should you use?

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 41
- (Exam Topic 4)
You have an Azure subscription that contains several Azure SQL databases and an Azure Sentinel workspace.
You need to create a saved query in the workspace to find events reported by Advanced Threat Protection for Azure SQL Database.
What should you do?

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

Answer: C

NEW QUESTION 42
- (Exam Topic 4)
You have an Azure subscription that contains an Azure SQL database named DB1 in the East US Azure region. You create the storage accounts shown in the following table.

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

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

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

Answer: C

NEW QUESTION 46
- (Exam Topic 4)
You have an Azure subscription named Subcription1 that contains the resources shown in the following table.

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

You have an Azure subscription named Subcription2 that contains the following resources:
≫ An Azure Sentinel workspace
≫ An Azure Event Grid instance
You need to ingest the CEF messages from the NVAs to Azure Sentinel. NOTE: Each correct selection is worth one point.

Answer Area

Subscription1: An Azure Log Analytics agent on a Linux virtual machine
A Data Factory pipeline
An Event Hubs namespace
Subscription2: An Azure Service Bus queue

Subscription2: A new Azure Log Analytics workspace
A new Azure Sentinel data connector
A new Azure Sentinel playbook
A new Event Grid resource provider

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

Subscription1: An Azure Log Analytics agent on a Linux virtual machine
A Data Factory pipeline
An Event Hubs namespace
Subscription: An Azure Service Bus queue

Subscription2: **A new Azure Log Analytics workspace**
A new Azure Sentinel data connector
A new Azure Sentinel playbook
A new Event Grid resource provider

NEW QUESTION 51
- (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 54
- (Exam Topic 4)
You have an Azure Storage account named storage1 and an Azure virtual machine named VM1. VM1 has a premium SSD managed disk.
You need to enable Azure Disk Encryption for VM1.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange then in the correct order.

Actions

Run the `Set-AzVMDiskEncryptionExtension` cmdlet.
Set the Key Vault access policy to **Enable access to Azure Virtual Machines for deployment**.
Set the Key Vault access policy to **Enable access to Azure Disk Encryption for volume encryption**.
Generate a key vault certificate.
Create an Azure key vault.
Configure storage1 to use a customer-managed key.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

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

---

NEW QUESTION 56
- (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 58
- (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 61
- (Exam Topic 4)
You have an Azure subscription that contains four Azure SQL managed instances.
You need to evaluate the vulnerability of the managed instances to SQL injection attacks. What should you do first?

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

Answer: B

NEW QUESTION 64
- (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 66
- (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 67
- (Exam Topic 4)
Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
Your company has an Active Directory forest with a single domain, named weylandindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.
You have been tasked with integrating Active Directory and the Azure AD tenant. You intend to deploy Azure AD Connect.
Your strategy for the integration must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.
Solution: You recommend the use of federation with Active Directory Federation Services (AD FS). Does the solution meet the goal?

A. Yes
B. No

Answer: B

Explanation:
A federated authentication system relies on an external trusted system to authenticate users. Some companies want to reuse their existing federated system investment with their Azure AD hybrid identity solution. The maintenance and management of the federated system falls outside the control of Azure AD. It's up to the organization by using the federated system to make sure it's deployed securely and can handle the authentication load.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

NEW QUESTION 68
- (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
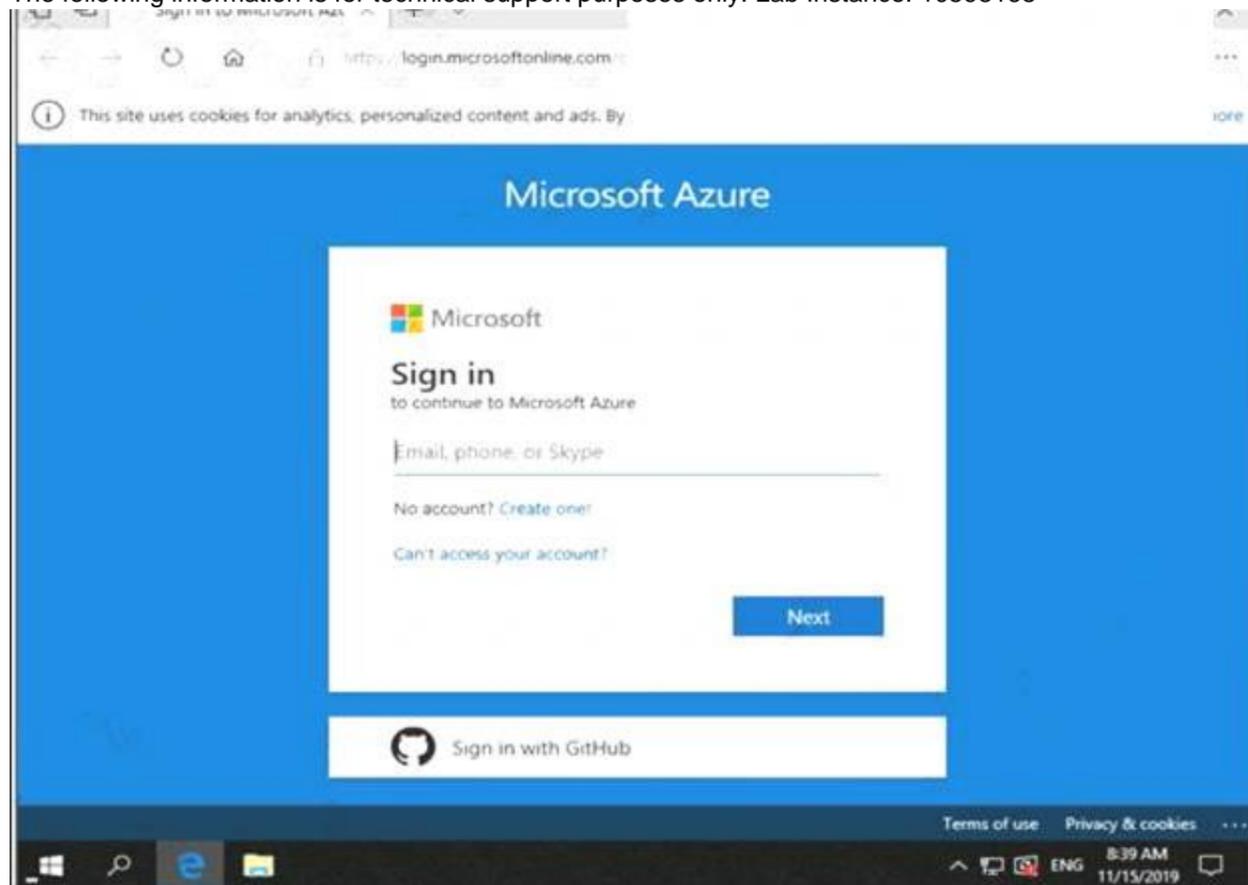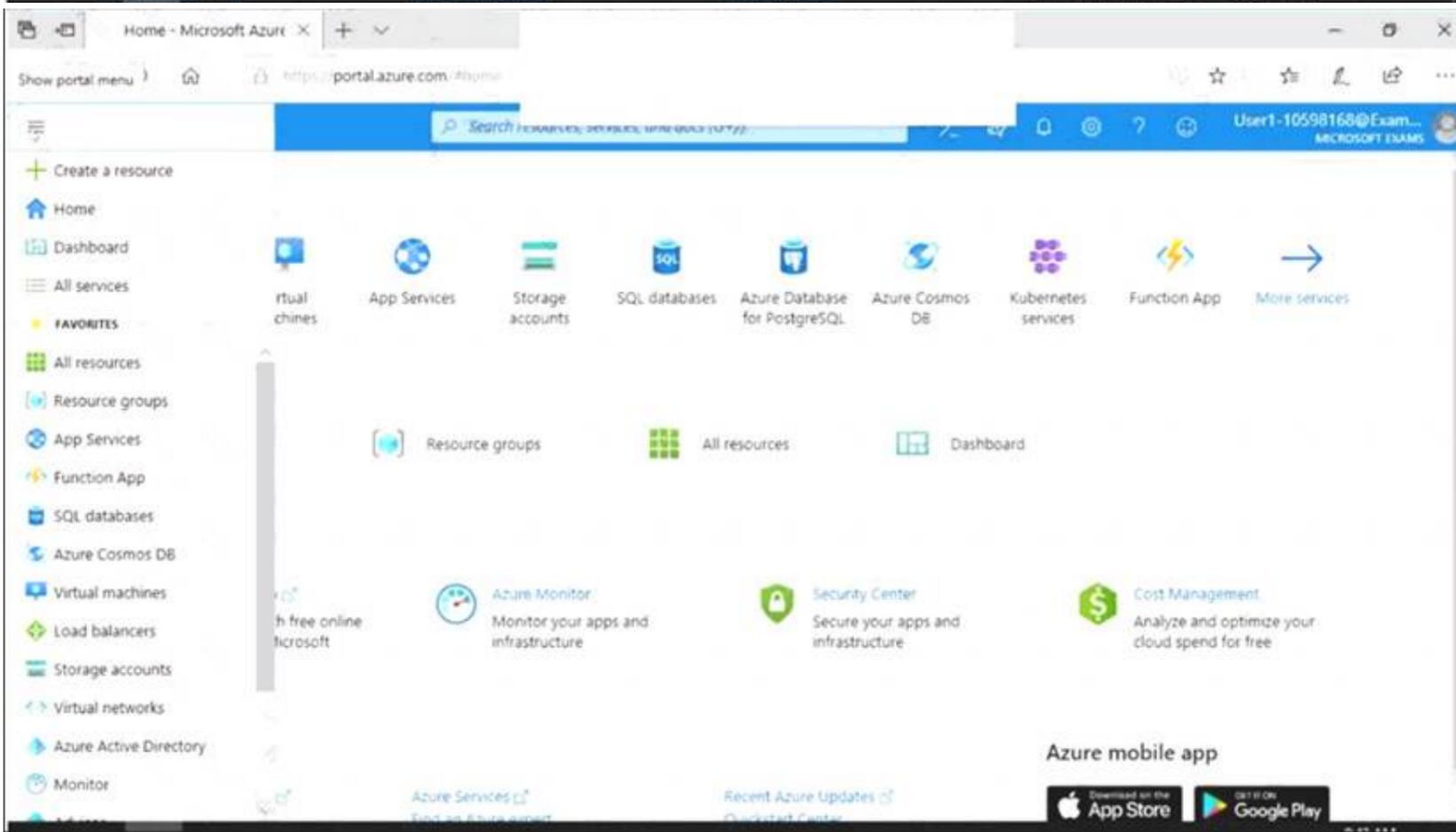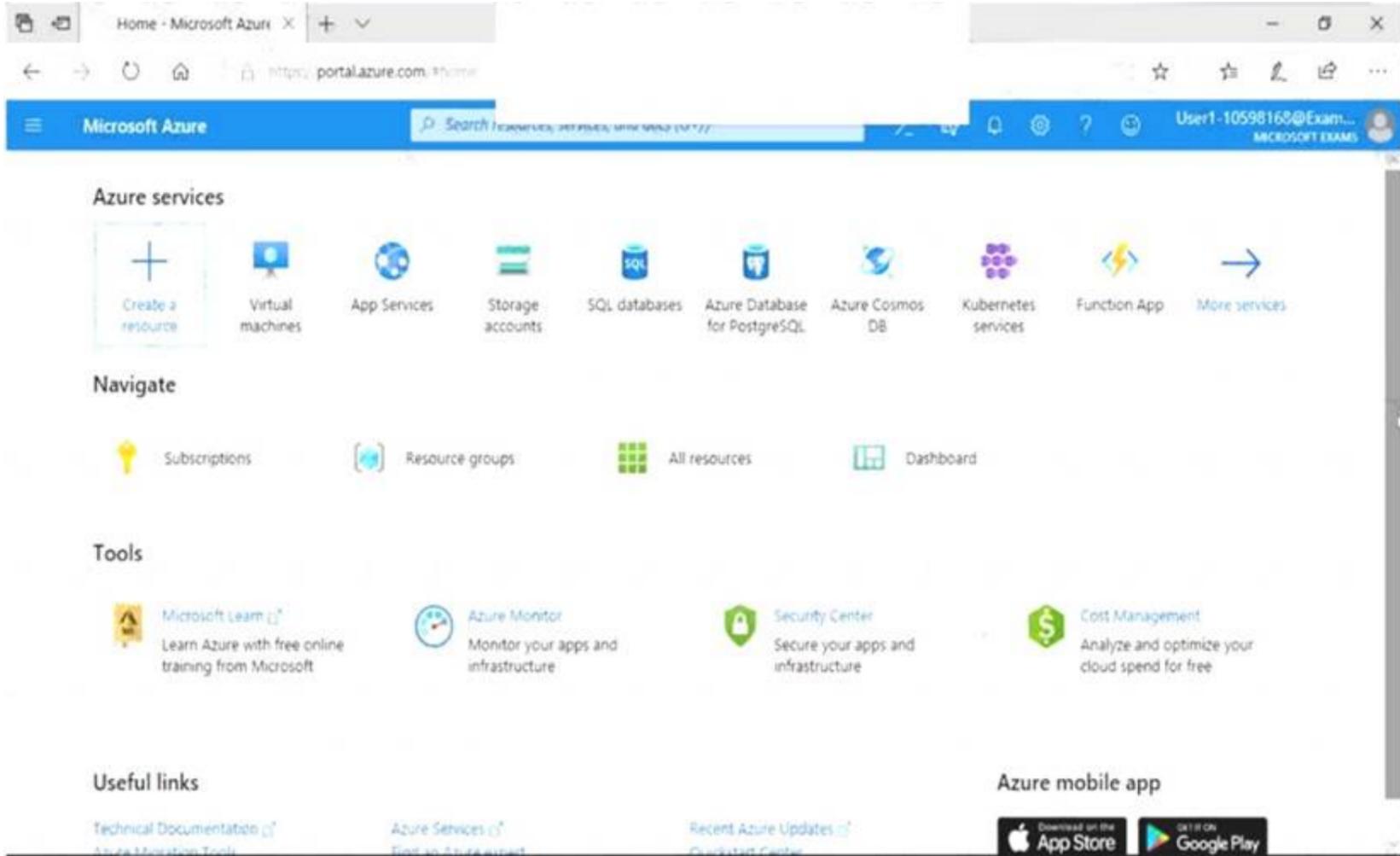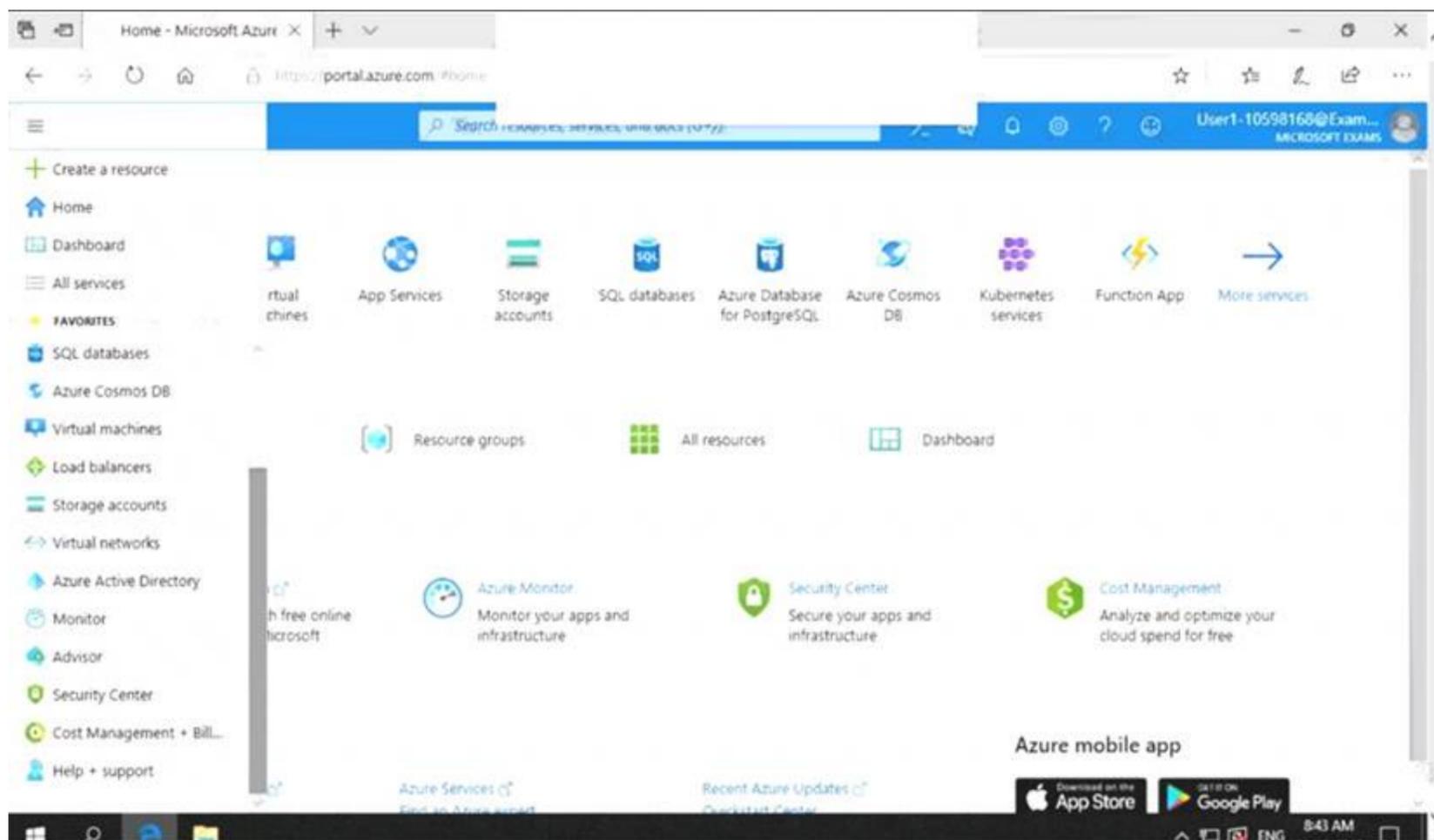
You need to create a new Azure Active Directory (Azure AD) directory named 10598168.onmicrosoft.com. The new directory must contain a user named user1@10598168.onmicrosoft.com who is configured to sign in by using Azure Multi-Factor Authentication (MFA).
To complete this task, sign in to the Azure portal.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Step 1: Create an Azure Active Directory tenant
* 1. Browse to the Azure portal and sign in with an account that has an Azure subscription.
* 2. Select the plus icon (+) and search for Azure Active Directory.
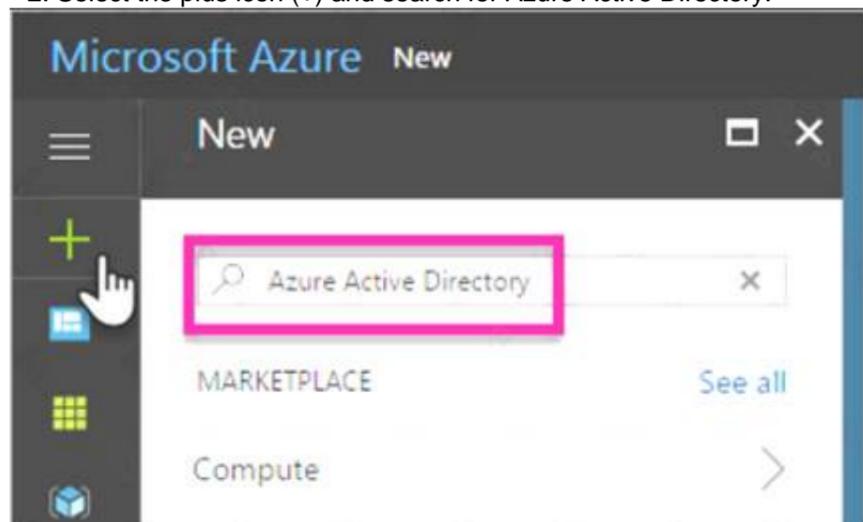
* 3. Select Azure Active Directory in the search results.
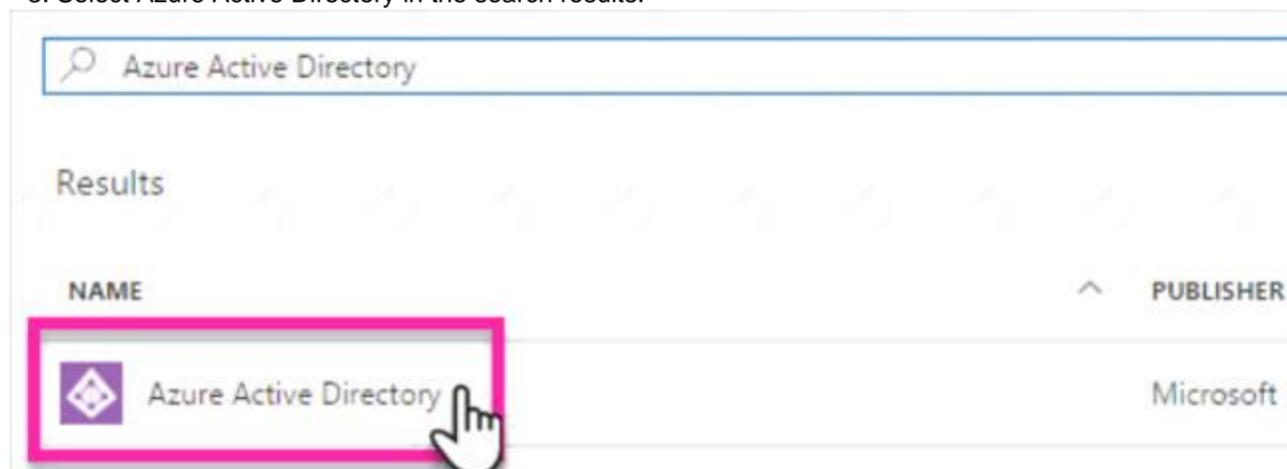
* 4. Select Create.
* 5. Provide an Organization name and an Initial domain name (10598168). Then select Create. Your directory is created.
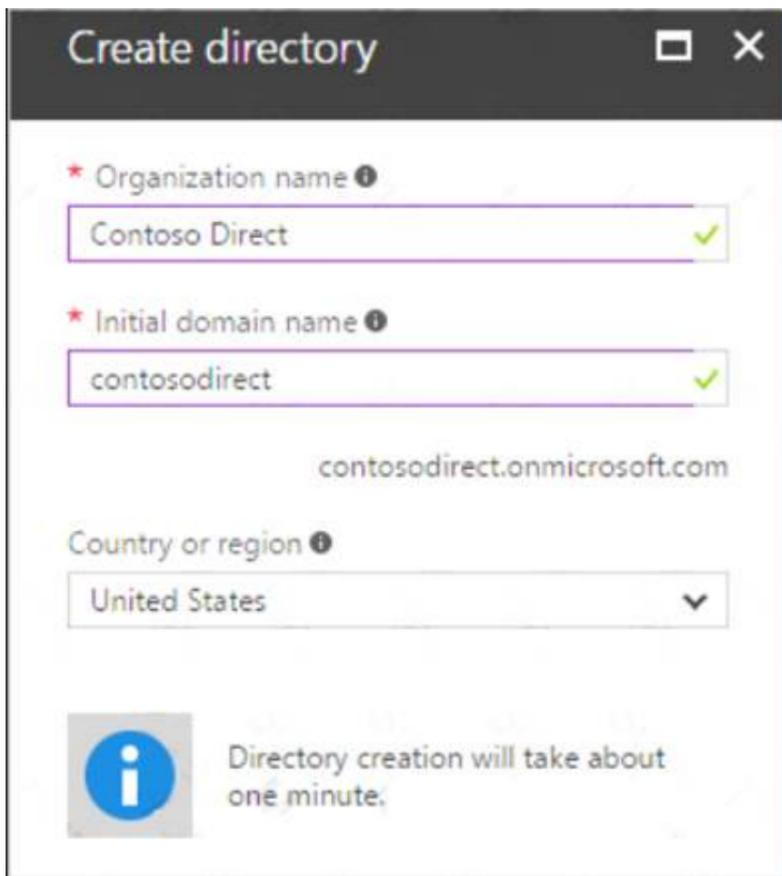
* 6. After directory creation is complete, select the information box to manage your new directory.Next, you're going to add tenant users.
Step 2: Create an Azure Active Directory tenant user
* 7. In the Azure portal, make sure you are on the Azure Active Directory fly out.
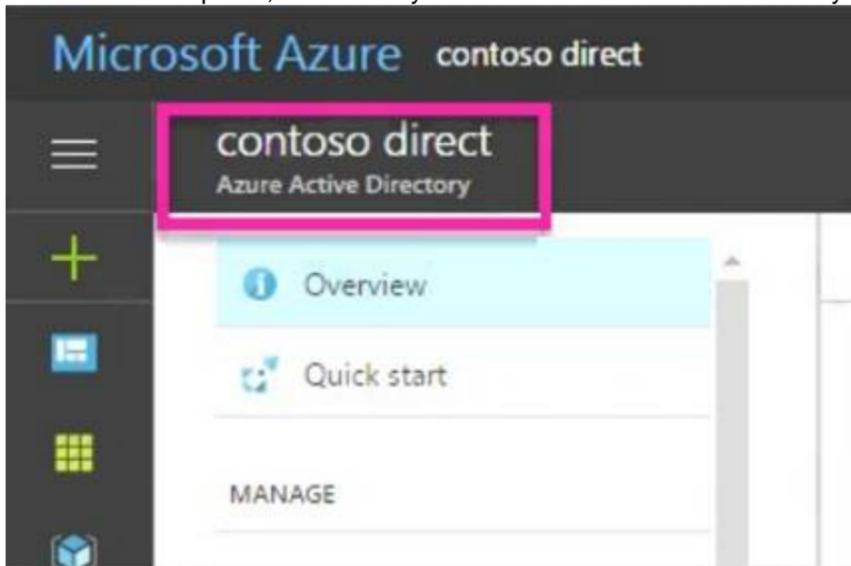
* 8. Under Manage, select Users.
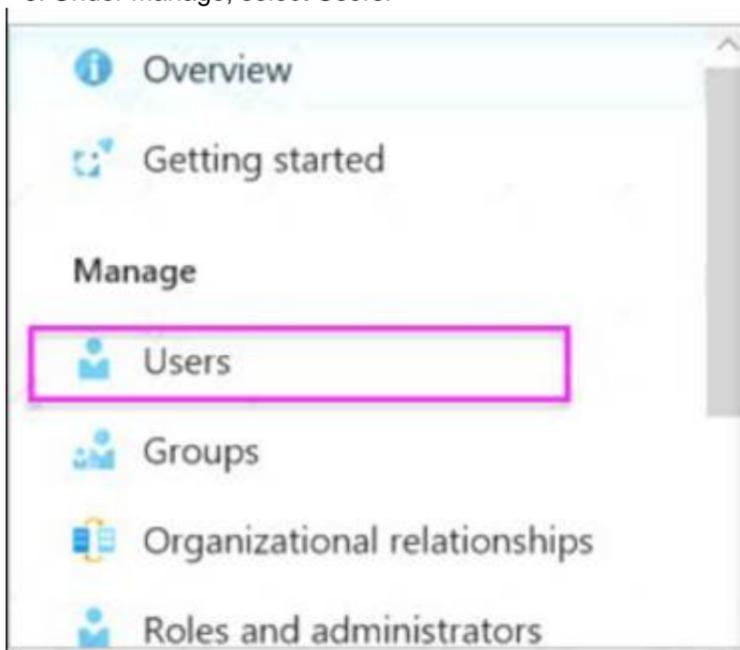
* 9. Select All users and then select + New user.
* 10. Provide a Name and User name (user1) for the regular user tenant You can also show the temporary password. When you're done, select Create.
Name: user1
User name: user1@10598168.onmicrosoft.com

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

NEW QUESTION 73
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.

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

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

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

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

Answer Area

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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

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

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

NEW QUESTION 76
- (Exam Topic 4)
You have an Azure subscription that contains a storage account named storage1 and several virtual machines. The storage account and virtual machines are in the same Azure region. The network configurations of the virtual machines are shown in the following table.

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

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

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

You configure the following Firewall and virtual networks settings for storage1:
≫ Allow access from: Selected networks
≫ Virtual networks: VNET3\Subnet3
≫ Firewall – Address range: 52.233.129.0/24
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 78
- (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/listKevs/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 81
- (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 85
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains two users named User1 and User2 and a registered app named App1.
You create an app-specific role named Role1.
You need to assign Role1 to User1 and enable User2 to request access to App1.
Which two settings should you modify? To answer select the appropriate settings in the answer area NOTE: Each correct selection is worth one pant.

| Owners |
| Roles and administrators (Preview) |
| Users and groups |
| Single sign-on |
| Provisioning |
| Application proxy ✅ |
| Self-service ✅ |

Security

| Conditional Access |
| Permissions |
| Token encryption |

Activity

| Sign-ins |
| Usage & insights |
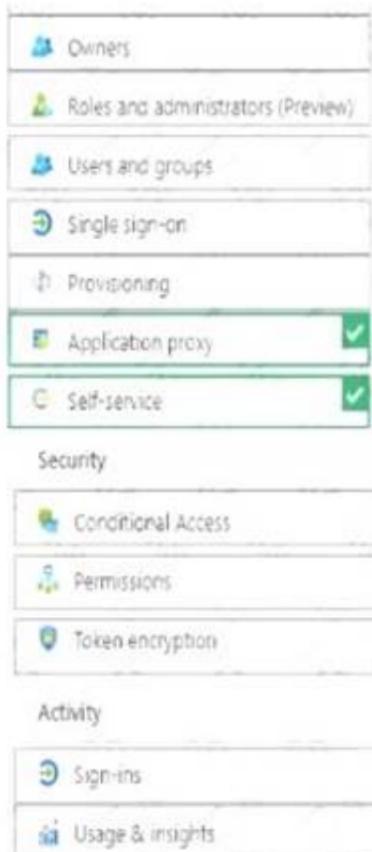
A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, application Description automatically generated

NEW QUESTION 87
- (Exam Topic 4)
You have an Azure subscription name Sub1 that contains an Azure Policy definition named Policy1. Policy1 has the following settings:

〉 Definition location: Tenant Root Group

〉 Category: Monitoring

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

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

Answer: D

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

NEW QUESTION 89
- (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?

Answer Area

NSGs:
| NSG2 only |
| NSG2 and NSG4 only |
| NSG2, NSG3, and NSG4 |

Virtual machines:
| VM3 only |
| VM2 and VM4 only |
| VM1, VM2, and VM4 only |
| VM2, VM3, and VM4 only |
| VM1, VM2, VM3, and VM4 |

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 92
- (Exam Topic 3)
From Azure Security Center, you need to deploy SecPol1. What should you do first?

A. Enable Azure Defender.
B. Create an Azure Management group.
C. Create an initiative.
D. Configure continuous export.

Answer: C

Explanation:
Reference:
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/security-center/custom-security-policies.md https://zimmergren.net/create-custom-security-center-recommendation-with-azure-policy/

NEW QUESTION 93
- (Exam Topic 2)
You are evaluating the security of the network communication between the virtual machines in Sub2. For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
No, Yes,
Yes

NEW QUESTION 96
- (Exam Topic 2)
HOTSPOT
You assign User8 the Owner role for RG4, RG5, and RG6.
In which resource groups can User8 create virtual networks and NSGs? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

User8 can create virtual networks in: ▼
RG4 only
RG6 only
RG4 and RG6 only
RG4, RG5, and RG6

User8 can create NSGs in: ▼
RG4 only
RG4 and RG5 only
RG4 and RG6 only
RG4, RG5, and RG6

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box1: RG6 only as there is not option for RG5 & RG6 which it should be. Box2: RG4 & RG6

NEW QUESTION 98
- (Exam Topic 2)
You are evaluating the effect of the application security groups on the network communication between the virtual machines in Sub2.
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Statements	Yes	No
From VM1, you can successfully ping the private IP address of VM4.	○	○
From VM2, you can successfully ping the private IP address of VM4.	○	○
From VM1, you can connect to the web server on VM4.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: No. VM4 is in Subnet13 which has NSG3 attached to it.
VM1 is in ASG1. NSG3 would only allow ICMP pings from ASG2 but not ASG1. Only TCP traffic is allowed from ASG1.
NSG3 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

Box 2: Yes.
VM2 is in ASG2. Any protocol is allowed from ASG2 so ICMP ping would be allowed.
Box3. VM1 is in ASG1. TCP traffic is allowed from ASG1 so VM1 could connect to the web server as connections to the web server would be on ports TCP 80 or TCP 443.

NEW QUESTION 102
- (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.

Actions

From the Azure portal, create an Azure AD administrator for LitwareSQLServer1.

In SQLDB1, create contained database users.

Connect to SQLDB1 by using Microsoft SQL Server Management Studio (SSMS).

In Azure AD, create a system-assigned managed identity.

In Azure AD, create a user-assigned managed identity.

Answer Area

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 107
- (Exam Topic 1)
You need to create Role1 to meet the platform protection requirements.
How should you complete the role definition of Role1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

```
{
    "Name":  "Role1",
    "Id":   "11111111-1111-1111-1111-111111111111",
    "IsCustom" : true,
    "Description": "VM storage operator"
    "Actions" : [
```

▼	▼
'Microsoft.Compute/	disks/*',
'Microsoft.Resources/	storageAccounts/*',
'Microsoft.Storage/	virtualMachines/disks/*',

```
                ],
    "NotActions":  [
                ],
    "AssignableScopes" :  [
```

▼
.
"/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4/resourceGroups/Resource Group1"
"/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4"

```
                ]
}
```

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 111
- (Exam Topic 4)
You create a new Azure subscription.
You need to ensure that you can create custom alert rules in Azure Security Center. Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Onboard Azure Active Directory (Azure AD) Identity Protection.
B. Create an Azure Storage account.
C. Implement Azure Advisor recommendations.
D. Create an Azure Log Analytics workspace.
E. Upgrade the pricing tier of Security Center to Standard.

Answer: DE

Explanation:
D: You need write permission in the workspace that you select to store your custom alert. References:
https://docs.microsoft.com/en-us/azure/security-center/security-center-custom-alert

NEW QUESTION 113
- (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 115
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant. The tenant contains users that are assigned Azure AD Premium Plan 2 licenses.
You have an partner company that has a domain named The fabrikam.com domain contains a user named user'. User' has an email address of userl@tabrikam.com.
You to provide User1 with to the resources in the tenant The solution must meet the following requirements: ❯ user1 must be able to sign in by using the userl@fabrikam.com credentials

❯ You must be able to grant User1 access to the resources in the tenant

❯ Administrative effort must be minimized.
What should you do?

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

Answer: B

NEW QUESTION 119
- (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.

Password1: [▼ dropdown]
Never
Always
Only after May 1, 2019

Password2: [▼ dropdown]
Never
Always
Only between March 1, 2019 and May 1. 2019

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 121
- (Exam Topic 4)
You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1. You have 500 Azure virtual machines that run Windows Server 2016 and are enrolled in LAW1.
You plan to add the System Update Assessment solution to LAW1.
You need to ensure that System Update Assessment-related logs are uploaded to LAW1 from 100 of the virtual machines only.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions | **Answer Area**

Create a new workspace.

Apply the scope configuration to the solution.

Create a scope configuration.

Create a computer group.

Create a data source.

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 126
- (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 128
- (Exam Topic 4)
You need to create a new Azure Active Directory (Azure AD) directory named 10317806.onmicrosoft.com. The new directory must contain a user named user10317806 who is configured to sign in by using Azure Multi-Factor Authentication (MFA).

A. Mastered
B. Not Mastered

Answer: A

Explanation:
To create a new Azure AD tenant:
* 1. Browse to the Azure portal and sign in with an account that has an Azure subscription.
* 2. Select the plus icon (+)
and search foAr zure Active Directory.
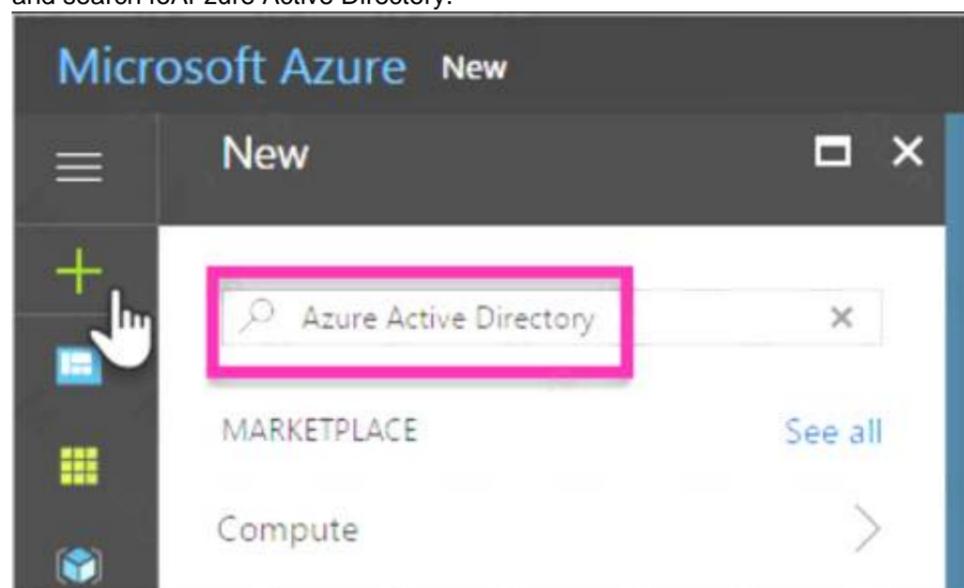
* 3. Select Azure Active Directory
in the search results.
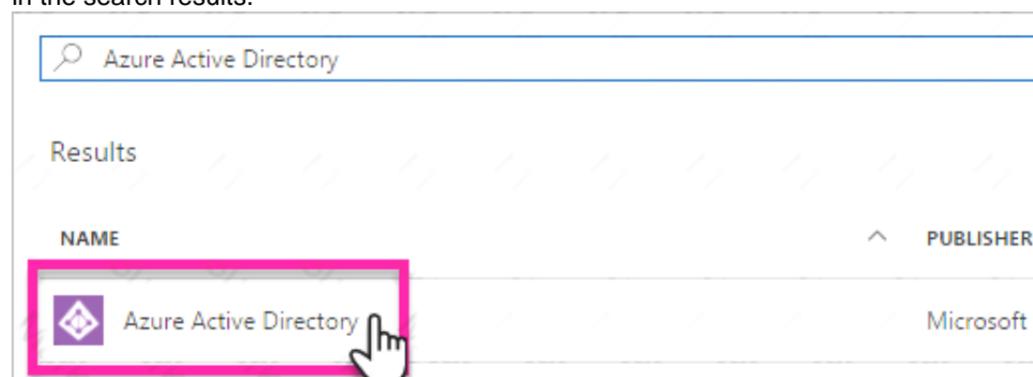
* 4. Select Create.
* 5. Provide an Organization name
This will create the directory named 10317806.onmicrosoft.com.
(10317806) and anInitial domain name (10317806). Then select Create.
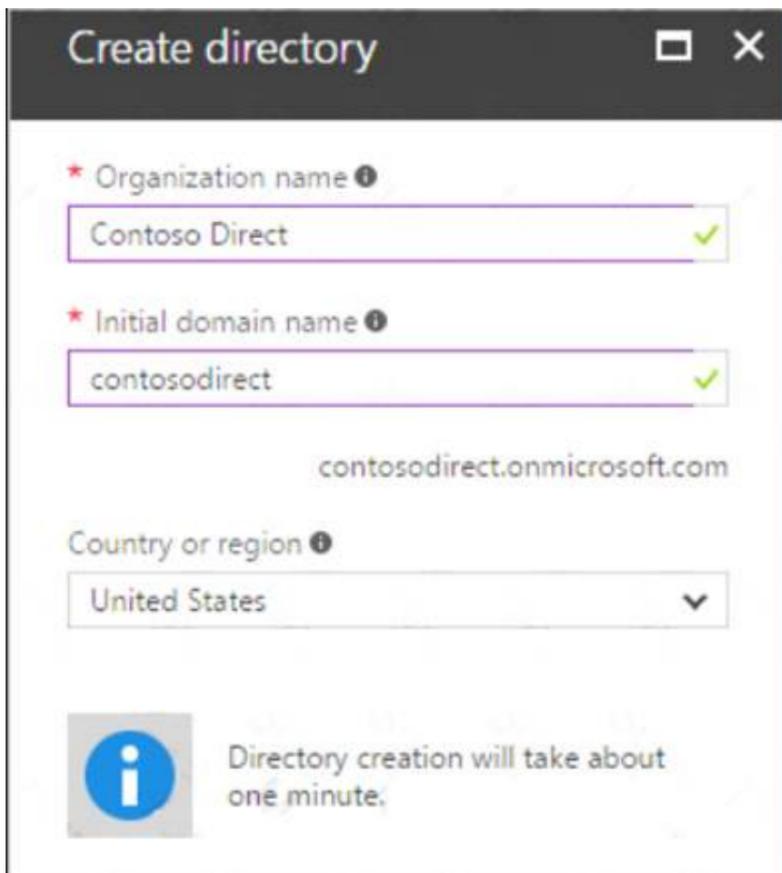
* 6. After directory creation is complete, select the information box to manage your new directory. To create the user:
* 1. In the Azure portal, make sure you are on the Azure Active Directory fly out.
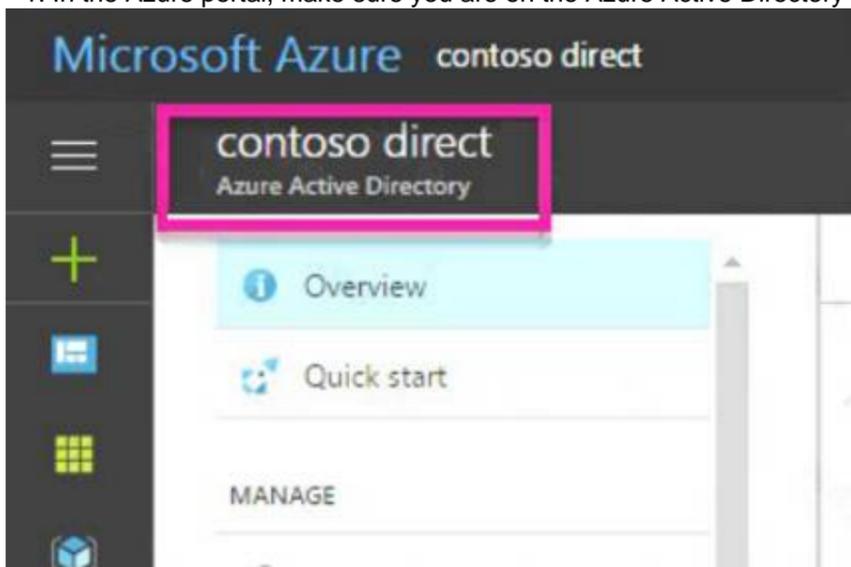
If not, select the Azure Active Directory icon from the left services navigation.
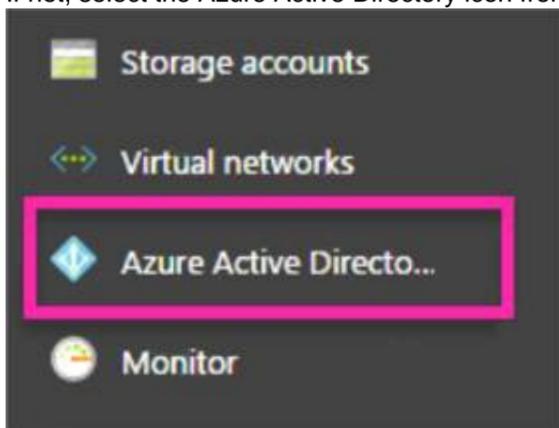
* 2. Under Manage, select Users.
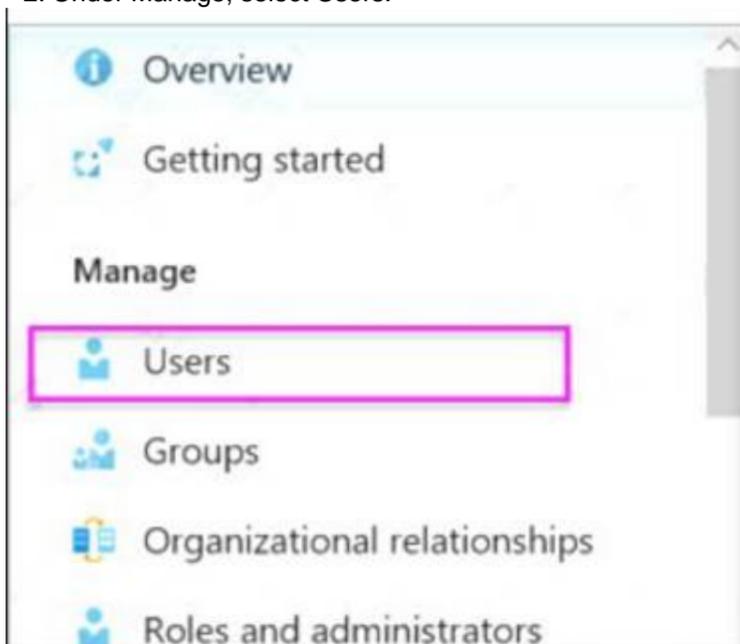
* 3. Select All users

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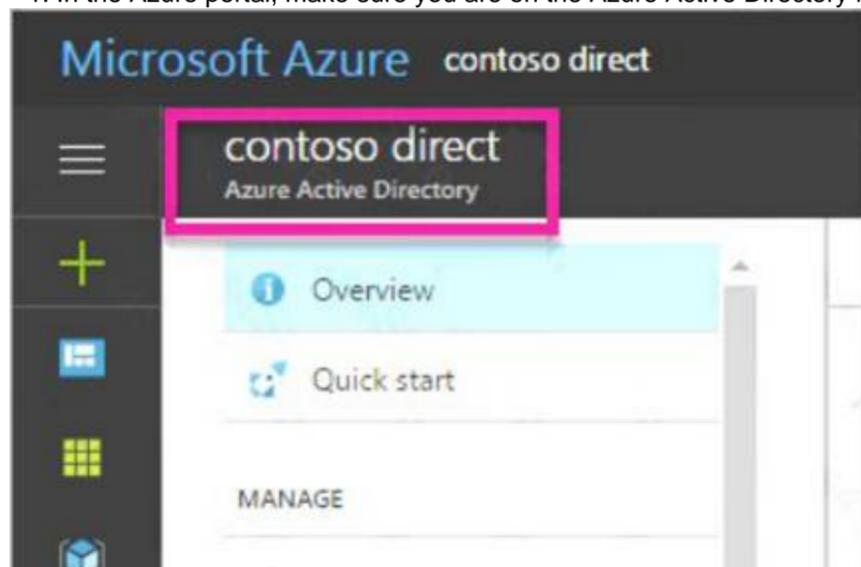
If not, select the Azure Active Directory icon from the left services navigation.

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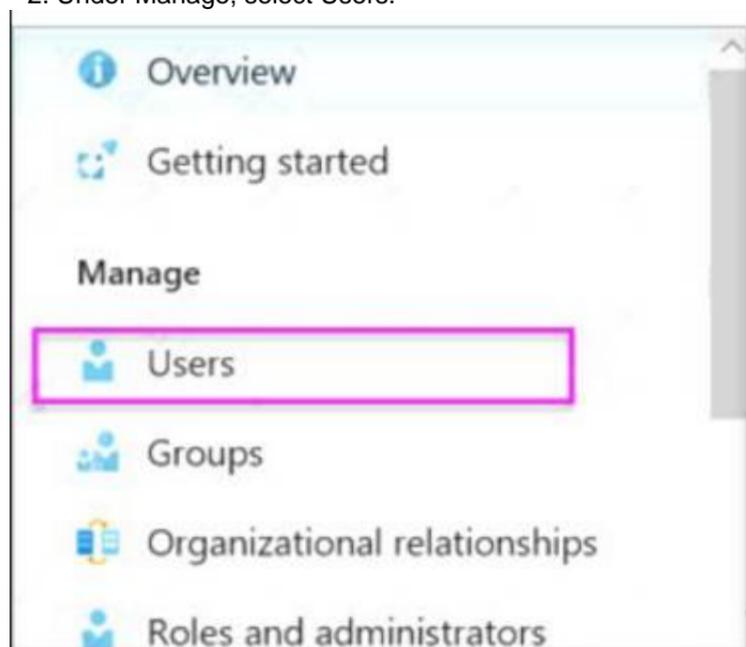
* 3. Click on the Multi-Factor Authentication link.
* 4. Tick the checkbox next to the user's name and click the Enable link.
Reference:
https://docs.microsoft.com/en-us/power-bi/developer/create-an-azure-active-directory-tenant

NEW QUESTION 131
- (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.

Cmdlets	Answer Area

New-AzStorageAccountKey

New-AzStorageTable

Register-AzProviderFeature

New-AzStorageAccount

Register-AzResourceProvider

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 136
- (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 138
- (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 141
- (Exam Topic 4)
You have an Azure subscription that contains an Azure SQL database named SQLDB1. SQLDB1 contains the columns shown in the following table.

Name	Data type	Sample value
Email	Varchar	admin@contoso.com
Birthday	Date	2010-07-07

For the Email and Birthday columns, you implement dynamic data masking by using the default masking function.
Which value will the users see in each column? To answer, drag the appropriate values to the correct columns. Each value 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.

Values		Answer Area	
1900-01-01		Email:	Value
1900-01-01 00:00:00.0000		Birthday:	Value
2010-XX-XX			
XXXX			

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Values		Answer Area	
1900-01-01		Email:	1900-01-01
1900-01-01 00:00:00.0000		Birthday:	2010-XX-XX
2010-XX-XX			
XXXX			

NEW QUESTION 145
- (Exam Topic 4)
You have an Azure subscription.
You configure the subscription to use a different Azure Active Directory (Azure AD) tenant. What are two possible effects of the change? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

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

Answer: AB

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

NEW QUESTION 146
- (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 150
- (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 155
- (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 158
- (Exam Topic 4)
You have the Azure Information Protection conditions shown in the following table.

Name	Pattern	Case sensitivity
Condition1	White	On
Condition2	Black	Off

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

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

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

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

▼
No label
Label1 only
Label2 only
Label1 and Label2

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

▼
No label
Label1 only
Label2 only
Label1 and Label2

A. Mastered
B. Not Mastered

Answer: A

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

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

➢ The most sensitive label is applied.

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

NEW QUESTION 163
- (Exam Topic 4)
You need to prevent administrators from performing accidental changes to the Homepage app service plan. To complete this task, sign in to the Azure portal.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
You need to configure a 'lock' for the app service plan. A read-only lock ensures that no one can make changes to the app service plan without first deleting the lock.

➢ In the Azure portal, type App Service Plans in the search box, select App Service Plans from the search results then select Homepage. Alternatively, browse to App Service Plans in the left navigation pane.

➢ In the properties of the app service plan, click on Locks.

➢ Click the Add button to add a new lock.

➢ Enter a name in the Lock name field. It doesn't matter what name you provide for the exam.

➢ For the Lock type, select Read-only.

➢ Click OK to save the changes.

NEW QUESTION 168
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains two administrative units named AU1 and AU2.
Users are assigned to the administrative units as shown in the following table.

User name	Member of
Admin1	AU1
Admin2	AU1
Admin3	AU2
Admin4	AU2
User1	AU1

Answer Area

Statements	Yes	No
Admin1 can reset the password of User1.	○	○
Admin2 can reset the password of User3.	○	○
Admin3 can reset the password of Admin4.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Admin1 can reset the password of User1.	⊙	○
Admin2 can reset the password of User3.	⊙	○
Admin3 can reset the password of Admin4.	○	⊙

NEW QUESTION 173
- (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 177
- (Exam Topic 4)
You have an Azure subscription that contains the virtual machines shown in the following table.

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

You create the Azure policies shown in the following table.

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

You create the resource locks shown in the following table.

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

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

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 180
- (Exam Topic 4)
You have an Azure virtual machines shown in the following table.

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

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

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

Answer: C

Explanation:
Note: Create a workspace
➢ In the Azure portal, click All services. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics.
➢ Click Create, and then select choices for the following items:
Provide a name for the new Log Analytics workspace, such as DefaultLAWorkspace. OMS workspaces are now referred to as Log Analytics workspaces.
Select a Subscription to link to by selecting from the drop-down list if the default selected is not appropriate. For Resource Group, select an existing resource group that contains one or more Azure virtual machines. Select the Location your VMs are deployed to. For additional information, see which regions Log Analytics is available in.

NEW QUESTION 184
- (Exam Topic 4)
You suspect that users are attempting to sign in to resources to which they have no access.
You need to create an Azure Log Analytics query to identify failed user sign-in attempts from the last three days. The results must only show users who had more than five failed sign-in attempts.
How should you configure the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

```
let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AcccountType == 'User' and  [▼] ==4625
```
ActivityID
DataType
EventID
QuantityUnit

```
| Summarie failed_login_attempts=  [▼]
```
Count(),
Countif(),
Makeset(),
Split(),

```
      latest_failed_login=arg_max(TimeGenerated by Account
| where failed login attempts > 5
```

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 186
- (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 187
- (Exam Topic 4)
A user named Debbie has the Azure app installed on her mobile device.
You need to ensure that debbie@contoso.com is alerted when a resource lock is deleted. To complete this task, sign in to the Azure portal.

A. Mastered

B. Not Mastered

Answer: A

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

NEW QUESTION 191
- (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 196
- (Exam Topic 4)
You have an Azure subscription that contains an Azure key vault named Vault1. In Vault1, you create a secret named Secret1.
An application developer registers an application in Azure Active Directory (Azure AD). You need to ensure that the application can use Secret1.
What should you do?

A. In Azure AD, create a role.
B. In Azure Key Vault, create a key.
C. In Azure Key Vault, create an access policy.
D. In Azure AD, enable Azure AD Application Proxy.

Answer: C

Explanation:
"You may need to configure the target resource to allow access from your application. For example, if you request a token to Key Vault, you need to make sure you have added an access policy that includes your application's identity. Otherwise, your calls to Key Vault will be rejected, even if they include the token"
https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity?tabs=dotnet

NEW QUESTION 201
- (Exam Topic 4)
Your company has an Azure Active Directory (Azure AD) tenant named contoso.com.
The company is developing an application named App1. App1 will run as a service on server that runs Windows Server 2016. App1 will authenticate to contoso.com and access Microsoft Graph to read directory data.
You need to delegate the minimum required permissions to App1.
Which three actions should you perform in sequence from the Azure portal? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

| Grant permissions |

| Add a delegated permission. |

| Configure Azure AD Application Proxy. |

| Add an application permission. |

| Create an app registration. |

Answer Area
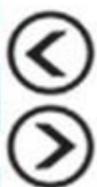
A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 205
- (Exam Topic 4)
You have an Azure virtual machine named VM1.
From Azure Security Center, you get the following high-severity recommendation: "Install endpoint protection solutions on virtual machine".
You need to resolve the issue causing the high-severity recommendation. What should you do?

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

Answer: A

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

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

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

You need to ensure that ServerAdmins can perform the following tasks: Create virtual machine to the existing virtual network in RG2 only.
The solution must use the principle of least privilege.
Which two role-based access control (RBAC) roles should you assign to ServerAdmins? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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

Answer: BF

NEW QUESTION 212
- (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.	O	O
An Azure virtual machine on Subnet2 can access data in Contoso1901.	O	O
A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901.	O	O

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 213
- (Exam Topic 4)
You need to configure an access review. The review will be assigned to a new collection of reviews and reviewed by resource owners.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Create an access review program.

Set Reviewers to Selected users.

Create an access review audit.

Create an access review control.

Set Reviewers to Group owners.

Set Reviewers to Members.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

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

Reviewers

Reviewers   Group owners   ∧

                   Group owners

Programs   Selected users

Link to program   Members (self)

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

NEW QUESTION 218
- (Exam Topic 4)
You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1. You have 100 on-premises servers that run Windows Server 2012 R2 and Windows Server 2016. The servers
connect to LAW1. LAW1 is configured to collect security-related performance counters from the connected
servers.
You need to configure alerts based on the data collected by LAW1. The solution must meet the following requirements:
≫ Alert rules must support dimensions.
≫ The time it takes to generate an alert must be minimized.
≫ resolved.
Which signal type should you use when you create the alert rules?

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

Answer: C

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

NEW QUESTION 221
- (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.

CosmosDB1:

Authenticate Azure AD users and generate resource tokens.
Authenticate Azure AD users and relay resource tokens.
Create database users and generate resource tokens.

WebApp1:

Authenticate Azure AD users and generate resource tokens.
Authenticate Azure AD users and relay resource tokens.
Create database users and generate resource tokens.

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
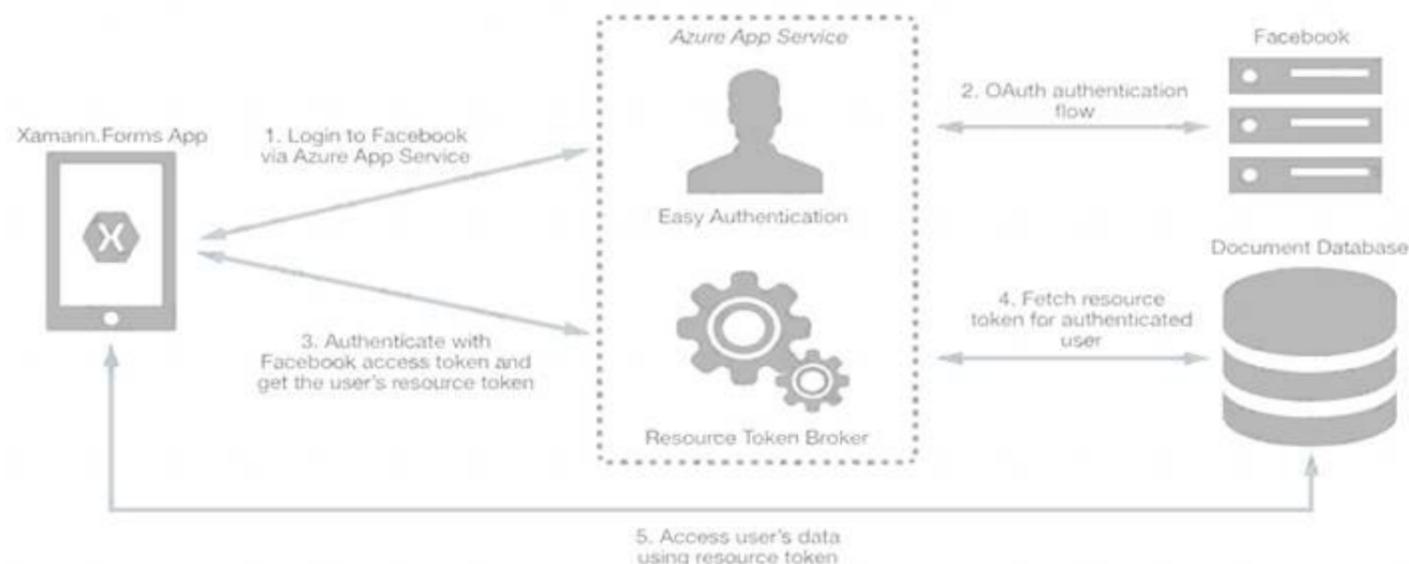
NEW QUESTION 224
- (Exam Topic 4)
You company has an Azure Active Directory (Azure AD) tenant named contoso.com. You plan to create several security alerts by using Azure Monitor.
You need to prepare the Azure subscription for the alerts. What should you create first?

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 229
- (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 230
- (Exam Topic 4)
You need to ensure that the events in the NetworkSecurityGroupRuleCounter log of the
VNET01-Subnet0-NSG network security group (NSG) are stored in the logs11597200 Azure Storage account for 30 days.
To complete this task, sign in to the Azure portal.

A. Mastered
B. Not Mastered

Answer: A

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

➤ In the Azure portal, type Network Security Groups in the search box, select Network Security Groups from the search results then select VNET01-Subnet0-NSG. Alternatively, browse to Network Security Groups in the left navigation pane.

➤ In the properties of the Network Security Group, click on Diagnostic Settings.

➤ Click on the Add diagnostic setting link.

➤ Provide a name in the Diagnostic settings name field. It doesn't matter what name you provide for the exam.

➤ In the Log section, select NetworkSecurityGroupRuleCounter.

➤ In the Destination details section, select Archive to a storage account.

➤ In the Storage account field, select the logs11597200 storage account.

➤ In the Retention (days) field, enter 30.

➤ Click the Save button to save the changes.

NEW QUESTION 231
- (Exam Topic 4)
You have an Azure subscription named Subscription1.
You need to view which security settings are assigned to Subscription1 by default. Which Azure policy or initiative definition should you review?

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

Answer: B

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

NEW QUESTION 236
- (Exam Topic 4)
You have an Azure subscription that contains the storage accounts shown in the following table.

Name	Type
storage1	Azure Blob storage
storage2	Azure Files SMB
storage3	Azure Table storage

You need to configure authorization access.
Which authorization types can you use for each storage account? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

storage1:

Shared Key only
Shared access signature (SAS) only
Azure Active Directory (Azure AD) only
Shared Key and shared access signature (SAS) only
Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

storage2:

Shared Key only
Shared access signature (SAS) only
Shared Key and shared access signature (SAS)

storage3:

Shared Key only
Shared access signature (SAS) only
Azure Active Directory (Azure AD) only
Shared Key and shared access signature (SAS) only
Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

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/storage/common/authorize-data-access

NEW QUESTION 239
- (Exam Topic 4)
You have an Azure subscription that contains the resources shown in the following table.

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

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

Name	Usage location
User1	United States
User2	Germany

You create the groups shown in the following table.

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

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

Dynamic membership rules · · ·   ✕

💾 Save   ✕ Discard | ♡ Got feedback?

Configure Rules   Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. ⓘ Learn more

And/Or	Property	Operator	Value	🗑
	accountEnabled	Equals	true	
Or ⌄	usageLocation ⌄	Equals ⌄	US ⌄	🗑

✛ Add expression   ✛ Get custom extension properties ⓘ

Rule syntax   ✎ Edit

```
(user.accountEnabled -eq true) or (user.usageLocation - eq "US")
```

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

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 244
- (Exam Topic 4)
You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant.
When a developer attempts to register an app named App1 in the tenant, the developer receives the error message shown in the following exhibit.

You need to ensure that the developer can register App1 in the tenant. What should you do for the tenant?

A. Modify the User settings
B. Set Enable Security default to Yes.
C. Modify the Directory properties.
D. Configure the Consent and permissions settings for enterprise applications.

Answer: A

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

NEW QUESTION 248
- (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
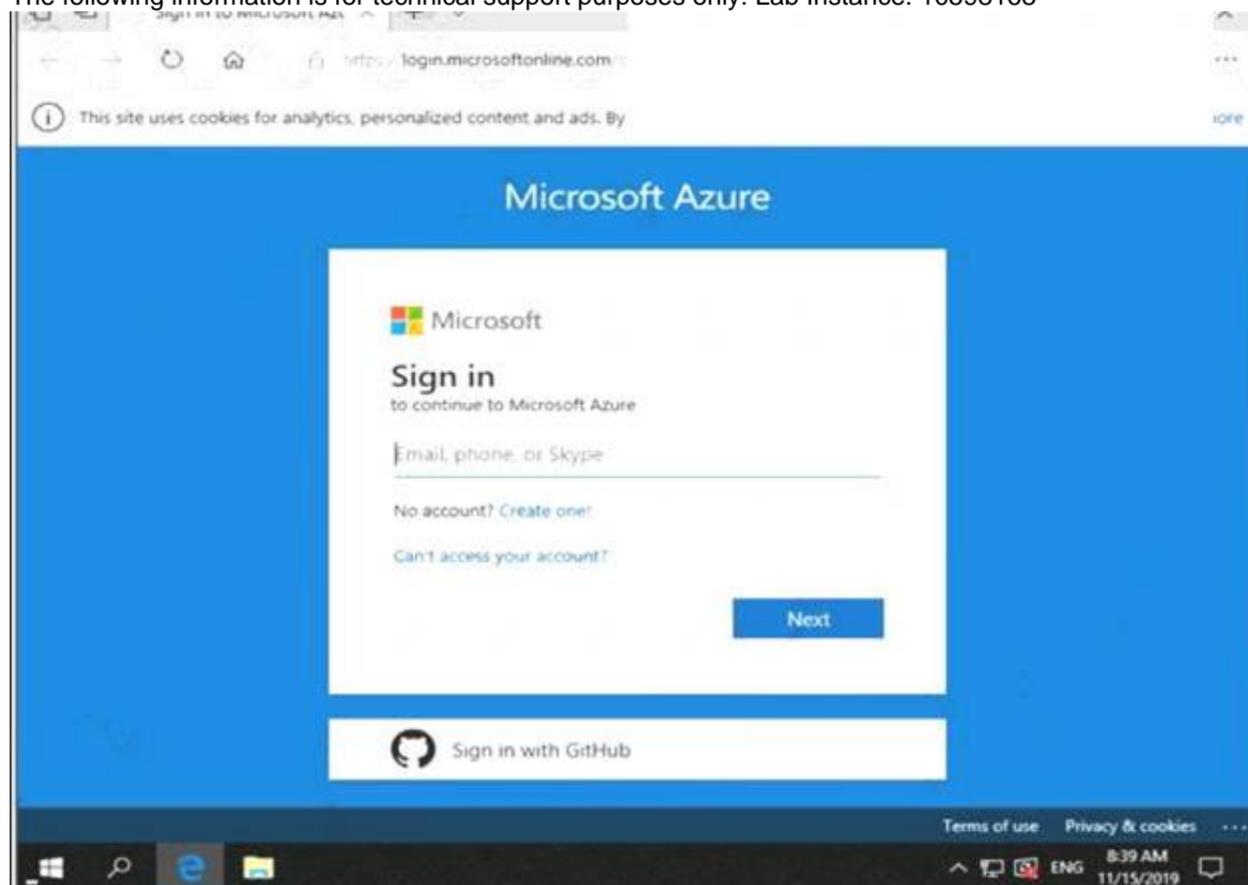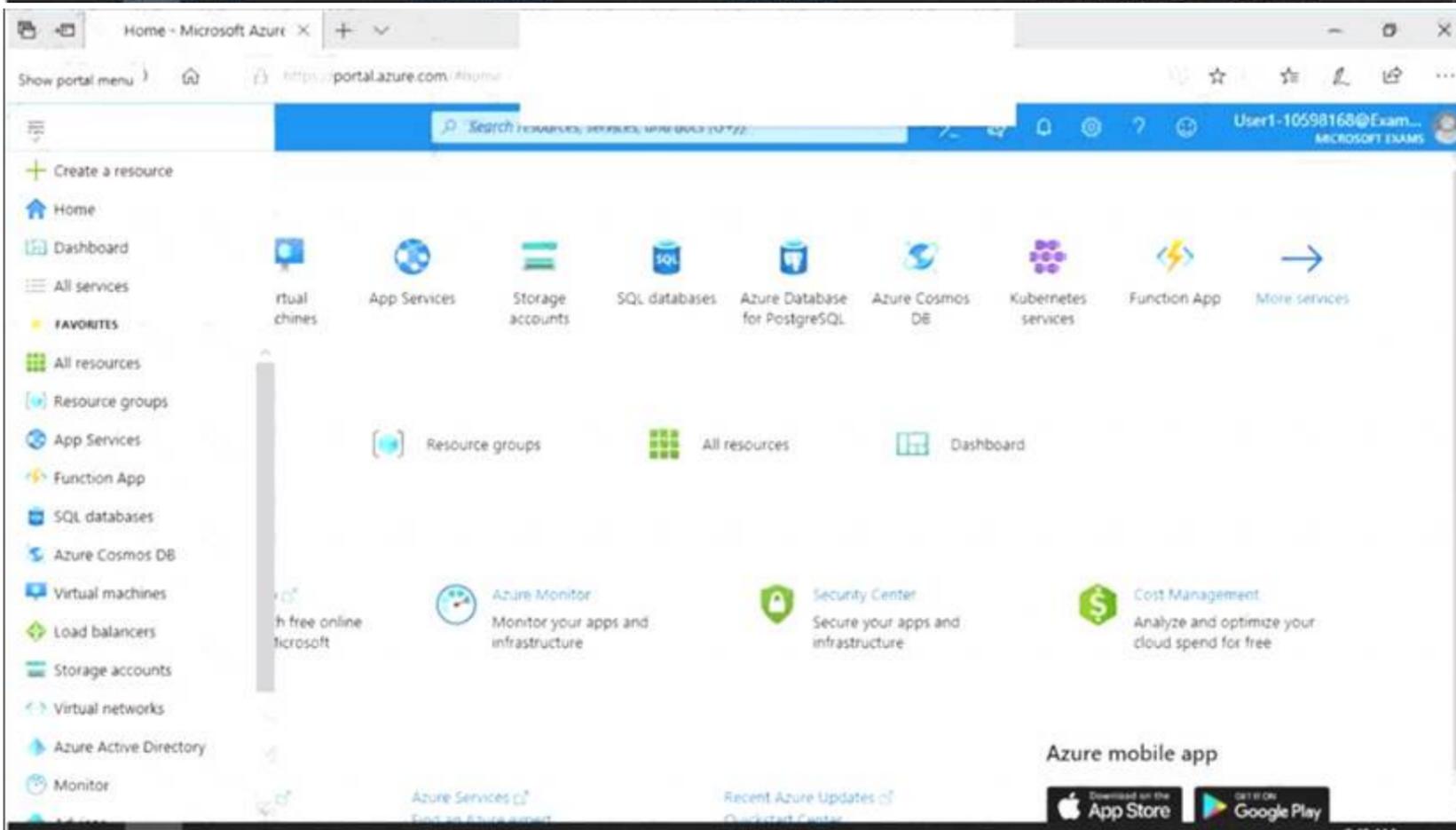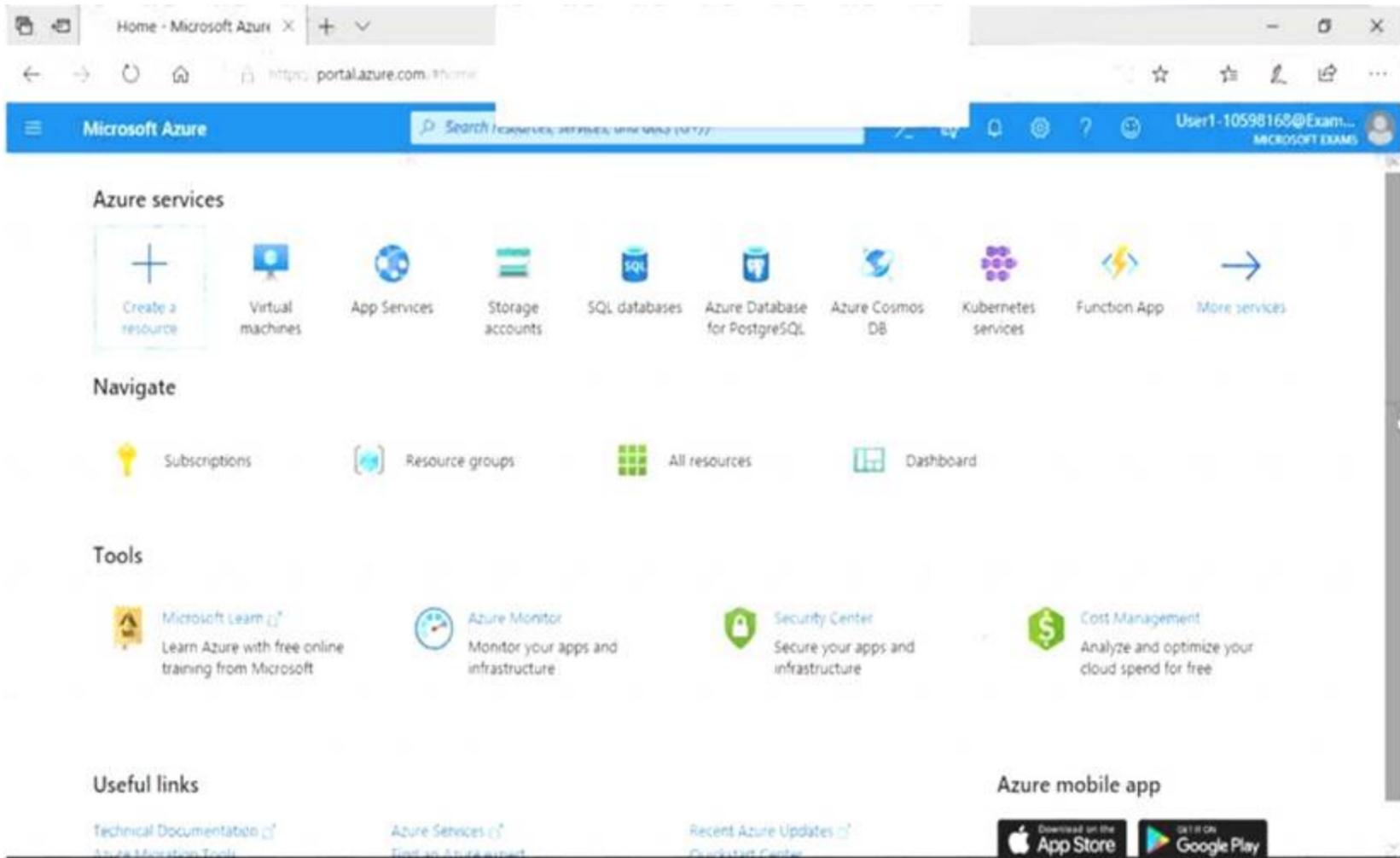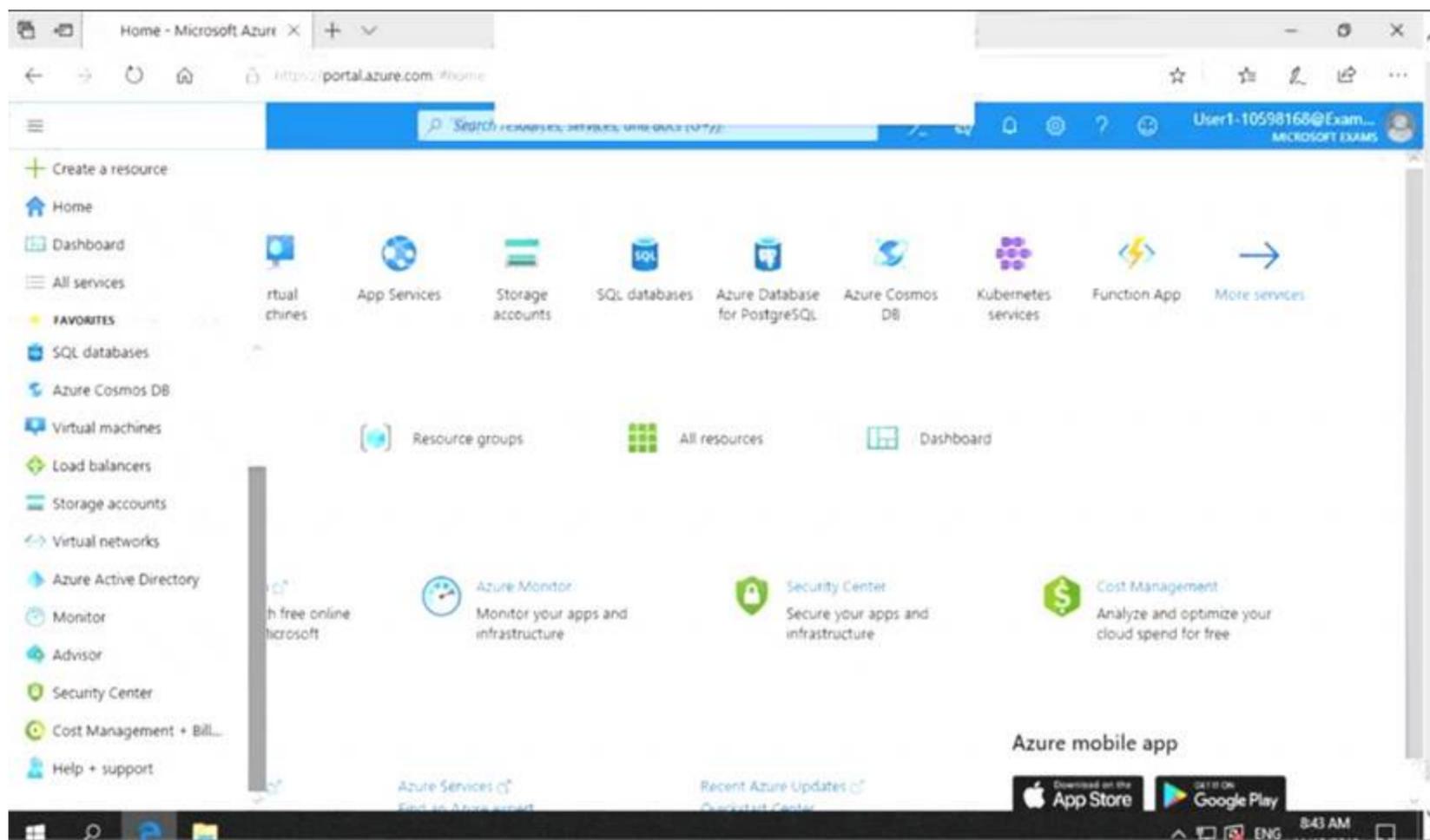
You need to prevent administrative users from accidentally deleting a virtual network named VNET1. The administrative users must be allowed to modify the settings of VNET1.

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

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 Settings blade for virtual network VNET, select Locks.
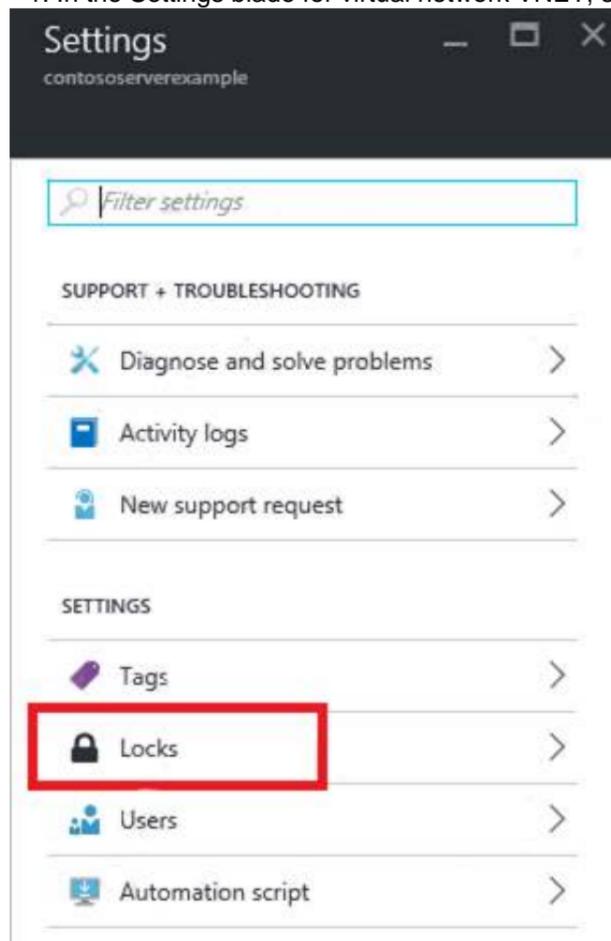
* 2. To add a lock, select Add.

* 3. For Lock type select Delete lock, and click OK Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources
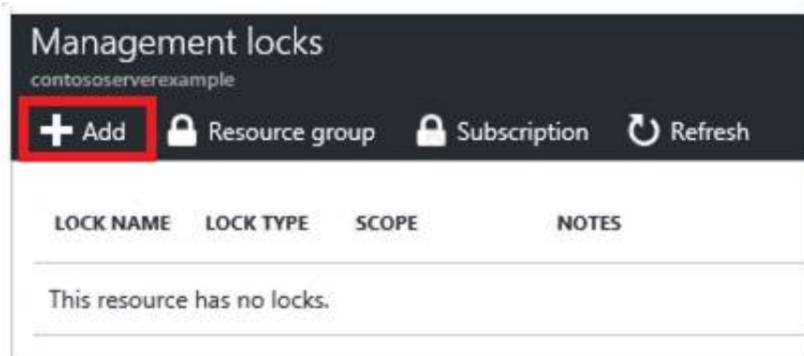
NEW QUESTION 252
- (Exam Topic 4)
You have a Microsoft 365 tenant that uses an Azure Active Directory (Azure AD) tenant The Azure AD tenant syncs to an on-premises Active Directory domain by using an instance of Azure AD Connect.
You create a new Azure subscription
You discover that the synced on-premises user accounts cannot be assigned rotes in the new subscription. You need to ensure that you can assign Azure and Microsoft 365 roles to the synced Azure AD user accounts. What should you do first?

A. Change the Azure AD tenant used by the new subscription.
B. Configure the Azure AD tenant used by the new subscription to use pass-through authenticate
C. Configure the Azure AD tenant used by the new subscription to use federated authentication.
D. Configure a second instance of Azure AD Connect.

Answer: A

NEW QUESTION 254
- (Exam Topic 4)
You have an Azure subscription named Subscription1.
You deploy a Linux virtual machine named VM1 to Subscription1. You need to monitor the metrics and the logs of VM1.
D18912E1457D5D1DDCBD40AB3BF70D5D
What should you use?

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

Answer: A

NEW QUESTION 255
- (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
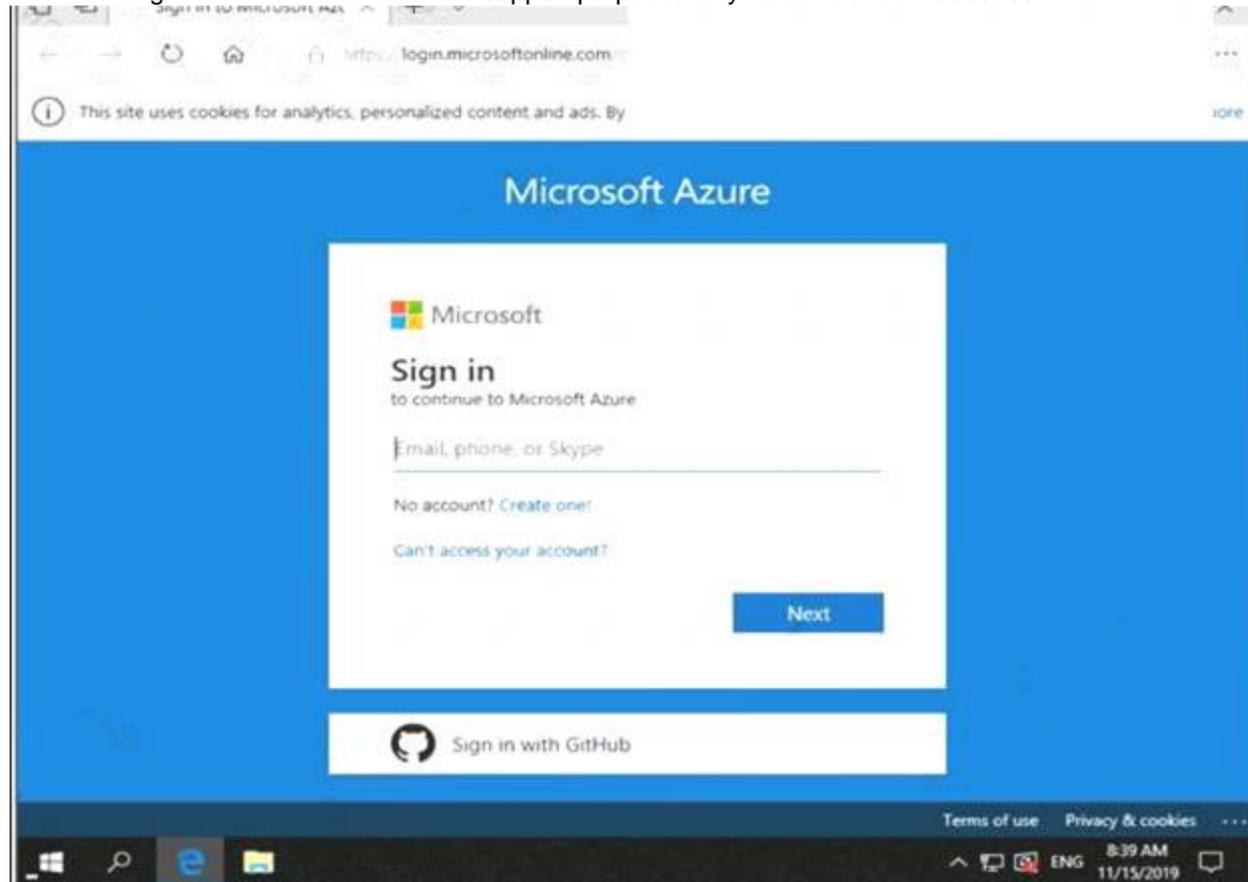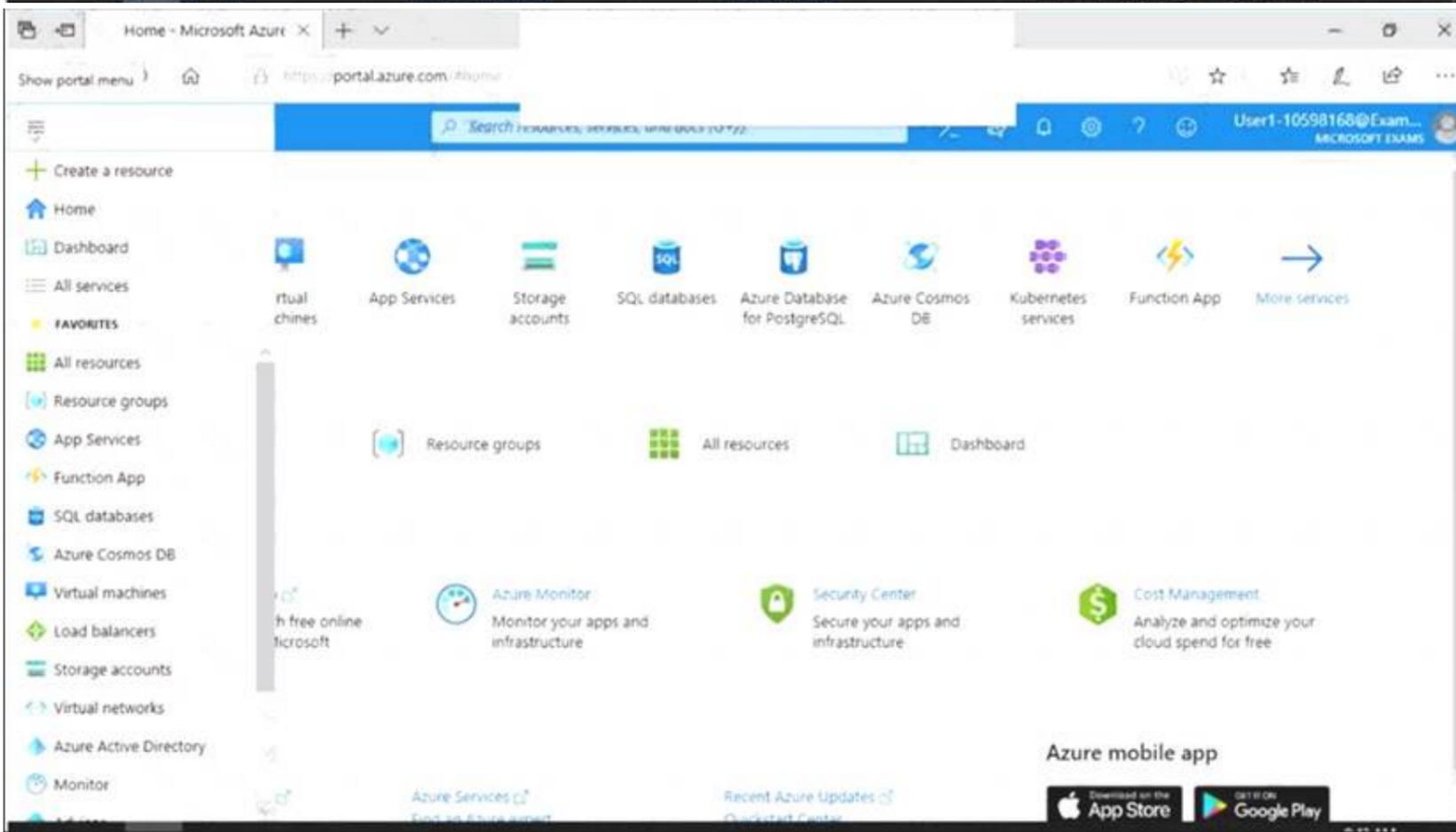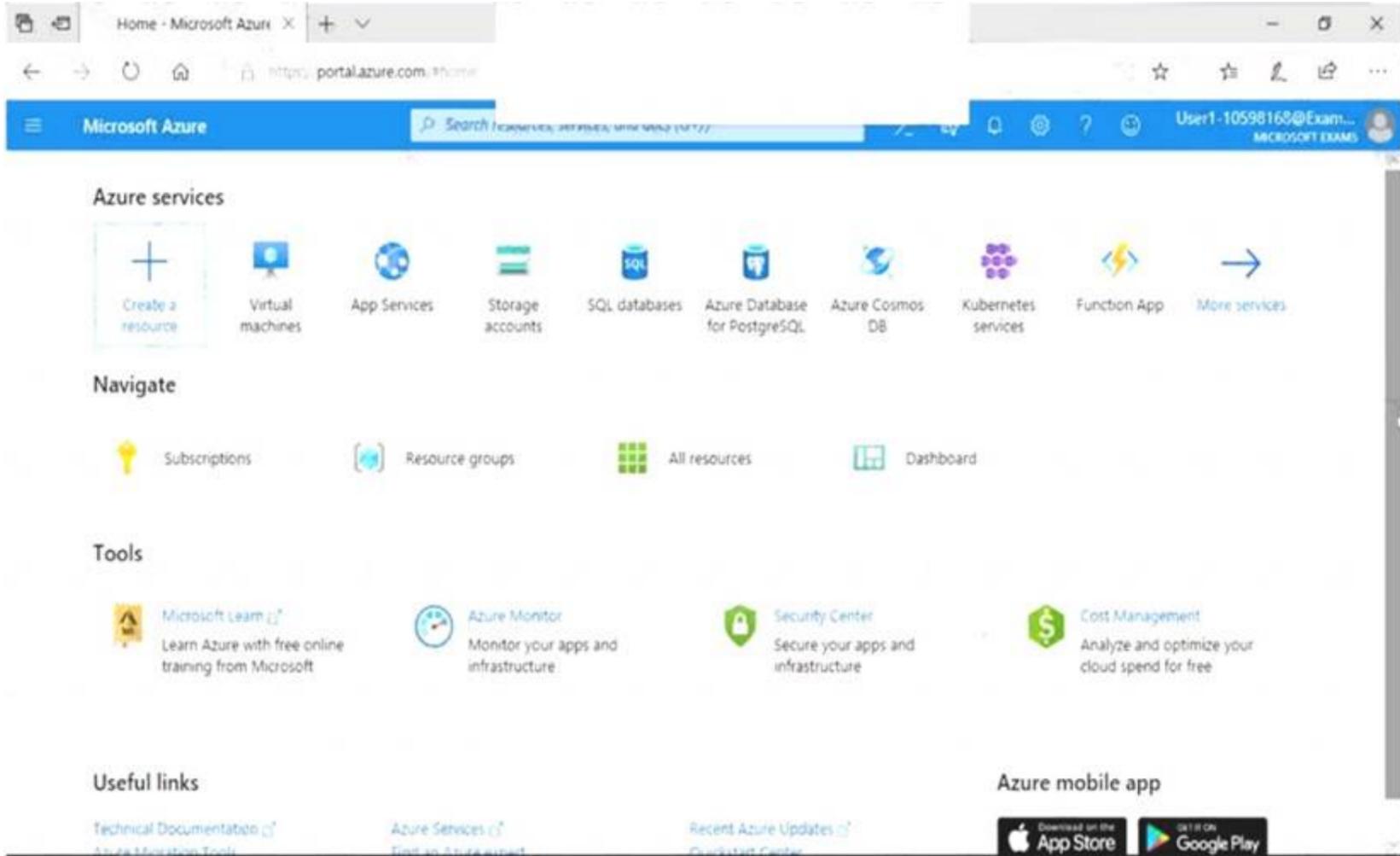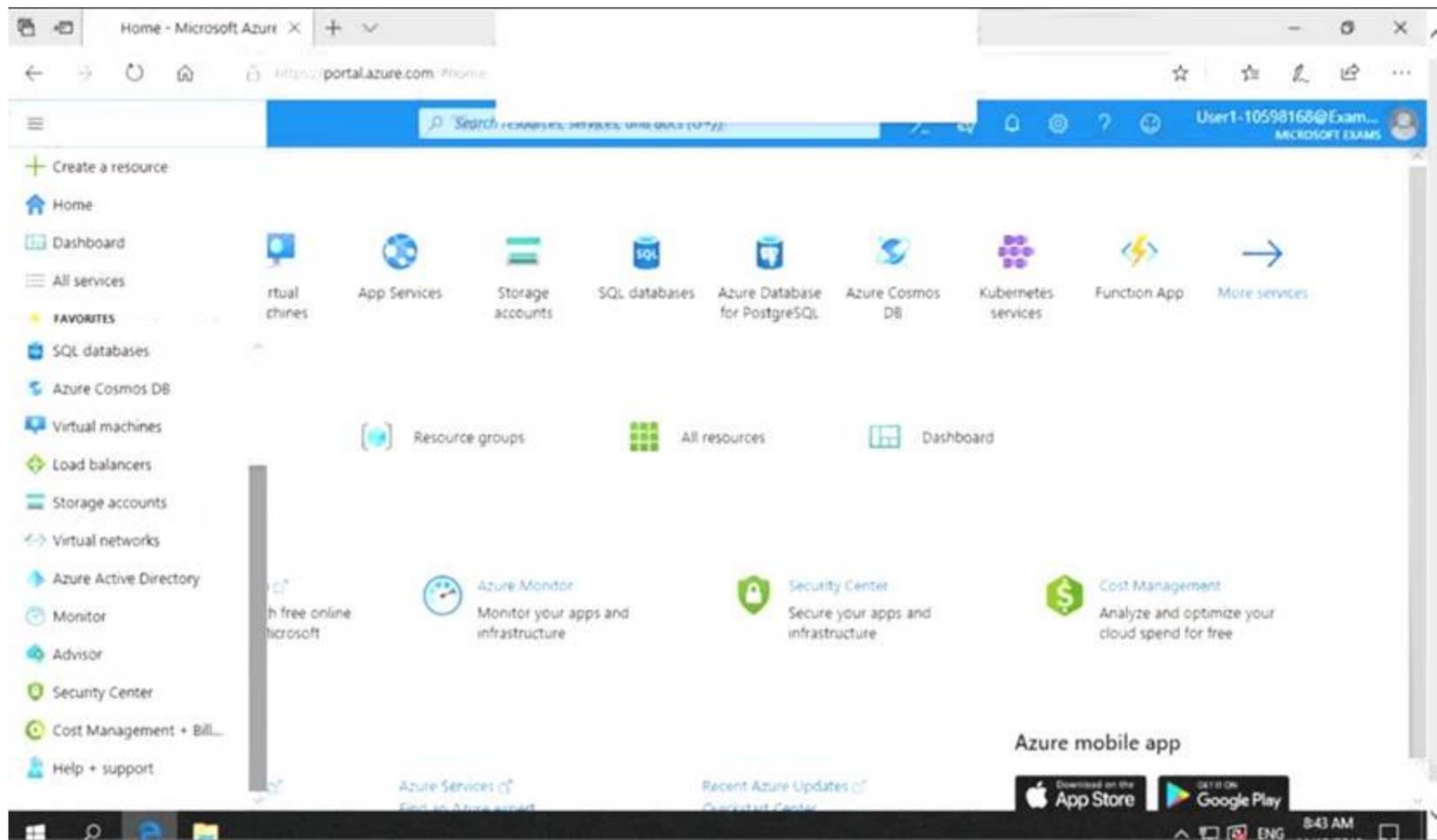
You need to configure Azure to allow RDP connections from the Internet to a virtual machine named VM1. The solution must minimize the attack surface of VM1.
To complete this task, sign in to the Azure portal.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
To enable the RDP port in an NSG, follow these steps:

> Sign in to the Azure portal.

> In Virtual Machines, select VM1

> In Settings, select Networking.

> In Inbound port rules, check whether the port for RDP is set correctly. The following is an example of the configuration:
Priority: 300 Name: Port_3389
Port(Destination): 3389 Protocol: TCP
Source: Any Destinations: Any Action: Allow Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-nsg-problem

NEW QUESTION 260
- (Exam Topic 4)
From the Azure portal, you are configuring an Azure policy.
You plan to assign policies that use the DeployIfNotExist, AuditIfNotExist, Append, and Deny effects.
Which effect requires a managed identity for the assignment?

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

Answer: C

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

NEW QUESTION 261
- (Exam Topic 4)
You need to enable Advanced Data Security for the SQLdb1 Azure SQL database. The solution must ensure that Azure Advanced Threat Protection (ATP) alerts
are sent to User1@contoso.com.
To complete this task, sign in to the Azure portal and modify the Azure resources.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

>

In the Azure portal, type SQL in the search box, select SQL databases from the search results then select SQLdb1. Alternatively, browse to SQL databases in the left navigation pane.

⟩ In the properties of SQLdb1, scroll down to the Security section and select Advanced data security.

⟩ Click on the Settings icon.

⟩ Tick the Enable Advanced Data Security at the database level checkbox.

⟩ Click Yes at the confirmation prompt.

⟩ In the Storage account select a storage account if one isn't selected by default.

⟩ Under Advanced Threat Protection Settings, enter User1@contoso.com in the Send alerts to box.

⟩ Click the Save button to save the changes.

Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/database/advanced-data-security

NEW QUESTION 265
- (Exam Topic 4)
You have an Azure subscription that has a managed identity named identity and is linked to an Azure Active Directory (Azure AD) tenant. The tenant contains the resources shown in the following table.
Which resources can be added to AUI and AU2? To answer, select the appropriate options in the answer area.

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

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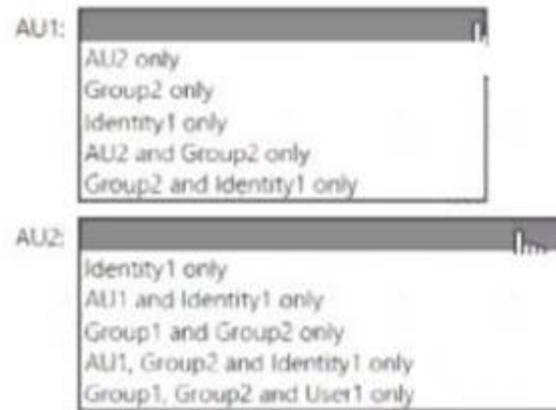
Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

NEW QUESTION 267
- (Exam Topic 4) You have an Azure SQL database. You implement Always Encrypted.
You need to ensure that application developers can retrieve and decrypt data in the database.
Which two pieces of information should you provide to the developers? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. a stored access policy
B. a shared access signature (SAS)
C. the column encryption key
D. user credentials
E. the column master key

Answer: CE

Explanation:
Always Encrypted uses two types of keys: column encryption keys and column master keys. A column encryption key is used to encrypt data in an encrypted column. A column master key is a key-protecting key that encrypts one or more column encryption keys.
References:
https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine

NEW QUESTION 272
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a hybrid configuration of Azure Active Directory (AzureAD). You have an Azure HDInsight cluster on a virtual network.
You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials. You need to configure the environment to support the planned authentication.
Solution: You deploy the On-premises data gateway to the on-premises network. Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 273
- (Exam Topic 4)
You have an Azure Active directory tenant that syncs with an Active Directory Domain Services (AD DS) domain.
You plan to create an Azure file share that will contain folders and files.
Which identity store can you use to assign permissions to the Azure file share and folders within the share? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Azure files share:	▼
Folders in the file share:	▼

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Azure files share:	AD DS only ▼
Folders in the file share:	AD DS and Azure AD ▼

NEW QUESTION 275
- (Exam Topic 4)
You need to ensure that a user named Danny11597200 can sign in to any SQL database on a Microsoft SQL server named web11597200 by using SQL Server Management Studio (SSMS) and Azure Active Directory (Azure AD) credentials.
To complete this task, sign in to the Azure portal.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
You need to provision an Azure AD Admin for the SQL Server.
≫ In the Azure portal, type SQL Server in the search box, select SQL Server from the search results then select the server named web11597200. Alternatively, browse to SQL Server in the left navigation pane.

> In the SQL Server properties page, click on Active Directory Admin.
> Click the Set Admin button.
> In the Add Admin window, search for and select Danny11597200.
> Click the Select button to add Danny11597200.
> Click the Save button to save the changes. Reference:
https://docs.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-configure?tabs=azure-powershell

NEW QUESTION 279
- (Exam Topic 4)
You have a Azure subscription.
You enable Azure Active Directory (Azure AD) Privileged identify (PIM).
Your company's security policy for administrator accounts has the following conditions:
* The accounts must use multi-factor authentication (MFA).
* The account must use 20-character complex passwords.
* The passwords must be changed every 180 days.
* The account must be managed by using PIM.
You receive alerts about administrator who have not changed their password during the last 90 days. You need to minimize the number of generated alerts.
Which PIM alert should you modify?

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

Answer: D

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

NEW QUESTION 283
- (Exam Topic 4)
You have an Azure subscription that contains a virtual network. The virtual network contains the subnets shown in the following table.

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

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

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

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

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

Answer: C

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

NEW QUESTION 288
......

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your az-500 Exam with Our Prep Materials Via below:

https://www.certleader.com/az-500-dumps.html