

Microsoft

Exam Questions az-500

Microsoft Azure Security Technologies



NEW QUESTION 1

- (Exam Topic 4)

You are securing access to the resources in an Azure subscription.

A new company policy states that all the Azure virtual machines in the subscription must use managed disks. You need to prevent users from creating virtual machines that use unmanaged disks.

What should you use?

- A. Azure Monitor
- B. Azure Policy
- C. Azure Security Center
- D. Azure Service Health

Answer: B

NEW QUESTION 2

- (Exam Topic 4)

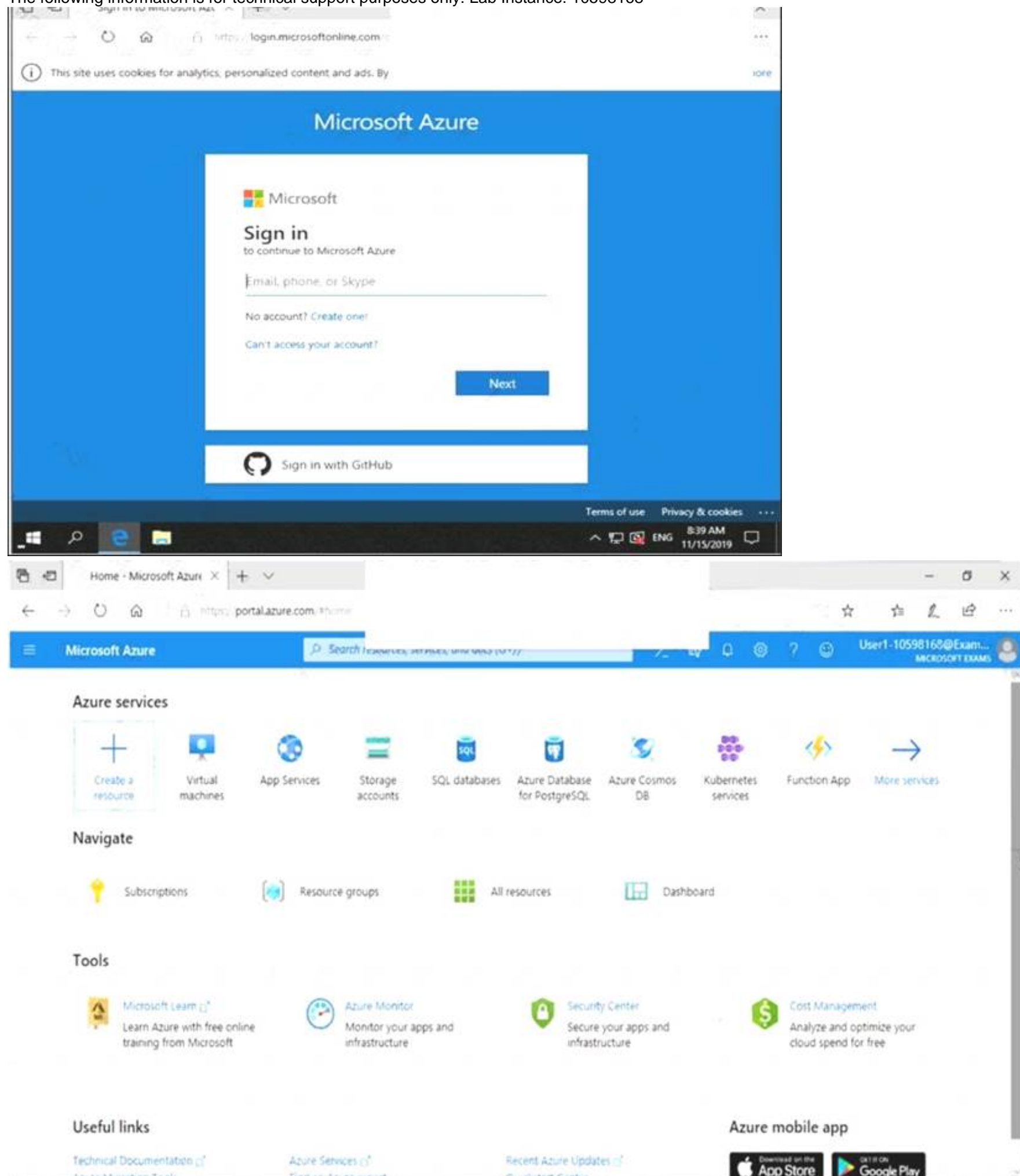
Use the following login credentials as needed:

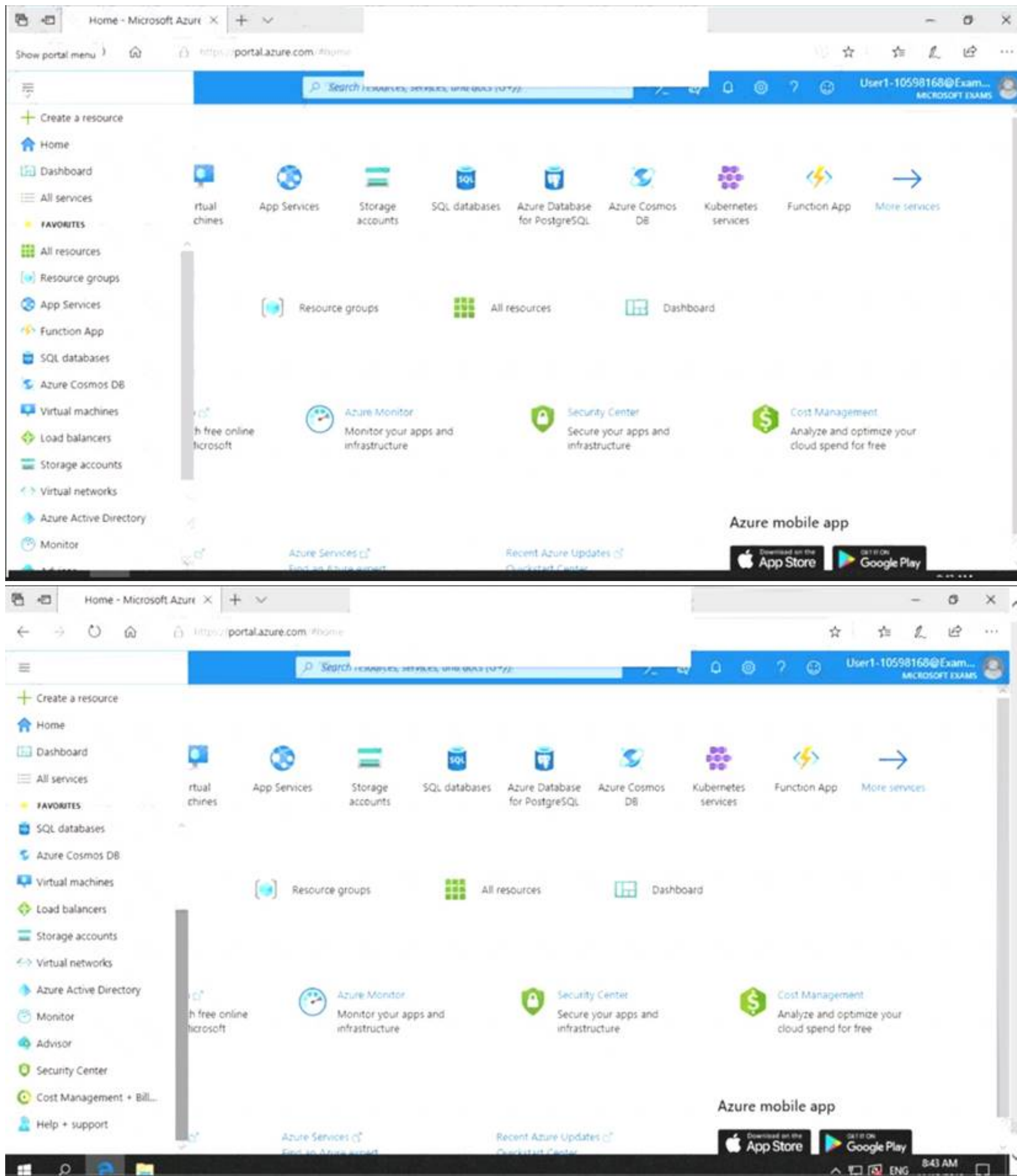
To enter your username, place your cursor in the Sign in box and click on the username below.

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.

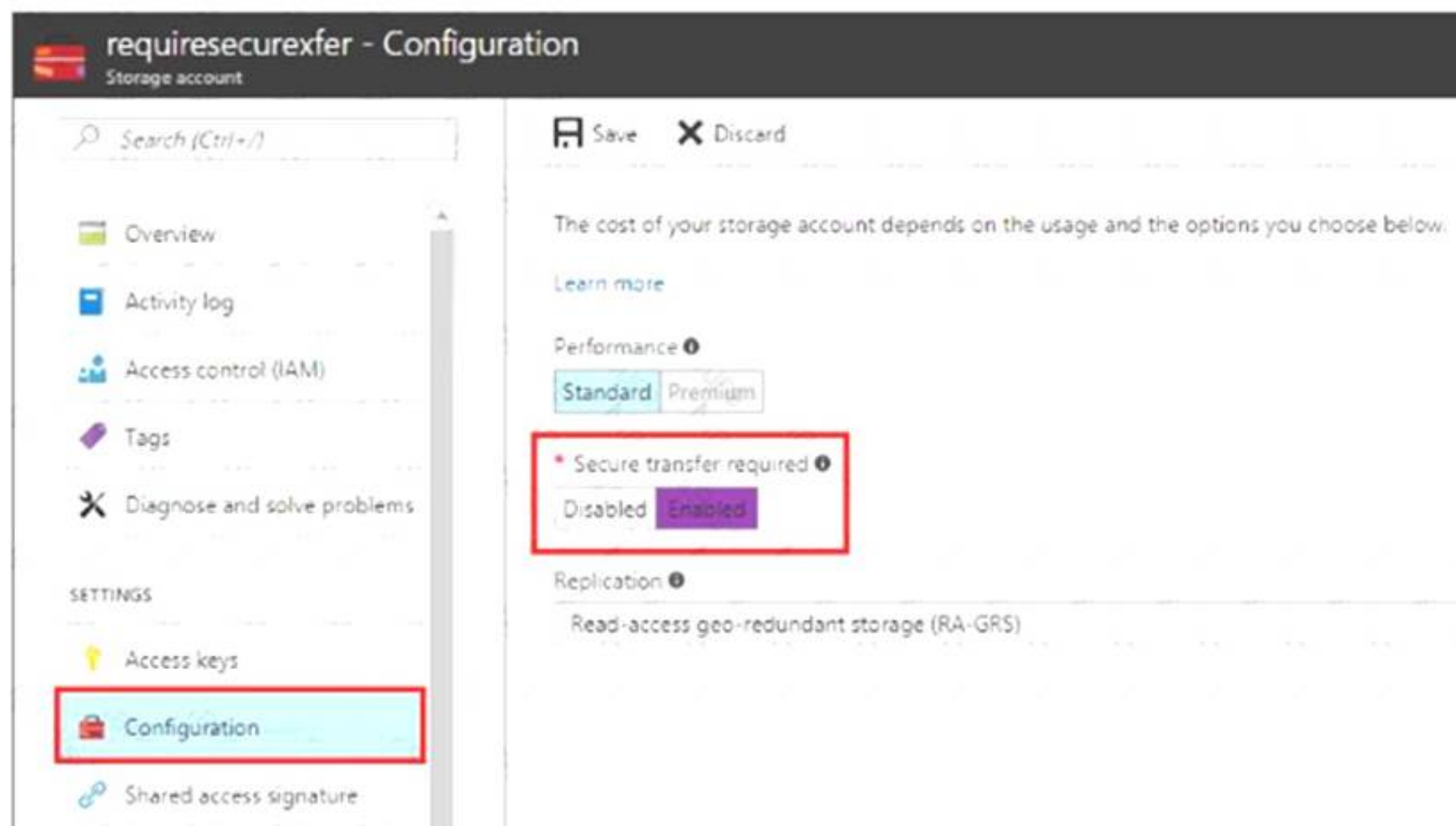
- A. Mastered
- B. Not Mastered

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)

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 configuration policies in Microsoft Intune
- B. an Azure Desired State Configuration (DSC) virtual machine extension
- C. security policies in Azure Security Center
- D. Azure Logic Apps

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

DSC-Service 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.

Reference:

<https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started>

NEW QUESTION 4

- (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 logout

Lockout threshold ⓘ ✓

Lockout duration in seconds ⓘ ✓

Custom banned passwords

Enforce custom list ⓘ

Yes

No

Custom banned password list ⓘ

Adatum

✓

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ

Yes

No

Mode ⓘ

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.	<input type="radio"/>	<input type="radio"/>
User2 can change the password to @d@tum_C0mpleX123.	<input type="radio"/>	<input type="radio"/>
User3 can change the password to Adatum123!.	<input type="radio"/>	<input type="radio"/>

- 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 5

- (Exam Topic 4)

You have an Azure subscription that contains a user named User1 and a storage account named storage 1. The storage1 account contains the resources shown in the following table:

Name	Type
container1	Container
folder1	File share
table1	Table

User1 is assigned the following roles for storage1:

- Storage Blob Data Reader
- Storage Table Data Contributor
- Storage File Data SMB Share Reader

Statements	Yes	No
On October 1, 2022, if User1 accesses folder1 by using SAS1, he can delete the files in folder1.	<input type="radio"/>	<input type="radio"/>
On October 1, 2022, if User1 maps folder1 as a network drive by using his Azure Active Directory (Azure AD) credentials, he can delete the files in folder1.	<input type="radio"/>	<input type="radio"/>
On October 1, 2022, User1 can delete the rows in table1 by using SAS1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:
No, Yes, No

NEW QUESTION 6

- (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: <input type="text"/>
Metrics	Query the security events of a virtual machine that runs Windows Server 2016: <input type="text"/>
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 7

- (Exam Topic 4)

You need to configure a weekly backup of an Azure SQL database named Homepage. The backup must be retained for eight weeks. To complete this task, sign in to the Azure portal.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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

NEW QUESTION 8

- (Exam Topic 4)

Your company has an Azure subscription named Subscription1 that contains the users shown in the following table.

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

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

User:

▼

User1

User2

User3

User4

Tool:

▼

Azure Account Center

Azure Cloud Shell

Azure PowerShell

Azure Security Center

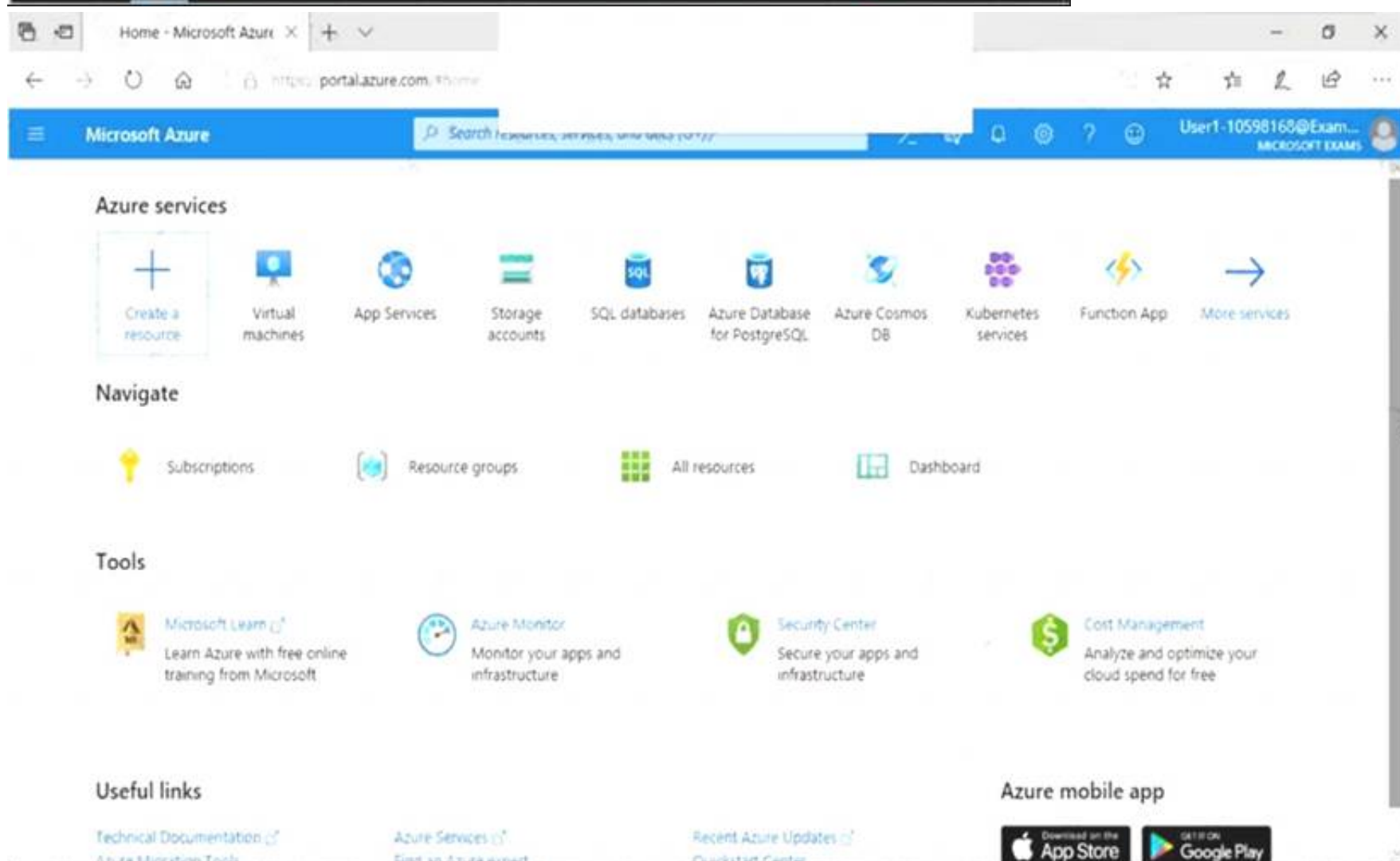
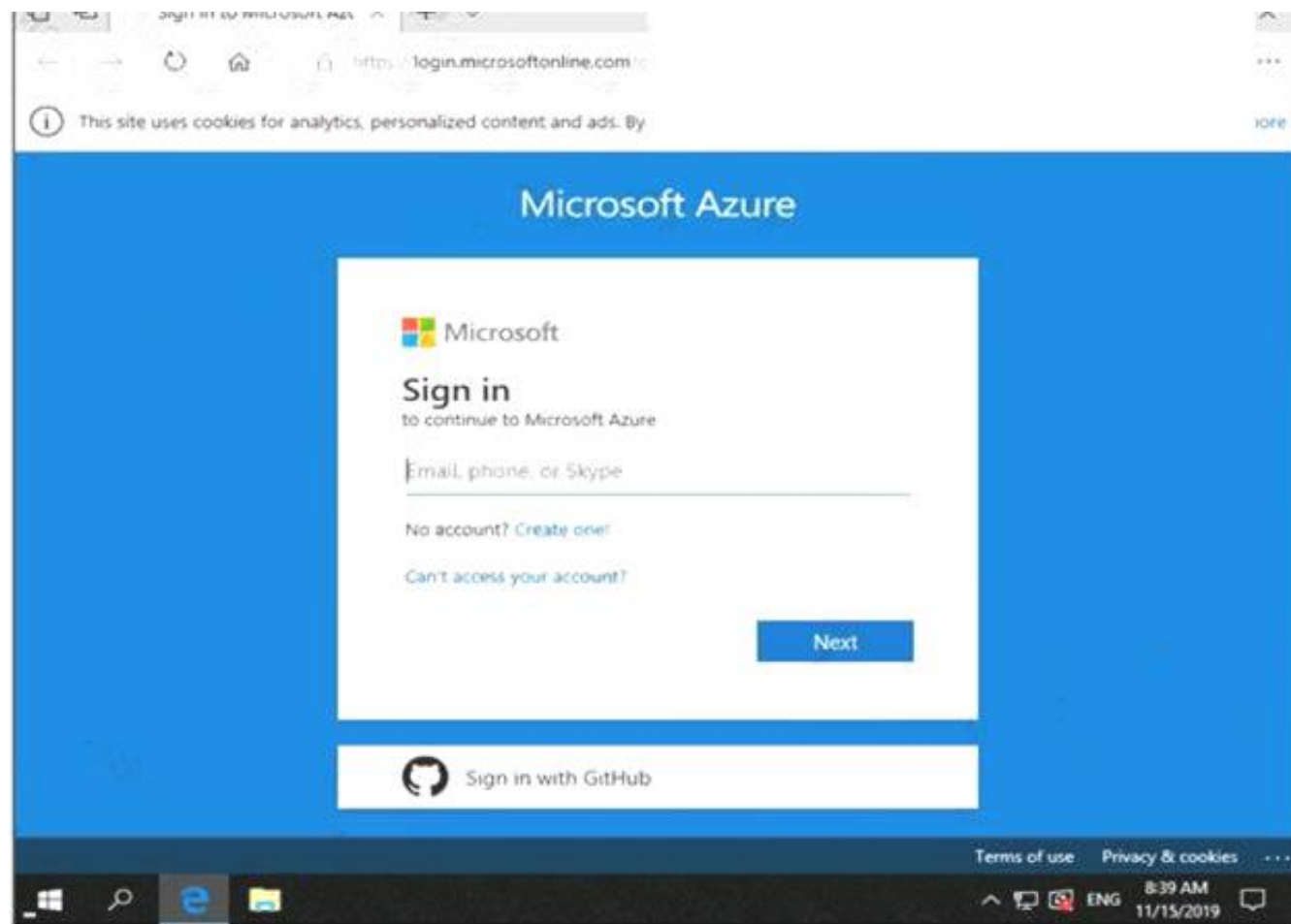
- A. Mastered
- B. Not Mastered

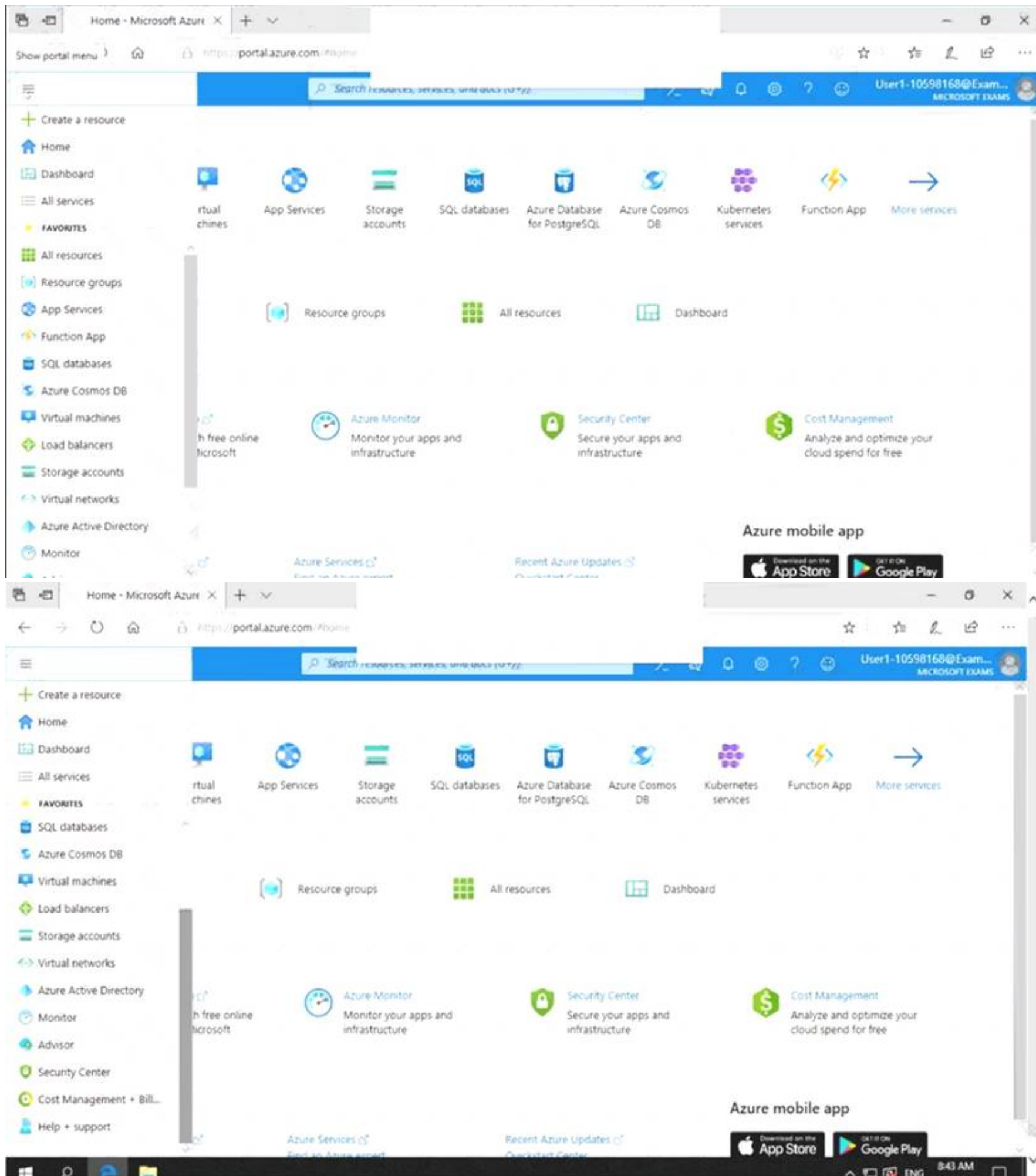
Answer: A

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

NEW QUESTION 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 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+J)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
- Networking
- Disks
- Size
- Security
- Extensions**

+ Add

Search to filter items...

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

* 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 10

- (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 10

- (Exam Topic 4)

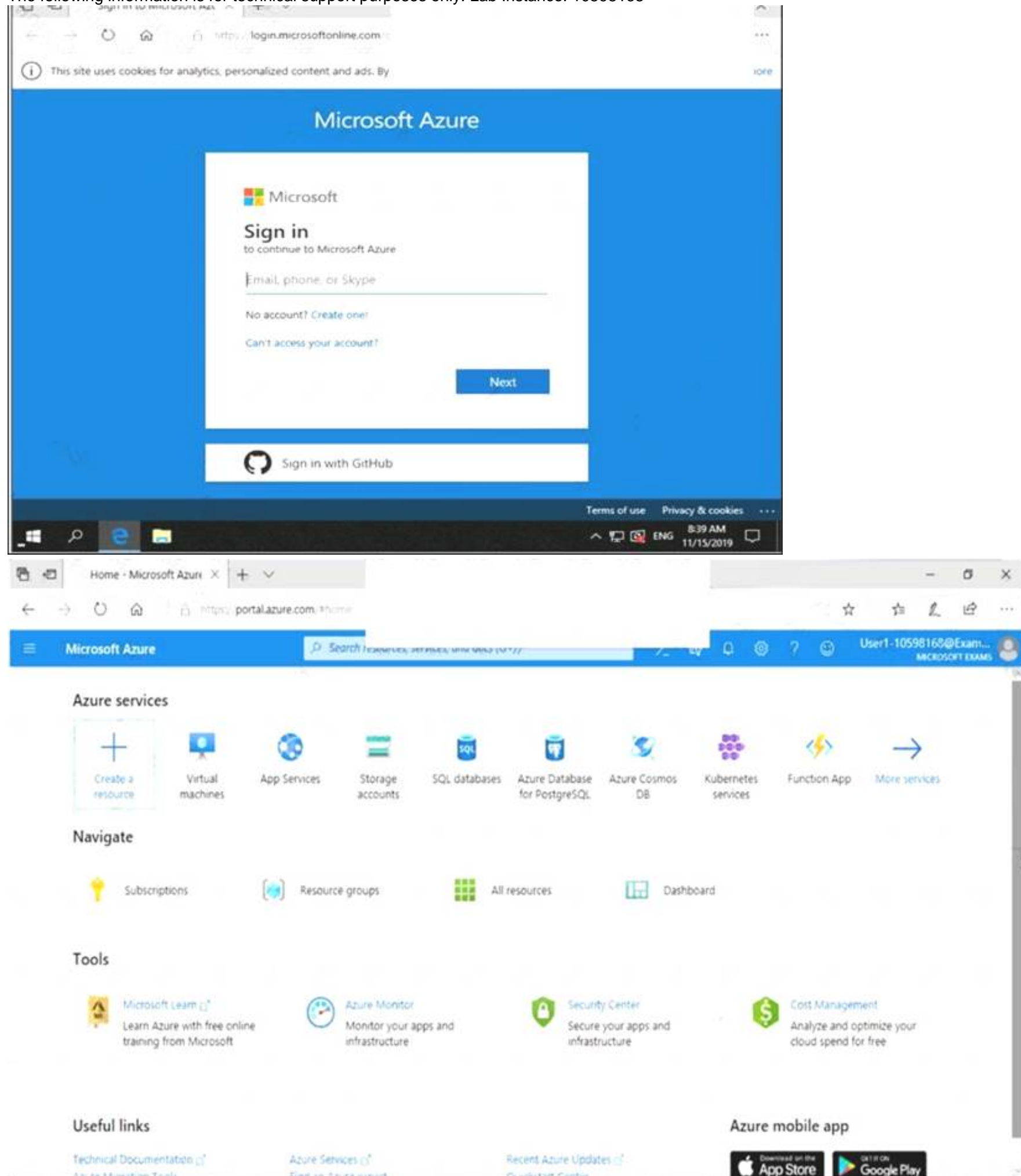
Use the following login credentials as needed:

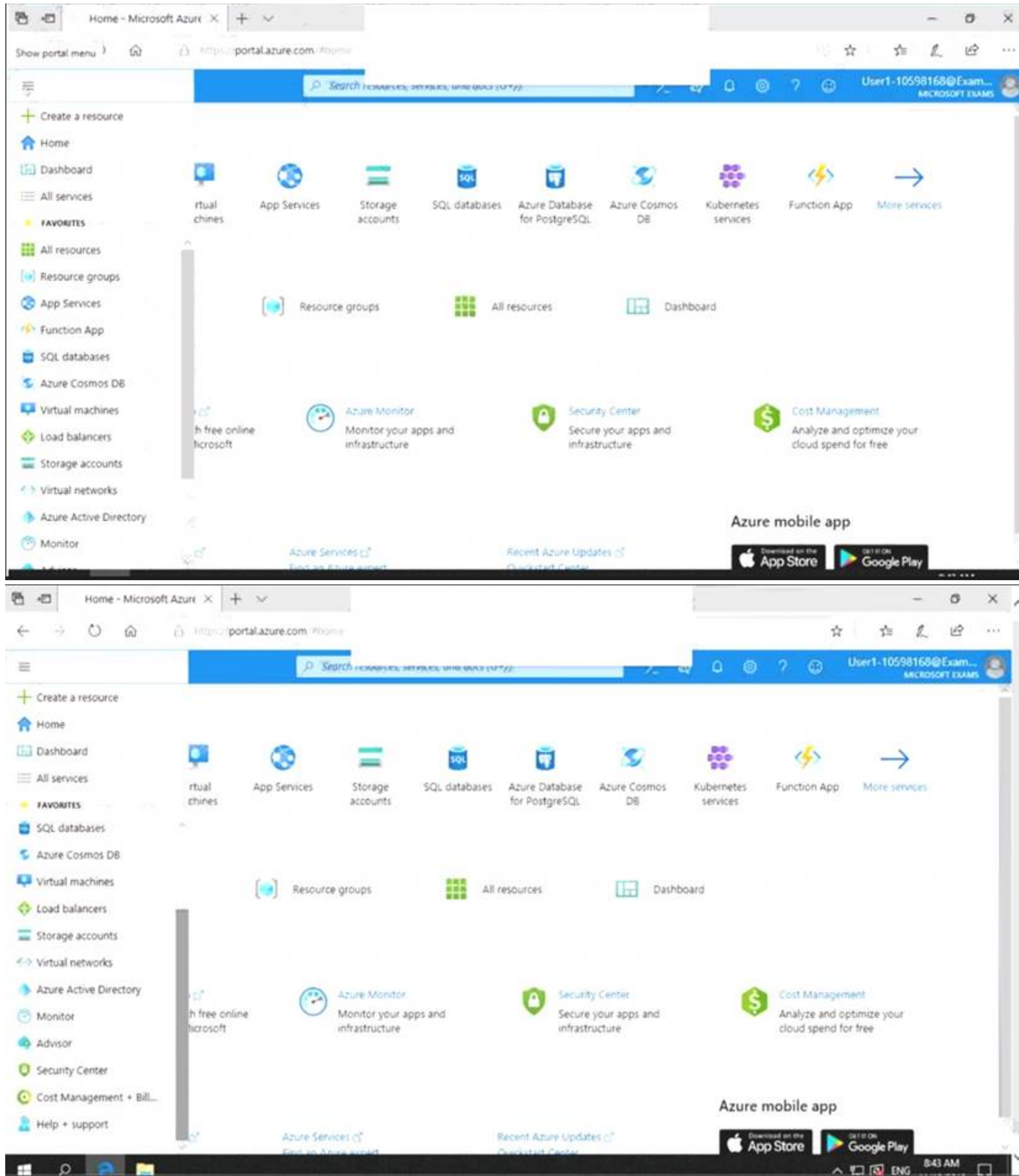
To enter your username, place your cursor in the Sign in box and click on the username below.

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 13

- (Exam Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription named Sub1.

You have an Azure Storage account named Sa1 in a resource group named RG1.

Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.

You discover that unauthorized users accessed both the file service and the blob service. You need to revoke all access to Sa1.

Solution: You create a lock on Sa1. Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it.

References:

<https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy>

NEW QUESTION 17

- (Exam Topic 4)

Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD). Azure AD Connect is installed on a domain member server named Server1.

You need to ensure that a domain administrator for the adatum.com domain can modify the synchronization options. The solution must use the principle of least privilege.

Which Azure AD role should you assign to the domain administrator?

A. Security administrator

B. Global administrator

C. User administrator

Answer: B

Explanation:

Reference:

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

NEW QUESTION 21

- (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

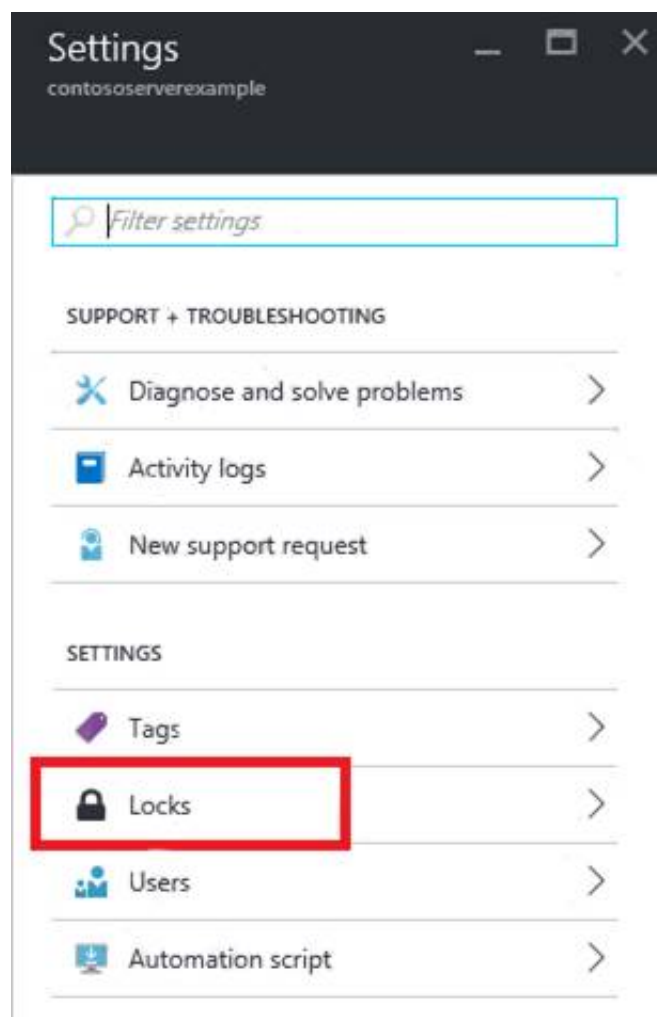
Explanation:

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

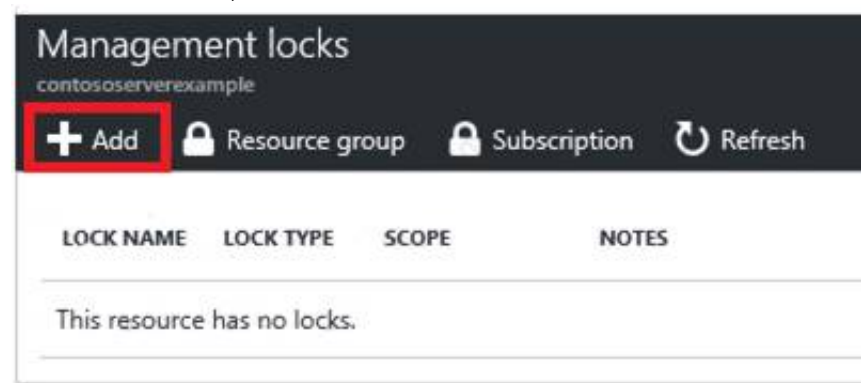
Note: In Azure, the term resource refers to an entity managed by Azure. For example, virtual machines, virtual networks, and storage accounts are all referred to as Azure resources.

* 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 26

- (Exam Topic 4)

You have an Azure subscription named Sub1 that contains the Azure key vaults shown in the following table:

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

In Sub1, you create a virtual machine that has the following configurations:

- > Name: VM1
- > Size: DS2v2
- > Resource group: RG1
- > Region: West Europe
- > Operating system: Windows Server 2016

You plan to enable Azure Disk Encryption on VM1.

In which key vaults can you store the encryption key for VM1?

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

Answer: A

Explanation:

In order to make sure the encryption secrets don't cross regional boundaries, Azure Disk Encryption needs the Key Vault and the VMs to be co-located in the same region. Create and use a Key Vault that is in the same region as the VM to be encrypted.

Reference:

<https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-prerequisites>

NEW QUESTION 30

- (Exam Topic 4)

You are testing an Azure Kubernetes Service (AKS) cluster. The cluster is configured as shown in the exhibit. (Click the Exhibit tab.)

BASICS

Subscription	Microsoft Azure Sponsorship
Resource group	AzureBackupRG_eastus2_1
Region	East US
Kubernetes cluster name	akscluster2
Kubernetes version	1.1 1.5
DNS name prefix	akscluster2
Node count	3
Node size	Standard_DS2_v2
Virtual nodes (preview)	Disabled

AUTHENTICATION

Enable RBAC	No
-------------	----

NETWORKING

HTTP application routing	Yes
Network configuration	Basic

MONITORING

Enable container monitoring	No
-----------------------------	----

TAGS

You plan to deploy the cluster to production. You disable HTTP application routing.

You need to implement application routing that will provide reverse proxy and TLS termination for AKS services by using a single IP address.

What should you do?

- A. Create an AKS Ingress controller.
- B. Install the container network interface (CNI) plug-in.
- C. Create an Azure Standard Load Balancer.
- D. Create an Azure Basic Load Balancer.

Answer: A

Explanation:

An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services.

References:

<https://docs.microsoft.com/en-us/azure/aks/ingress-tls>

NEW QUESTION 32

- (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 33

- (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 38

- (Exam Topic 4)

You have an Azure subscription.

You plan to create a workflow automation in Azure Security Center that will automatically remediate a security vulnerability.

What should you create first?

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

Answer: E

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/workflow-automation>

NEW QUESTION 40

- (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.

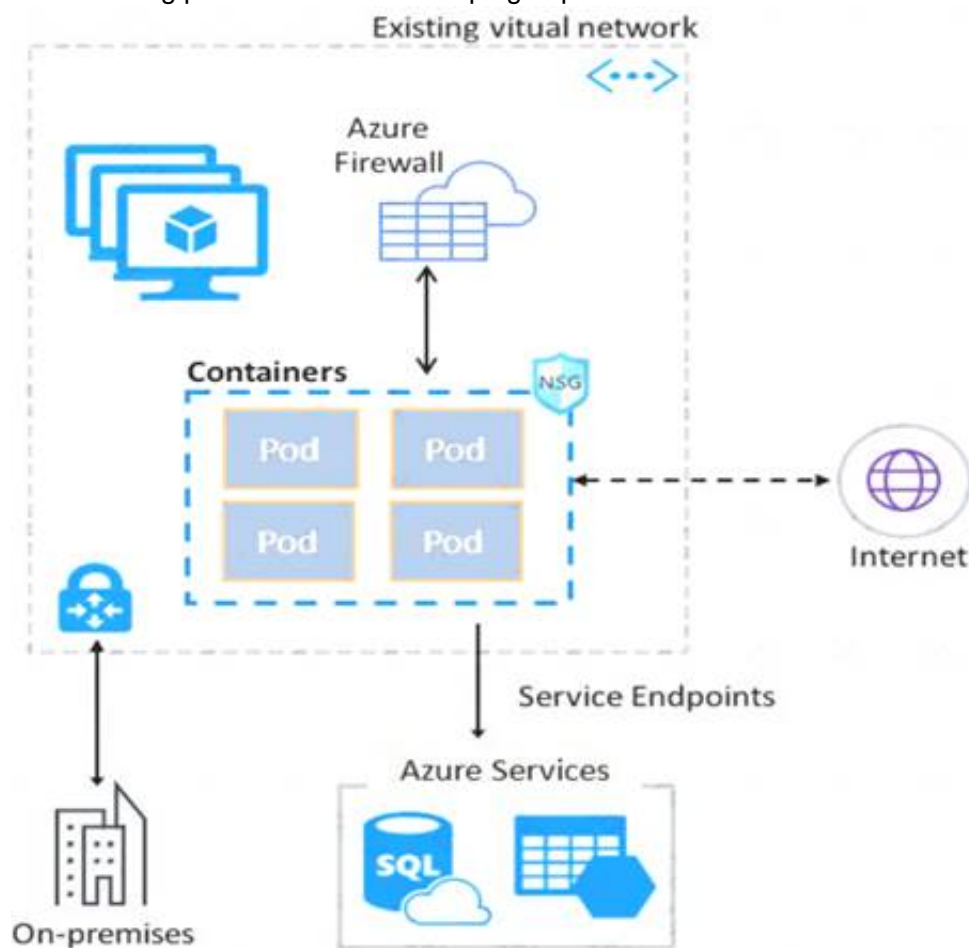
Answer: C

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 43

- (Exam Topic 4)

You have an Azure subscription that contains the Azure virtual machines shown in the following table.

Name	Operating system
VM1	Windows 10
VM2	Windows Server 2016
VM3	Windows Server 2019
VM4	Ubuntu Server 18.04 LTS

You create an MDM Security Baseline profile named Profile1.

You need to identify to which virtual machines Profile1 can be applied. Which virtual machines should you identify?

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

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines>

NEW QUESTION 45

- (Exam Topic 4)

You are troubleshooting a security issue for an Azure Storage account.

You enable the diagnostic logs for the storage account. What should you use to retrieve the diagnostics logs?

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

Answer: D

Explanation:

References:

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

NEW QUESTION 49

- (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 52

- (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	<i>Not applicable</i>
storage2	East US	Premium	Block blobs
storage3	East US	Premium	File shares
storage4	East US 2	Standard	<i>Not applicable</i>

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

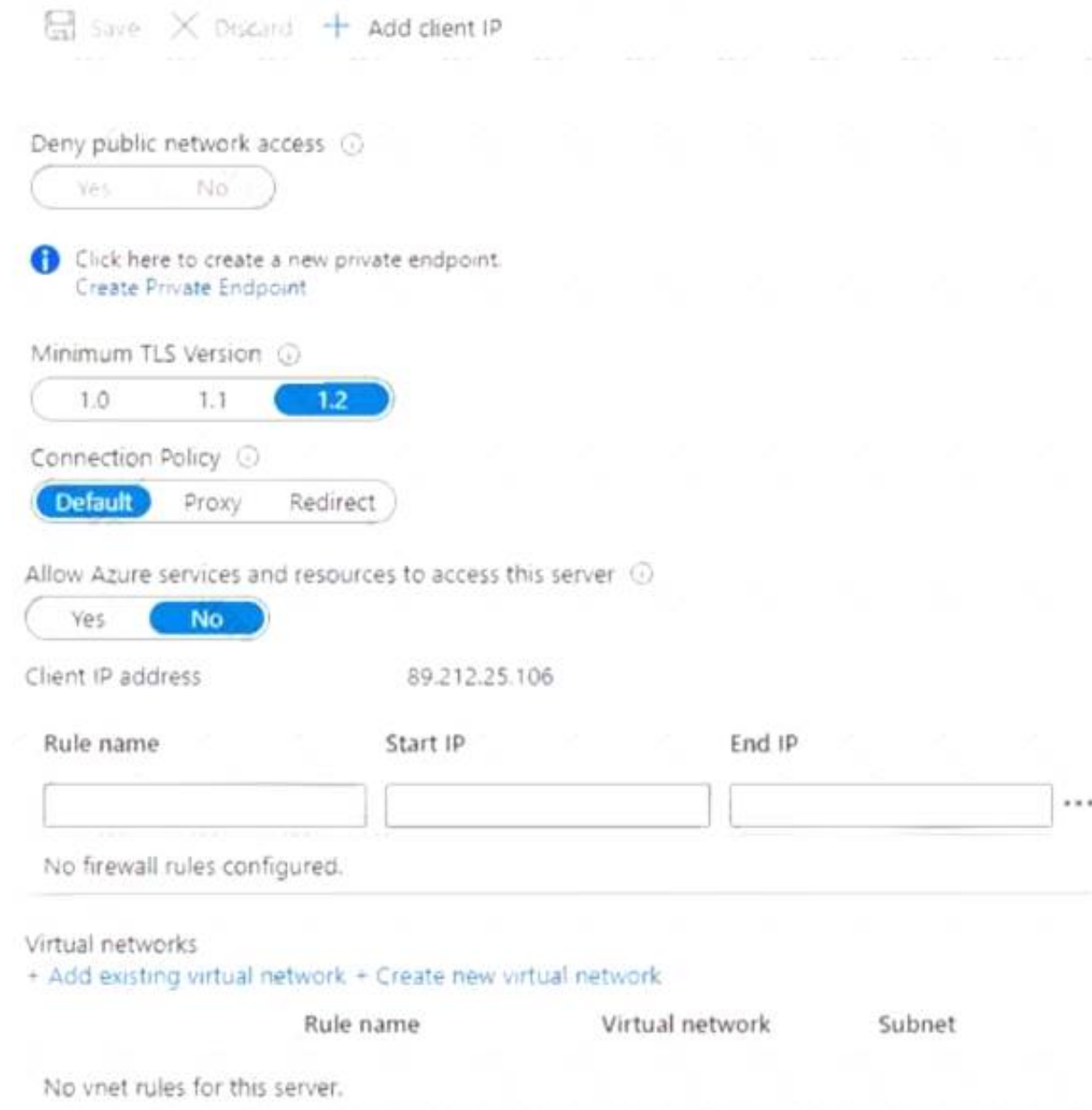
Answer: C

NEW QUESTION 56

- (Exam Topic 4)

You have an Azure subscription that contains an Azure SQL Database logic server named SQL1 and an Azure virtual machine named VM1. VM1 uses a private IP address only.

The Firewall and virtual networks settings for SQL1 are shown in the following exhibit.



The screenshot shows the Azure Firewall settings for a resource named SQL1. At the top, there are buttons for 'Save', 'Discard', and 'Add client IP'. Below this, the 'Deny public network access' toggle is set to 'No'. A link 'Click here to create a new private endpoint. Create Private Endpoint' is visible. The 'Minimum TLS Version' is set to '1.2'. The 'Connection Policy' is set to 'Default'. The 'Allow Azure services and resources to access this server' toggle is set to 'No'. The 'Client IP address' is '89.212.25.106'. Below this is a table for firewall rules with columns 'Rule name', 'Start IP', and 'End IP'. The table is empty, showing 'No firewall rules configured.' Below the table is a section for 'Virtual networks' with a link '+ Add existing virtual network + Create new virtual network'. Below this is another table with columns 'Rule name', 'Virtual network', and 'Subnet'. This table is also empty, showing 'No vnet rules for this server.'

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

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

Answer: C

NEW QUESTION 58

- (Exam Topic 4)

From Azure Security Center, you enable Azure Container Registry vulnerability scanning of the images in Registry1.

You perform the following actions:

- > Push a Windows image named Image1 to Registry1.
- > Push a Linux image named Image2 to Registry1.
- > Push a Windows image named Image3 to Registry1.
- > Modify Image1 and push the new image as Image4 to Registry1.
- > Modify Image2 and push the new image as Image5 to Registry1.

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

- A. Image4
- B. Image2
- C. Image1
- D. Image3
- E. Image5

Answer: BC

NEW QUESTION 63

- (Exam Topic 4)

You have an Azure subscription named Sub1.

In Azure Security Center, you have a workflow automation named WF1. WF1 is configured to send an email message to a user named User1.

You need to modify WF1 to send email messages to a distribution group named Alerts. What should you use to modify WF1?

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

Answer: C

Explanation:

Reference:

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

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

NEW QUESTION 68

- (Exam Topic 4)

You are configuring network connectivity for two Azure virtual networks named VNET1 and VNET2. You need to implement VPN gateways for the virtual networks to meet the following requirements:

* VNET1 must have six site-to-site connections that use BGP.

* VNET2 must have 12 site-to-site connections that use BGP.

* Costs must be minimized.

Which VPN gateway SKI) should you use for each virtual network? To answer, drag the appropriate SKUs to the correct networks. Each SKU may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point

SKUs

Basic

VpnGw1

VpnGw2

VpnGw3

Answer Area

VNET1:

SKU

VNET2:

SKU

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 70

- (Exam Topic 4)

You have an Azure subscription that contains the virtual machines shown in the following table.

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

You create the Azure policies shown in the following table.

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

You create the resource locks shown in the following table.

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
You can start VM1.	<input type="radio"/>	<input type="radio"/>
You can start VM2.	<input type="radio"/>	<input type="radio"/>
You can create a virtual machine in RG2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

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

NEW QUESTION 74

- (Exam Topic 4)
You have an Azure Sentinel workspace that has the following data connectors:

- > Azure Active Directory Identity Protection
- > Common Event Format (CEF)
- > Azure Firewall

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

Azure Active Directory Identity Protection:

AzureDiagnostics

CommonSecurityLog

SecurityAlert

SecurityEvent

Syslog

Azure Firewall:

AzureDiagnostics

CommonSecurityLog

SecurityAlert

SecurityEvent

Syslog

CEF:

AzureDiagnostics

CommonSecurityLog

SecurityAlert

SecurityEvent

Syslog

- A. Mastered
- B. Not Mastered

Answer: A

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

NEW QUESTION 77

- (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 79

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant named contoso1812.onmicrosoft.com that contains the users shown in the following table.

Name	Username	Type
User1	User1@contoso1812.onmicrosoft.com	Member
User2	User2@contoso1812.onmicrosoft.com	Member
User3	User3@contoso1812.onmicrosoft.com	Member
User4	User4@outlook.com	Guest

You create an Azure Information Protection label named Label1. The Protection settings for Label1 are configured as shown in the exhibit. (Click the Exhibit tab.)

Protection
Contoso1812 - Azure Information Protection

Protections settings ⓘ

Azure (cloud key)

HYOK (AD RMS)

Select the protection action type ⓘ

☒ Set permissions

☐ Set user-defined permissions (Preview)

USERS	PERMISSIONS
AuthenticatedUsers	Viewer
User1@contoso1812.onmicrosoft.com	Co-Author
User2@contoso1812.onmicrosoft.com	Reviewer

+Add permissions

Label1 is applied to a file named File1.

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

Statements	Yes	No
User1 can print File1.	<input type="radio"/>	<input type="radio"/>
User3 can read File1.	<input type="radio"/>	<input type="radio"/>
User4 can print File1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

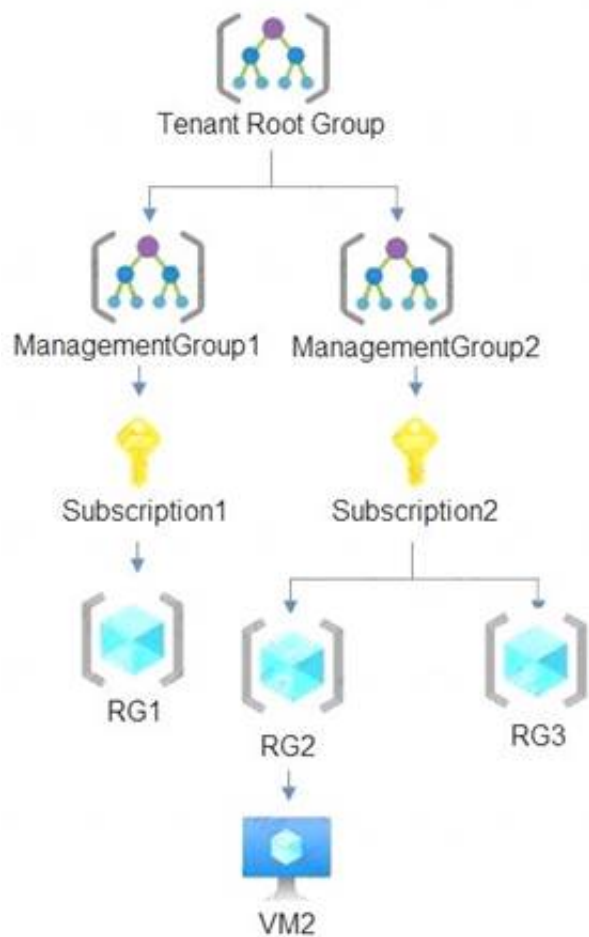
Answer: A

Explanation:

Statements	Yes	No
User1 can print File1.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can read File1.	<input checked="" type="radio"/>	<input type="radio"/>
User4 can print File1.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 81

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



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

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

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

Statements	Yes	No
User1 can deploy virtual machines to RG1.	<input type="radio"/>	<input type="radio"/>
User2 can delete VM2.	<input type="radio"/>	<input type="radio"/>
User3 can reset the password of the built-in Administrator account of VM2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can deploy virtual machines to RG1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can delete VM2.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can reset the password of the built-in Administrator account of VM2.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 83

- (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?

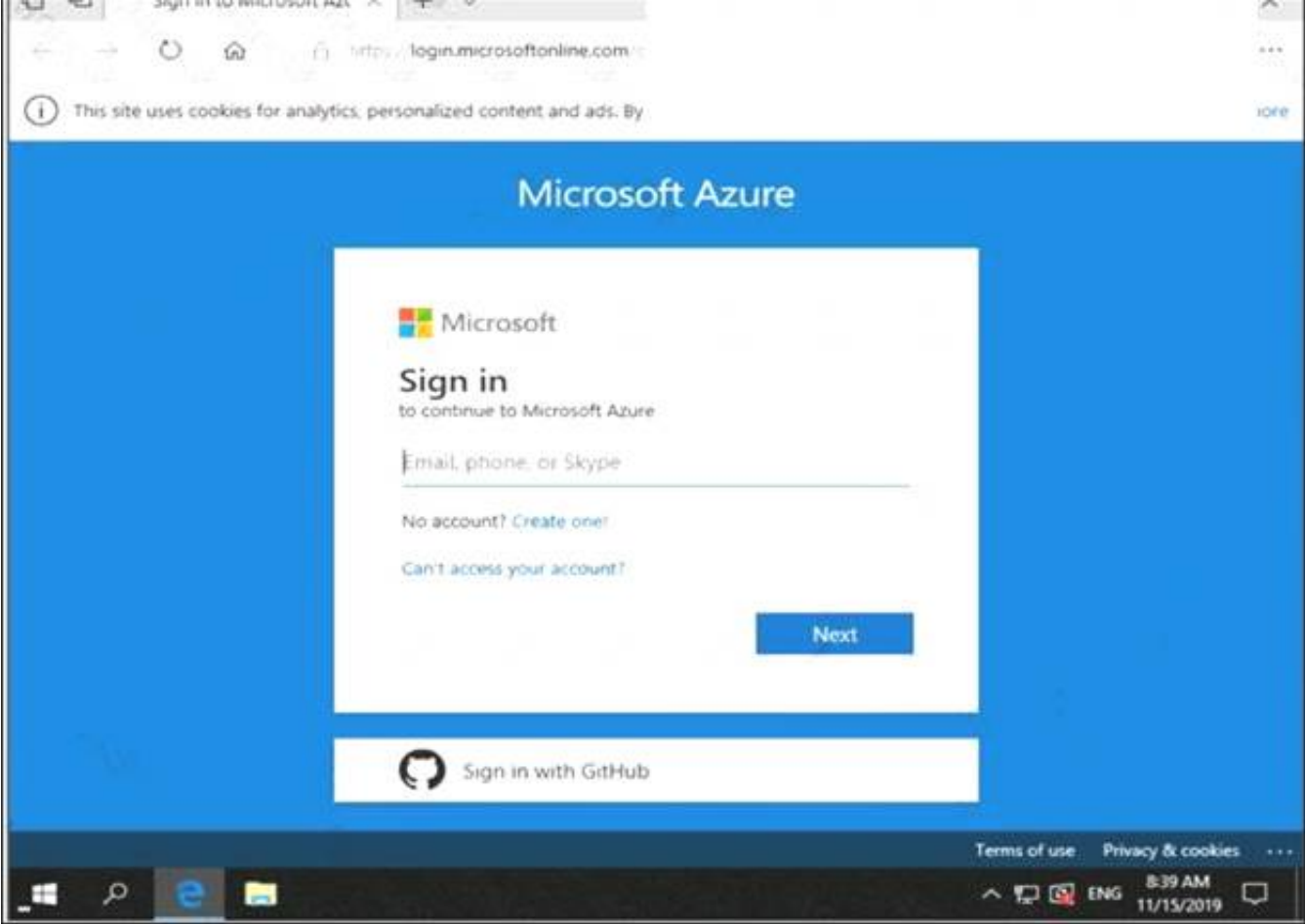
A. Azure Security Center
B. Azure Blueprints
C. Azure AD Privileged Identity Management (PIM)
D. Azure Policy

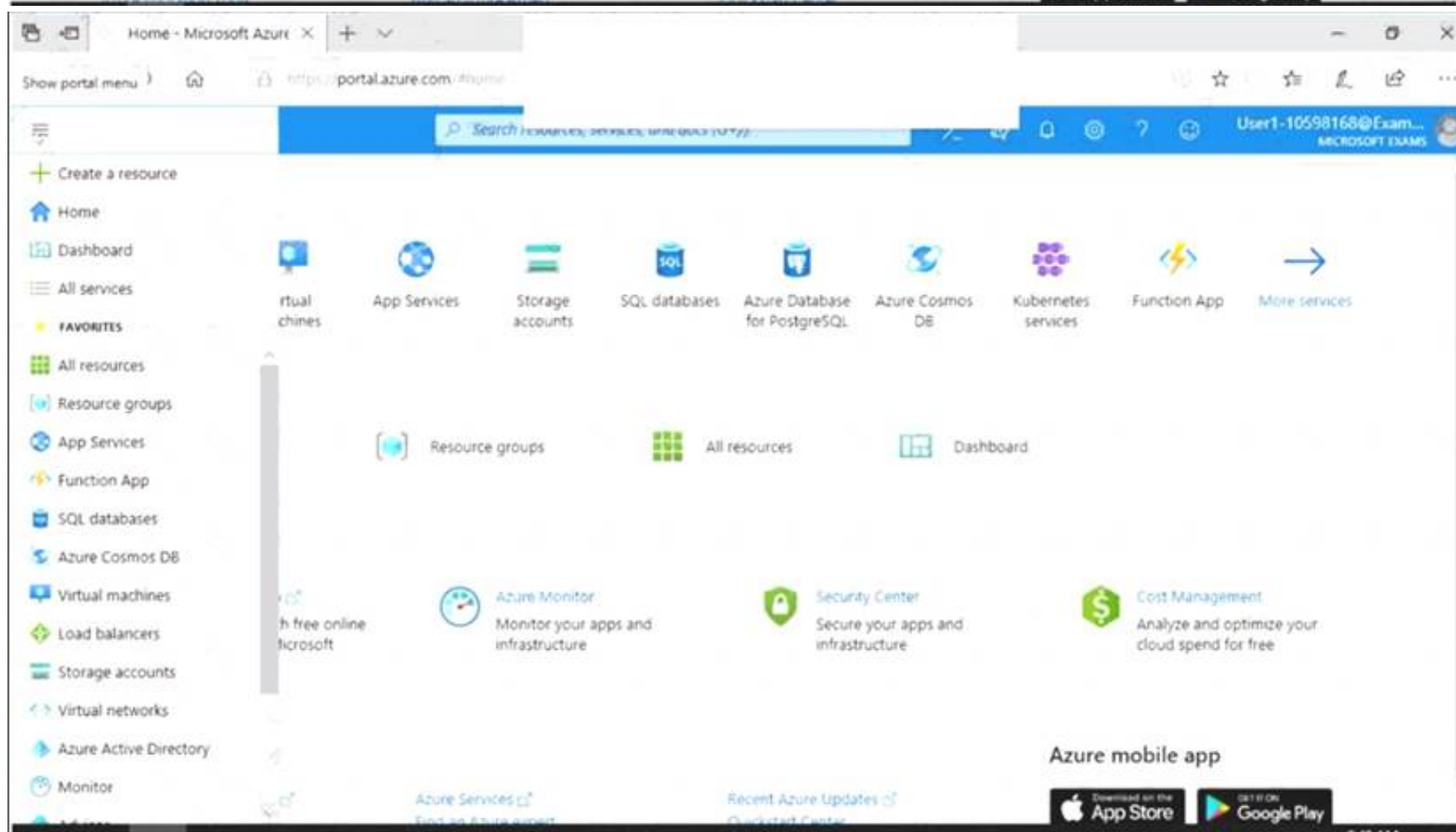
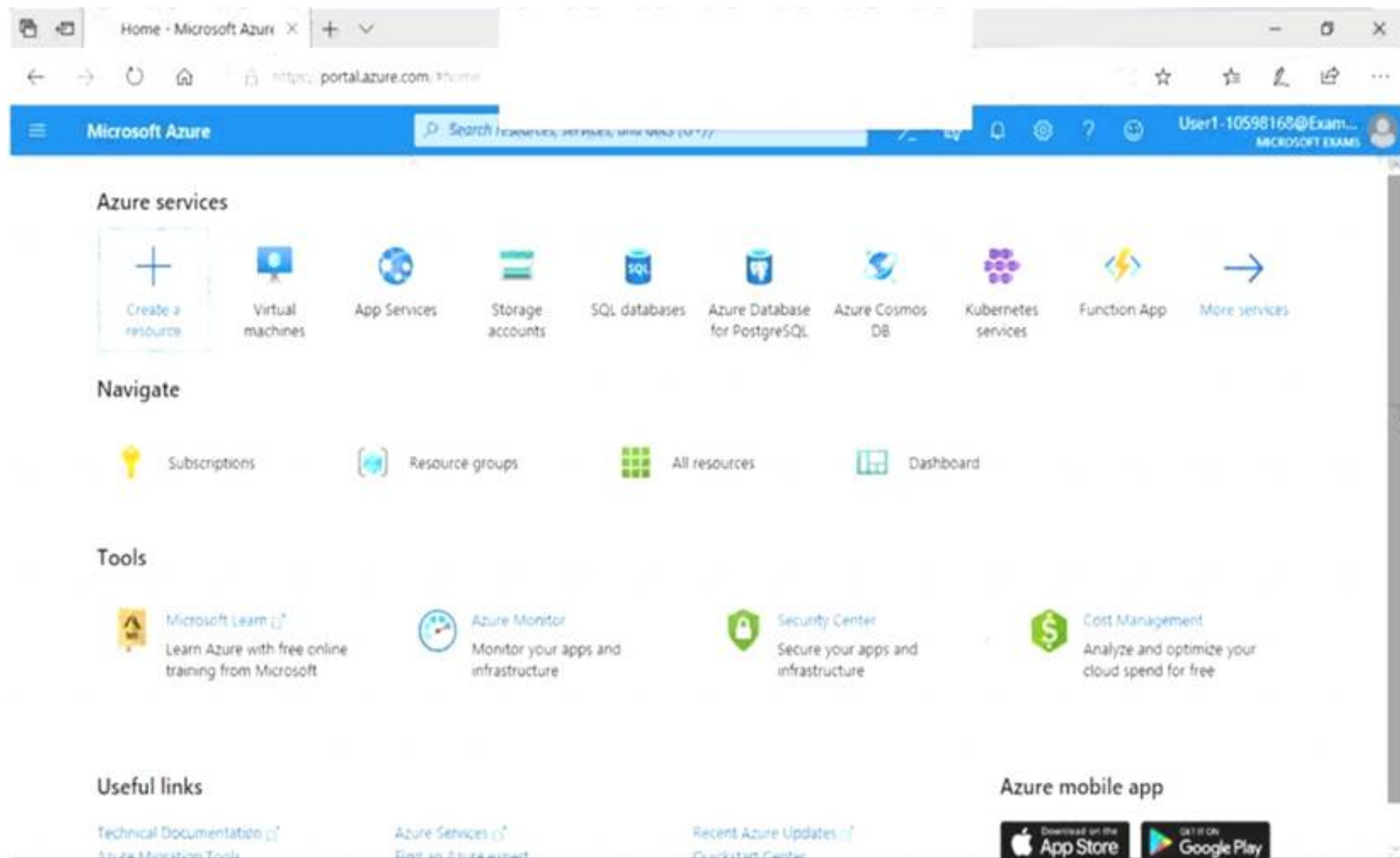
Answer: B

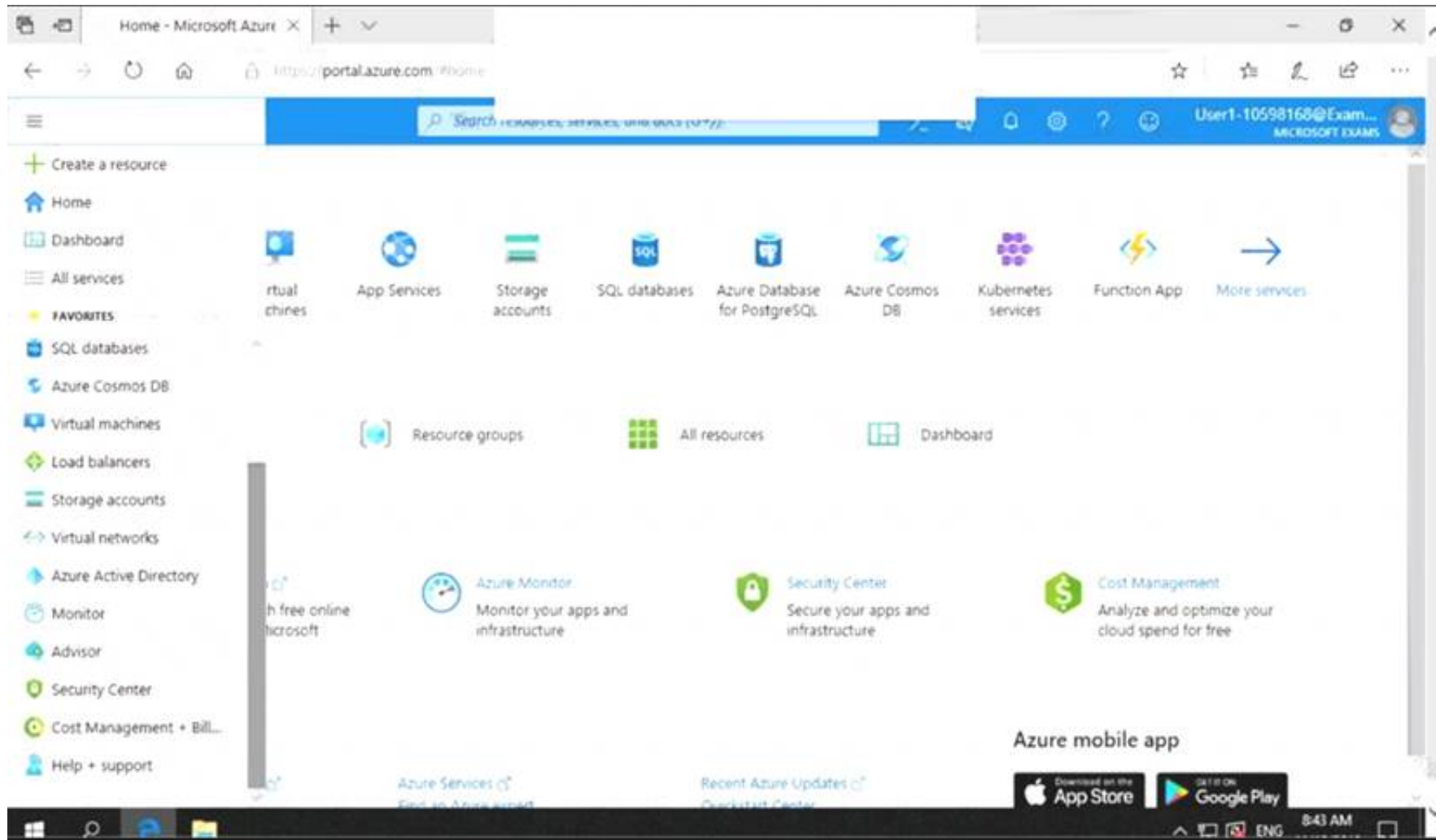
Explanation:
<https://docs.microsoft.com/en-us/azure/governance/blueprints/overview#blueprint-definition> <https://docs.microsoft.com/en-us/azure/governance/blueprints/overview>

NEW QUESTION 84

- (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.

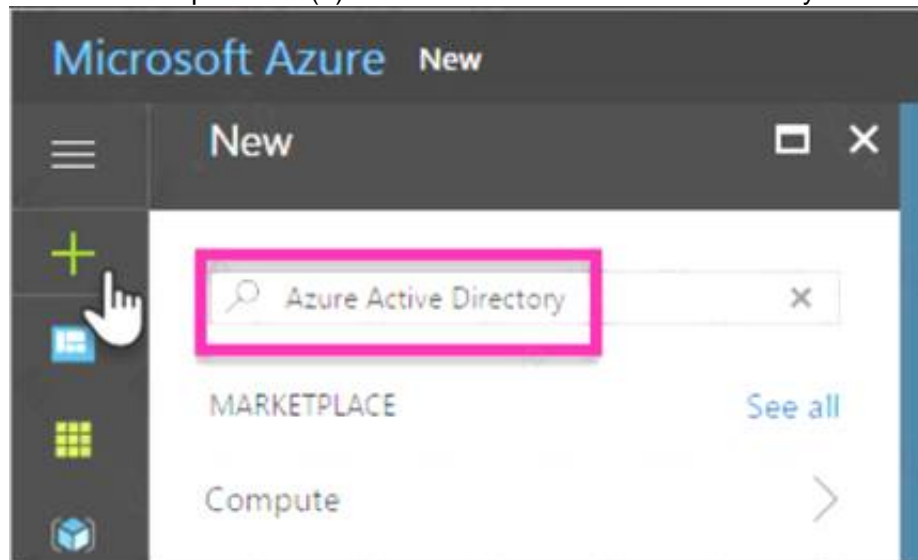
- A. Mastered
- B. Not Mastered

Answer: A

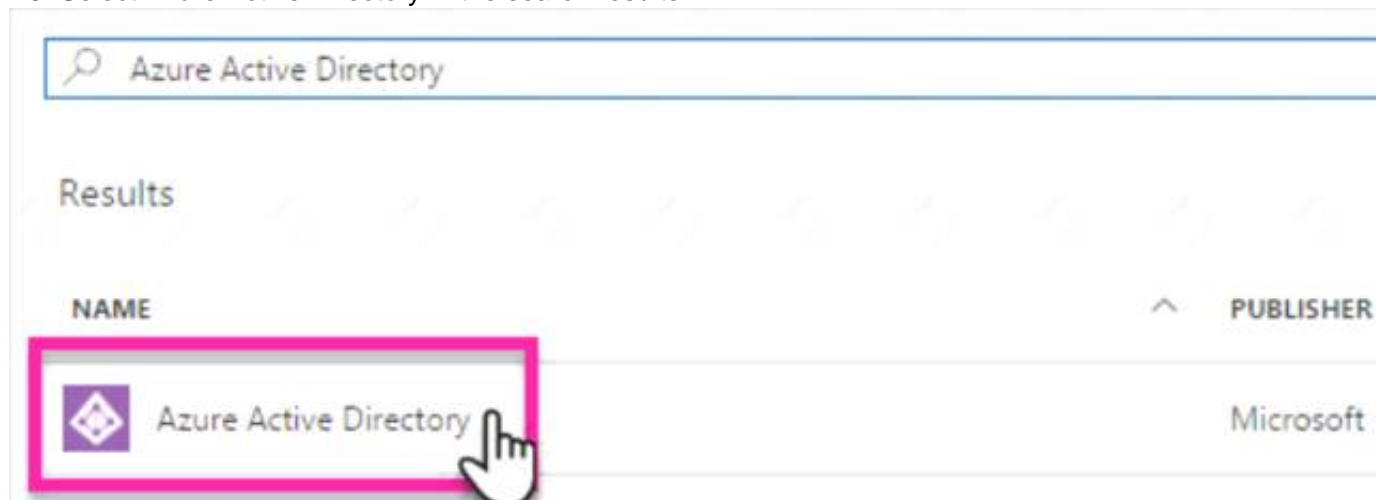
Explanation:

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.

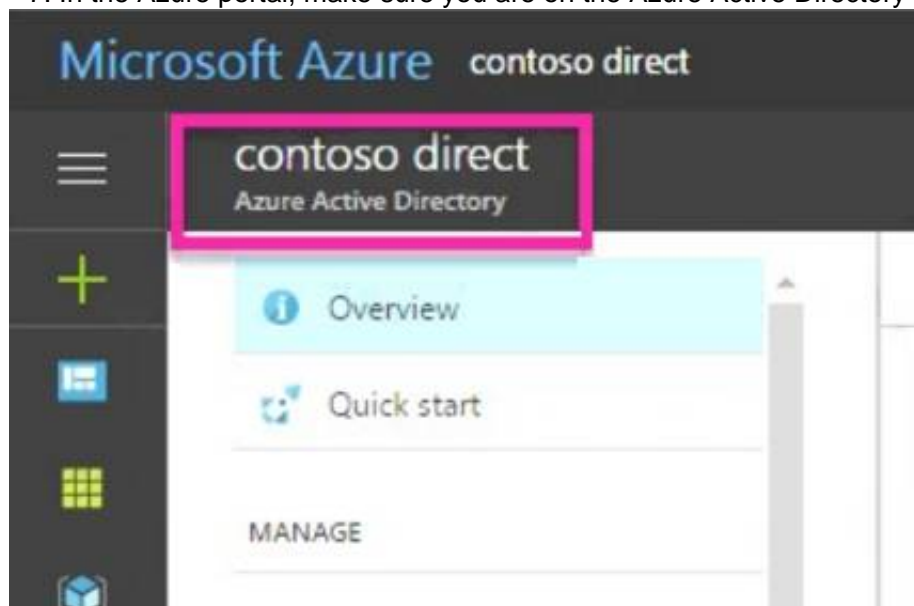


- * 4. Select Create.
- * 5. Provide an Organization name and an Initial domain name (10598168). Then select Create. Your directory is created.

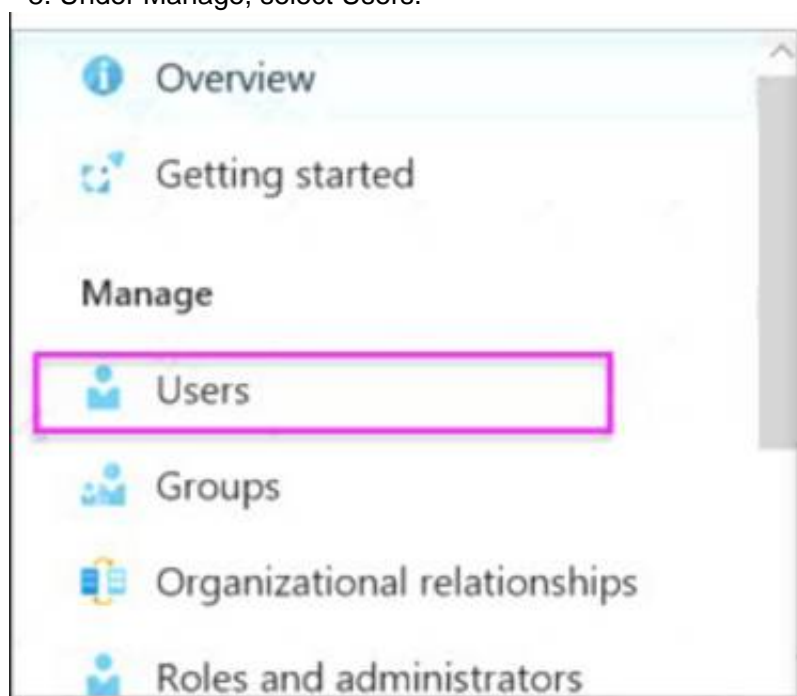
* 6. After directory creation is complete, select the information box to manage your new directory. Next, you're going to add tenant users.

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

User

contoso direct

Name ⓘ

PBI Embed

1

✓

User name ⓘ

pbiembed@contosodirect.onmicrosoft.com

2

✓

Profile ⓘ

Not configured

>

Properties ⓘ

Default

>

Groups ⓘ

0 groups selected

>

Directory role ⓘ

User

3

>

Password

☐ Show Password

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

NEW QUESTION 85
- (Exam Topic 4)

You have an Azure subscription that contains the following resources:

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

You need to ensure that when a high-priority alert is generated in Security Center for a virtual machine, an incident is created in Azure Sentinel and then a script is initiated to configure a firewall rule for the NVA.

How should you configure Azure Sentinel to meet the requirements? To answer, drag the appropriate components to the correct requirements. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Components

A data connector for Security Center

A data connector for the firewall software

A playbook

A rule

A Security Events connector

A workbook

Answer Area

Enable alert notifications from Security Center:

Component

Create an incident:

Component

Initiate a script to configure the firewall rule:

Component

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 88

- (Exam Topic 4)

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

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

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

Create an access review

Access reviews enable reviewers to attest to users access.

Review name

Review1

Description

Start date

2019-03-01

Frequency

One time

End date

2019-03-20

Users

Scope: Everyone

Review role membership

Password administrator

Reviewers

Reviewers: Members(self)

Agree comparison settings

Auto apply results to members:

Enable

Disable

Should reviewer not respond

Take recommendations

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

User3 can perform Review1 for

User3 only

User1 and User2 only

User1, User2, and User3

If User2 fails to complete Review1 by March 20, 2019

The Password administrator role will be revoked from User2

User2 will retain the Password administrator role

User3 will receive a confirmation request

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: User3 only

Use the Members (self) option to have the users review their own role assignments. Box 2: User3 will receive a confirmation request

Use the Should reviewer not respond list to specify what happens for users that are not reviewed by the reviewer within the review period. This setting does not impact users who have been reviewed by the reviewers manually. If the final reviewer's decision is Deny, then the user's access will be removed.

No change - Leave user's access unchanged Remove access - Remove user's access Approve access - Approve user's access

Take recommendations - Take the system's recommendation on denying or approving the user's continued access

References:
<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-start-s>

NEW QUESTION 92

- (Exam Topic 4)

You create an Azure subscription.

You need to ensure that you can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to secure Azure AD roles.

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

Actions

Verify your identity by using multi-factor authentication (MFA).

Consent to PIM.

Sign up PIM for Azure AD roles.

Discover privileged roles.

Discover resources.

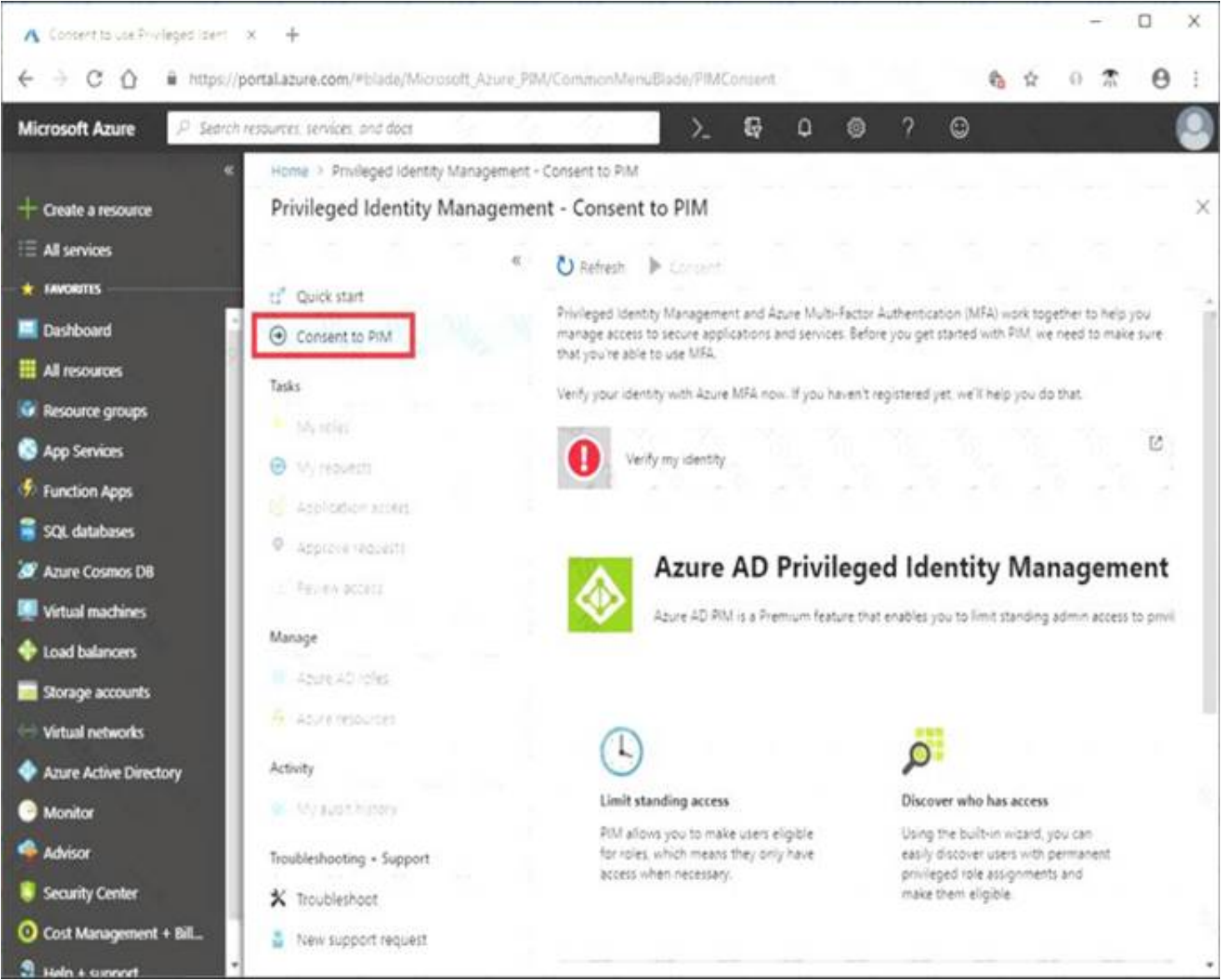
Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Step 1: Consent to PIM



Step: 2 Verify your identity by using multi-factor authentication (MFA)

Click Verify my identity to verify your identity with Azure MFA. You'll be asked to pick an account. Step 3: Sign up PIM for Azure AD roles

Once you have enabled PIM for your directory, you'll need to sign up PIM to manage Azure AD roles. References:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started>

NEW QUESTION 97

- (Exam Topic 4)

You have an Azure subscription that contains a resource group named RG1. RG1 contains a storage account named storage1.

You have two custom Azure roles named Role1 and Role2 that are scoped to RG1. The permissions for Role1 are shown in the following JSON code.

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

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

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

Answer Area	Statements	Yes	No
	User1 can read data in storage1.	<input type="radio"/>	<input type="radio"/>
	User2 can read data in storage1.	<input type="radio"/>	<input type="radio"/>
	User3 can restore storage1 from a backup in Azure Backup.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area	Statements	Yes	No
	User1 can read data in storage1.	<input checked="" type="radio"/>	<input type="radio"/>
	User2 can read data in storage1.	<input checked="" type="radio"/>	<input type="radio"/>
	User3 can restore storage1 from a backup in Azure Backup.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 99

- (Exam Topic 4)

You plan to create an Azure Kubernetes Service (AKS) cluster in an Azure subscription. The manifest of the registered server application is shown in the following exhibit.

Save Discard Upload Download

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

```
1 {
2   "id": "d6b00db3-7ef4-4f3c-b1e7-8346f0a59546",
3   "acceptMappedClaims": null,
4   "accessTokenAcceptedVersion": null,
5   "addIns": [],
6   "allowPublicClient": null,
7   "appId": "88137405-6a75-4c20-903a-f7b18ff7d496",
8   "appRoles": [],
9   "oauth2AllowUrlPathMatching": false,
10  "createdDateTime": "2019-07-15T21:09:20Z",
11  "groupMembershipClaims": null,
12  "identifierUris": [],
13  "informationalUrls": {
14    "termsOfService": null,
15    "support": null,
16    "privacy": null,
17    "marketing": null
18  },
19  "keyCredentials": [],
20  "knownClientApplications": [],
21  "logoUrl": null,
22  "logoutUrl": null,
23  "name": "AKSAzureADServer",
24  "oauth2AllowIdTokenImplicitFlow": false,
25  "oauth2AllowImplicitFlow": false,
26  "oauth2Permissions": [],
27  "oauth2RequirePostResponse": false,
28  "optionalClaims": null,
29  "orgRestrictions": [],
30  "parentalControlSettings": {
```

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

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 103

- (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 107

- (Exam Topic 4)
You have an Azure subscription that contains a resource group named RG1. RG1 contains a virtual machine named VM1 that uses Azure Active Directory (Azure AD) authentication.
You have two custom Azure roles named Role1 and Role2 that are scoped to RG1. The permissions for Role1 are shown in the following JSON code.

```
"permissions": [
  {
    "actions": [
      "Microsoft.Compute/virtualMachines/*"
    ],
    "notActions": [
      "Microsoft.Compute/virtualMachines/delete"
    ],
    "dataActions": [],
    "notDataActions": []
  }
]
```

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

```
"permissions": [
  {
    "actions": [
      "Microsoft.Compute/virtualMachines/*"
    ],
    "notActions": [],
    "dataActions": [],
    "notDataActions": []
  }
]
```

You assign the roles to the users shown in the following table.

Name	Role
User1	Role1
User2	Role1, Role2
User3	Role1, Role2

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

Answer Area

Statements	Yes	No
User1 can delete VM1.	<input type="radio"/>	<input type="radio"/>
User2 can delete VM1.	<input type="radio"/>	<input type="radio"/>
User3 can sign in to VM1 by using Azure AD credentials.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can delete VM1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can delete VM1.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can sign in to VM1 by using Azure AD credentials.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 108

- (Exam Topic 4)

You network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant. The tenant contains the users shown in the following table.

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

The tenant contains the groups shown in the following table.

Name	Members
Group1	User1, User2, User3
Group2	User2

You configure a multi-factor authentication (MFA) registration policy that and the following settings:

- > Assignments:
- > Include: Group1
- > Exclude Group2

Controls: Require Azure MFA registration Enforce Policy: On

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

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user’s next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>
User2 must configure MFA during the user’s next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>
User3 will be prompted to configure MFA registration during the user’s next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user’s next Azure AD authentication.	<input checked="" type="radio"/>	<input type="radio"/>
User2 must configure MFA during the user’s next Azure AD authentication.	<input type="radio"/>	<input checked="" type="radio"/>
User3 will be prompted to configure MFA registration during the user’s next Azure AD authentication.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 113

- (Exam Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You use Azure Security Center for the centralized policy management of three Azure subscriptions. You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create a resource graph and an assignment that is scoped to a management group. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/governance/management-groups/create>

NEW QUESTION 114

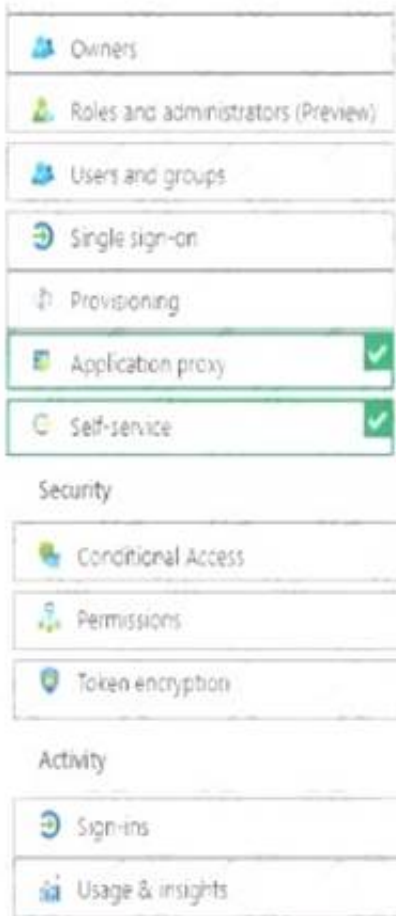
- (Exam Topic 4)

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 part.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application Description automatically generated

NEW QUESTION 116

- (Exam Topic 4)

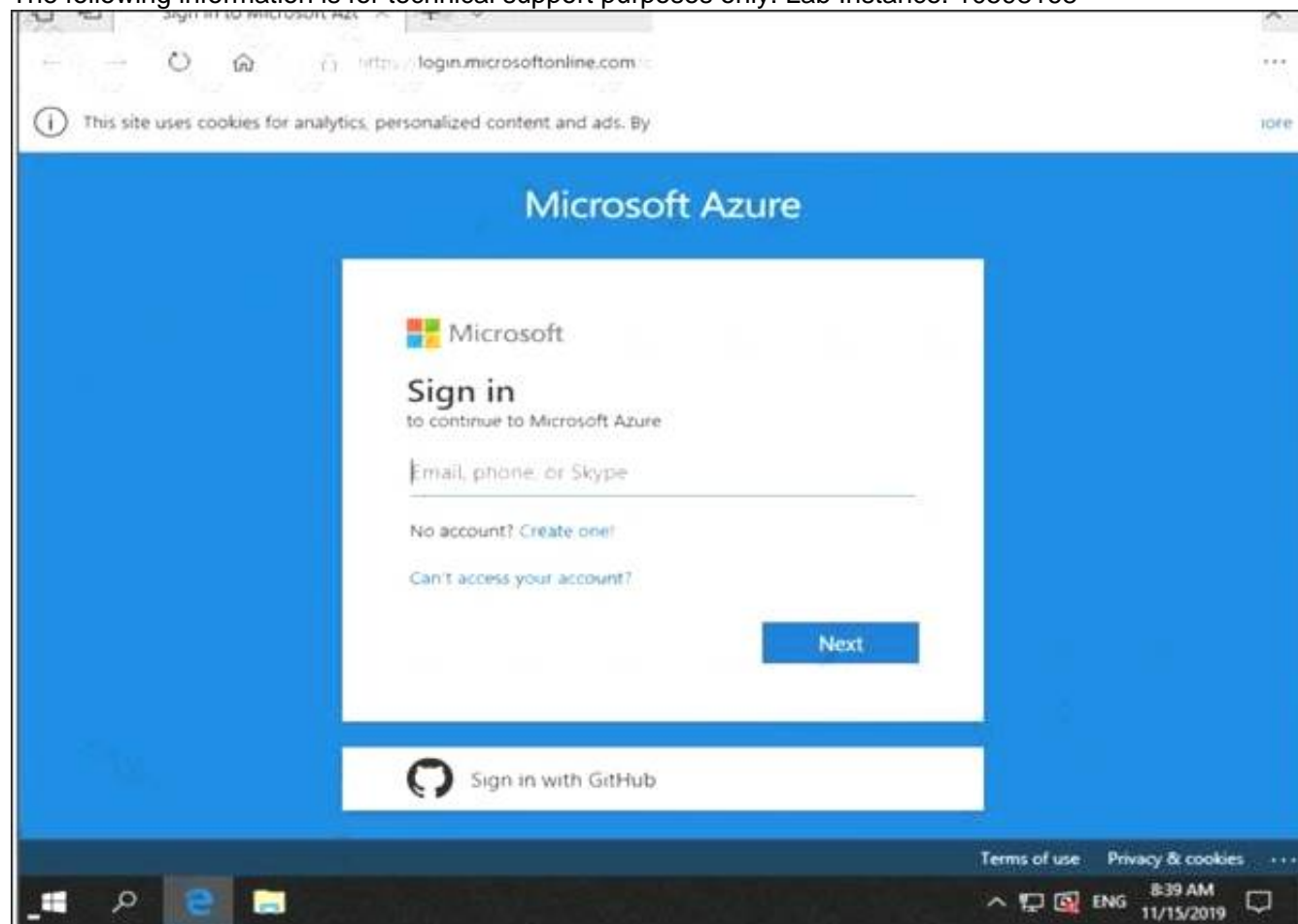
Use the following login credentials as needed:

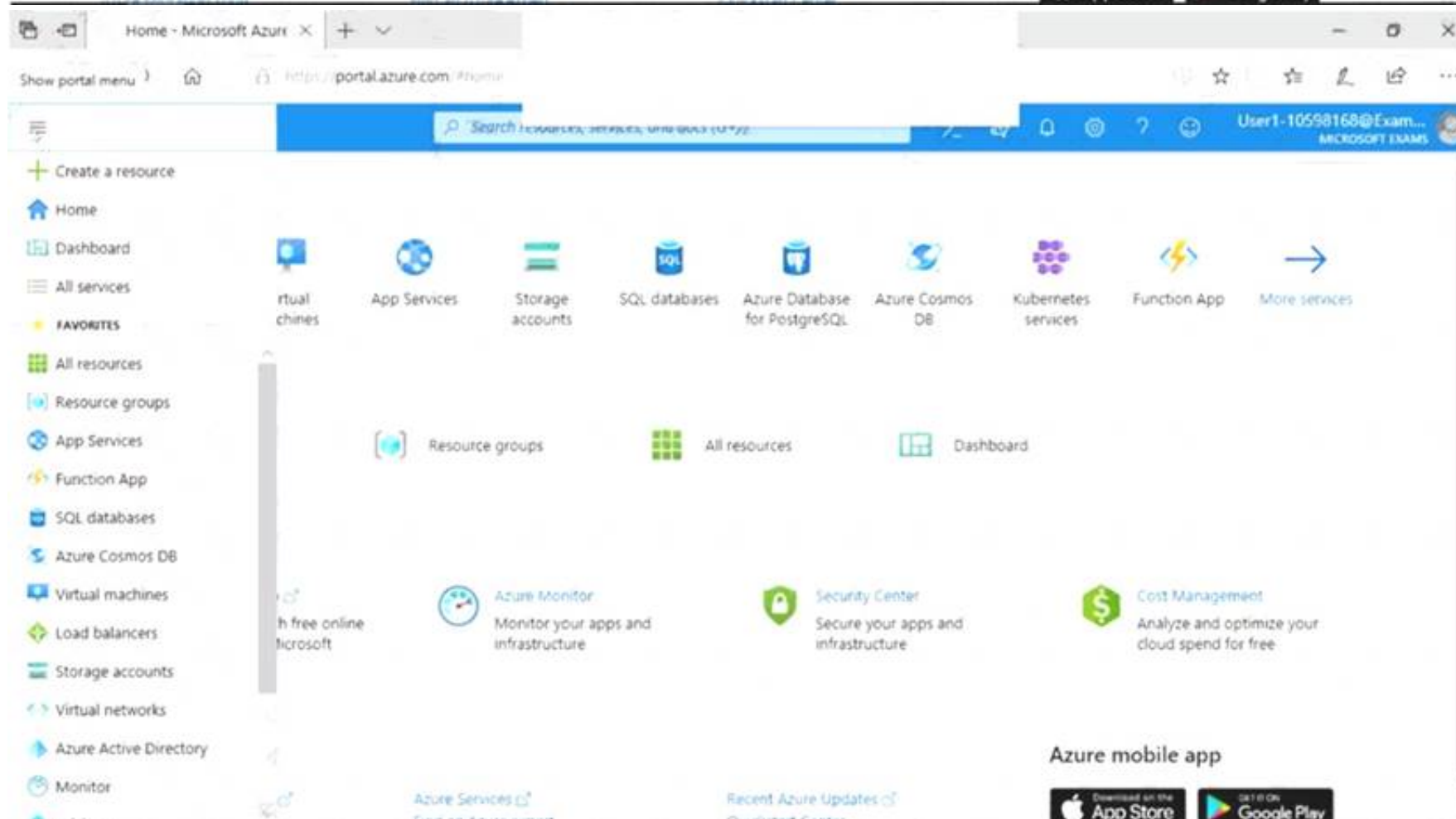
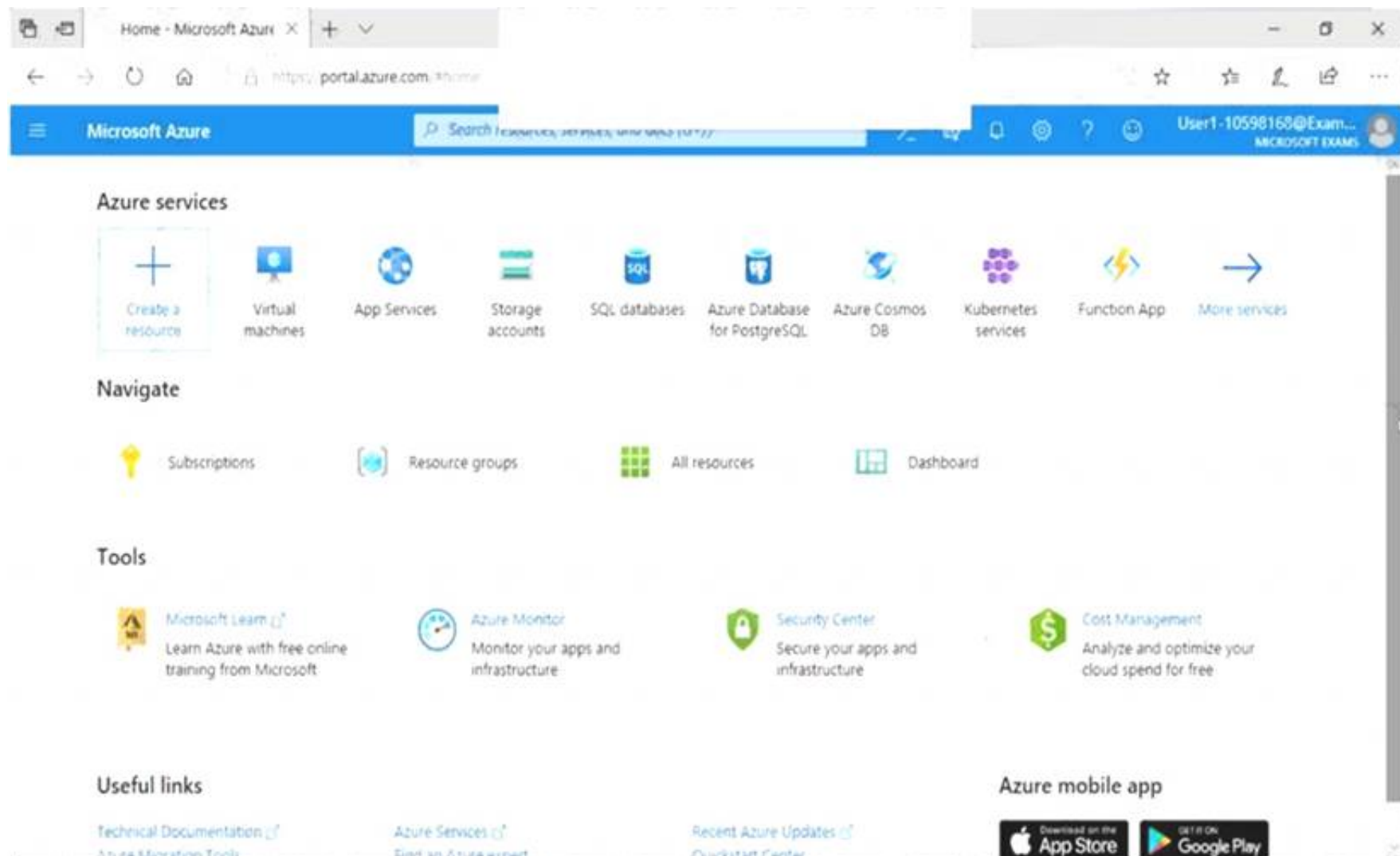
To enter your username, place your cursor in the Sign in box and click on the username below.

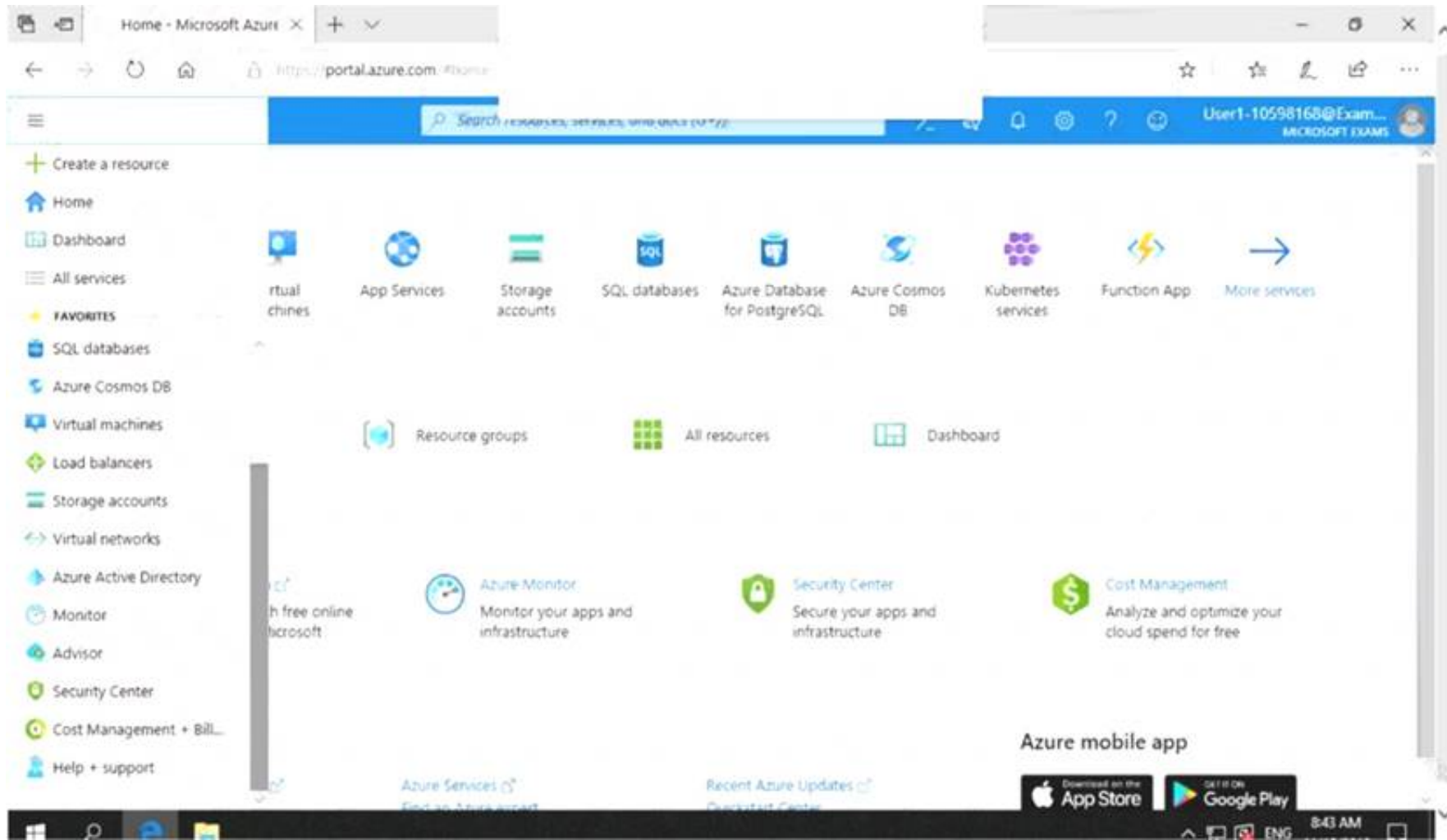
To enter your password, place your cursor in the Enter password box and click on the password below. Azure Username: User1-10598168@ExamUsers.com

Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only: Lab Instance: 10598168







You need to collect all the audit failure data from the security log of a virtual machine named VM1 to an Azure Storage account. To complete this task, sign in to the Azure portal. This task might take several minutes to complete. You can perform other tasks while the task completes.

- A. Mastered
- B. Not Mastered

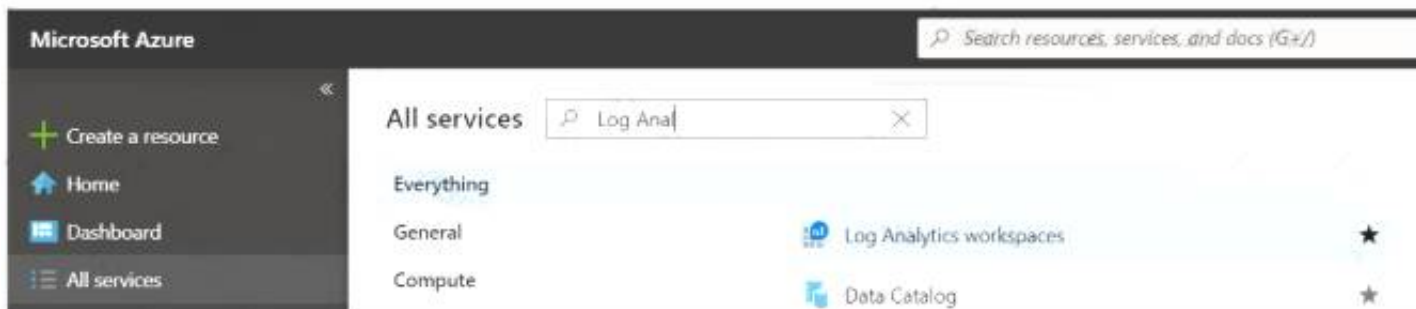
Answer: A

Explanation:

Step 1: Create a workspace

Azure Monitor can collect data directly from your Azure virtual machines into a Log Analytics workspace for detailed analysis and correlation.

* 1. In the Azure portal, select All services. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics workspaces.



* 2. Select Create, and then select choices for the following items:

Log Analytics workspace

Create new or link existing workspace

Create New

Link Existing

Log Analytics Workspace

DefaultLAWorkspace

Subscription

Microsoft Azure

Resource group

Prod

Create new

Location

East US

Pricing tier

Per GB (2018)

- * 3. After providing the required information on the Log Analytics workspace pane, select OK.
While the information is verified and the workspace is created, you can track its progress under Notifications from the menu.
- Step 2: Enable the Log Analytics VM Extension
- Installing the Log Analytics VM extension for Windows and Linux allows Azure Monitor to collect data from your Azure VMs.
- * 1. In the Azure portal, select All services found in the upper left-hand corner. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics workspaces.
- * 2. In your list of Log Analytics workspaces, select DefaultWorkspace (the name you created in step 1).
- * 3. On the left-hand menu, under Workspace Data Sources, select Virtual machines.
- * 4. In the list of Virtual machines, select a virtual machine you want to install the agent on. Notice that the Log Analytics connection status for the VM indicates that it is Not connected.
- * 5. In the details for your virtual machine, select Connect. The agent is automatically installed and configured for your Log Analytics workspace. This process takes a few minutes, during which time the Status shows Connecting.
- After you install and connect the agent, the Log Analytics connection status will be updated with This workspace.
- Reference: <https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-azurevm>

NEW QUESTION 121

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

Edit blueprint

Basics Artifacts		
Add artifacts to the blueprint. Add resource groups to organize where the artifacts should be deployed and assigned.		
NAME	ARTIFACT TYPE	PARAMETERS
Subscription		
Add artifact...		
RG2	Resource group	2 out of 2 parameters populated
User1 (User1@sk200628outlook.onmicrosoft.com) : Tag Contributor	Role assignment	1 out of 1 parameters populated
Add artifact...		

- You assign Blueprint1 to Subscription1 by using the following settings:
- > Lock assignment: Read Only
 - > Managed Identity: System assigned
- For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Statements	Yes	No
A locking mode of Read Only will be assigned to RG1.	<input type="radio"/>	<input type="radio"/>
User1 can add tags to RG2.	<input type="radio"/>	<input type="radio"/>
You can remove User1 from the Tag Contributor role for RG2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 126

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

Name	Type
Item1	Key
Item2	Secret
Policy1	Access policy

In KeyVault, the following events occur in sequence:

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

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

Statements	Yes	No
You can recover Policy1.	<input type="radio"/>	<input type="radio"/>
You can add a new key named Item1.	<input type="radio"/>	<input type="radio"/>
You can add a new secret named Item2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 131

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

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

Answer: A

NEW QUESTION 133

- (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 137

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

Container registries:

▼

0

1

2

3

Workspaces:

▼

0

1

2

3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 141

- (Exam Topic 3)
You need to encrypt storage1 to meet the technical requirements. Which key vaults can you use?

- A. KeyVault1 only
- B. KeyVault2 and KeyVault3 only
- C. KeyVault1 and KeyVault3 only
- D. KeyVault1 KeyVault2 and KeyVault3

Answer: B

Explanation:

The storage account and the key vault must be in the same region and in the same Azure Active Directory (Azure AD) tenant, but they can be in different subscriptions.
Storage1 is in the West US region. KeyVault1 is the only key vault in the same region. Reference:
<https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-overview>

NEW QUESTION 144

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

- A. KeyVault1
- B. KeyVault3
- C. KeyVault2

Answer: A

Explanation:

The key vault needs to be in the same subscription and same region as the VM. VM4 is in West US. KeyVault1 is the only key vault in the same region as the VM.

Reference:
<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault>

NEW QUESTION 149

- (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.	<input type="radio"/>	<input type="radio"/>
From VM1, you can successfully ping the private IP address of VM3.	<input type="radio"/>	<input type="radio"/>
From VM1, you can successfully ping the public IP address of VM5.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

No, Yes,
Yes

NEW QUESTION 153

- (Exam Topic 2)

HOTSPOT

Which virtual networks in Sub1 can User2 modify and delete in their current state? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Virtual networks that User2 can modify:

VNET4 only

VNET4 and VNET1 only

VNET4, VNET3, and VNET1 only

VNET4, VNET3, VNET2, and VNET1

Virtual networks that User2 can delete:

VNET4 only

VNET4 and VNET1 only

VNET4, VNET3, and VNET1 only

VNET4, VNET3, VNET2, and VNET1

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box 1: VNET4 and VNET1 only

RG1 has only Delete lock, while there are no locks on RG4. RG2 and RG3 both have Read-only locks.

Box 2: VNET4 only

There are no locks on RG4, while the other resource groups have either Delete or Read-only locks.

Note: As an administrator, you may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. You can set the lock level to CanNotDelete or ReadOnly. In the portal, the locks are called Delete and Read-only respectively.

> CanNotDelete means authorized users can still read and modify a resource, but they can't delete the resource.

> ReadOnly means authorized users can read a resource, but they can't delete or update the resource.

Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

Scenario:

User2 is a Security administrator.

Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6. User2 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

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

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

NEW QUESTION 157

- (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 161

- (Exam Topic 2)

What is the membership of Group1 and Group2? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Group1:

No members

Only User2

Only User2 and User4

User1, User2, User3, and User4

Group2:

No members

Only User3

Only User1 and User3

User1, User2, User3, and User4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: User1, User2, User3, User4

Contains "ON" is true for Montreal (User1), MONTREAL (User2), London (User 3), and Ontario (User4) as string and regex operations are not case sensitive.

Box 2: User1, User2, User3, User4 References:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership>

NEW QUESTION 162

- (Exam Topic 1)

You need to ensure that users can access VM0. The solution must meet the platform protection requirements.

What should you do?

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

Answer: D

Explanation:

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

NEW QUESTION 164

- (Exam Topic 1)

You need to deploy AKS1 to meet the platform protection requirements.

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

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Actions	Answer Area
Deploy an AKS cluster.	
Create a client application.	
Create a server application.	
Create an RBAC binding.	
Create a custom RBAC role.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Scenario: Azure AD users must be to authenticate to AKS1 by using their Azure AD credentials. Litewire plans to deploy AKS1, which is a managed AKS (Azure Kubernetes Services) cluster. Step 1: Create a server application

To provide Azure AD authentication for an AKS cluster, two Azure AD applications are created. The first application is a server component that provides user authentication. Step 2: Create a client application

The second application is a client component that's used when you're prompted by the CLI for authentication. This client application uses the server application for the actual authentication of the credentials provided by the client.

Step 3: Deploy an AKS cluster.

Use the az group create command to create a resource group for the AKS cluster. Use the az aks create command to deploy the AKS cluster.

Step 4: Create an RBAC binding.

Before you use an Azure Active Directory account with an AKS cluster, you must create role-binding or cluster role-binding. Roles define the permissions to grant, and bindings apply them to desired users. These assignments can be applied to a given namespace, or across the entire cluster.

Reference:

<https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration>

NEW QUESTION 166

- (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/",
      "Microsoft.Resources/",
      "Microsoft.Storage/"
    ],
    [
      "disks/**",
      "storageAccounts/**",
      "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) /subscription/{subscriptionId}/resourceGroups/{Resource Group Id}

A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.

NEW QUESTION 171

- (Exam Topic 1)

You need to configure WebApp1 to meet the data and application requirements.

Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

Answer: BE

Explanation:

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

NEW QUESTION 174

- (Exam Topic 1)

You need to ensure that the Azure AD application registration and consent configurations meet the identity and access requirements.

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

To configure the registration settings:

Azure AD – User settings

Azure AD – App registrations settings

Enterprise Applications – User settings

To configure the consent settings:

Azure AD – User settings

Azure AD – App registrations settings

Enterprise Applications – User settings

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 179

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

Create a custom policy definition that has effect set to:

Append

Deny

DeployIfNotExists

Create a policy assignment and modify:

The Create a Managed Identify setting

The exclusion settings

The scope

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

- * 1. DeployifNotExists
- * 2. Scope

NEW QUESTION 184

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

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

Admin1 performs the following actions on RG1:

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

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

Adding VNET1:

Rule2 only
Rule4 only
Rule2 and Rule 4 only
Rule3 and Rule 4 only
Rule1, Rule2, Rule3 and Rule 4

Adding Lock1:

Rule2 only
Rule4 only
Rule2 and Rule 4 only
Rule3 and Rule 4 only
Rule1, Rule2, Rule3 and Rule 4

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Adding VNET1:

Rule2 only
Rule4 only
Rule2 and Rule 4 only
Rule3 and Rule 4 only
Rule1, Rule2, Rule3 and Rule 4

Adding Lock1:

Rule2 only
Rule4 only
Rule2 and Rule 4 only
Rule3 and Rule 4 only
Rule1, Rule2, Rule3 and Rule 4

NEW QUESTION 188

- (Exam Topic 4)

You need to configure a Microsoft SQL server named Web11597200 only to accept connections from the Subnet0 subnet on the VNET01 virtual network. To complete this task, sign in to the Azure portal.

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

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

NEW QUESTION 190

- (Exam Topic 4)

You have a management group named MG1 that contains an Azure subscription and a resource group named RG1. RG1 contains a virtual machine named VM1. You have the custom Azure roles shown in the following table.

Name	Scoped to
Role1	MG1
Role2	RG1

The permissions for Role1 are shown in the following role definition file.

```
"permissions": [
  {
    "actions": [
      "Microsoft.Compute/virtualMachines/*"
    ],
    "notActions": [
      "Microsoft.Compute/virtualMachines/delete"
    ],
    "dataActions": [],
    "notDataActions": []
  }
]
```

The permissions for Role2 are shown in the following role definition file.

```
"permissions": [
  {
    "actions": [
      "Microsoft.Compute/virtualMachines/*"
    ],
    "notActions": [],
    "dataActions": [],
    "notDataActions": []
  }
]
```

You assign the roles to the users shown in the following table.

Name	Role
User1	Role1
User2	Role1, Role2
User3	Role2

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

Answer Area

Statements	Yes	No
User1 can delete VM1.	<input type="radio"/>	<input type="radio"/>
User2 can delete VM1.	<input type="radio"/>	<input type="radio"/>
User3 can delete VM1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can delete VM1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can delete VM1.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can delete VM1.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 194

- (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 199

- (Exam Topic 4)

You have an Azure subscription that contains 100 virtual machines and has Azure Security Center Standard tier enabled.

You plan to perform a vulnerability scan of each virtual machine.

You need to deploy the vulnerability scanner extension to the virtual machines by using an Azure Resource Manager template.

Which two values should you specify in the code to automate the deployment of the extension to the virtual machines? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

Answer: AC

NEW QUESTION 203

- (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 208

- (Exam Topic 4)

You need to ensure that the rg1lod10598168n1 Azure Storage account is encrypted by using a key stored in the KeyVault10598168 Azure key vault.

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

- A. Mastered
- B. Not Mastered

Answer: A

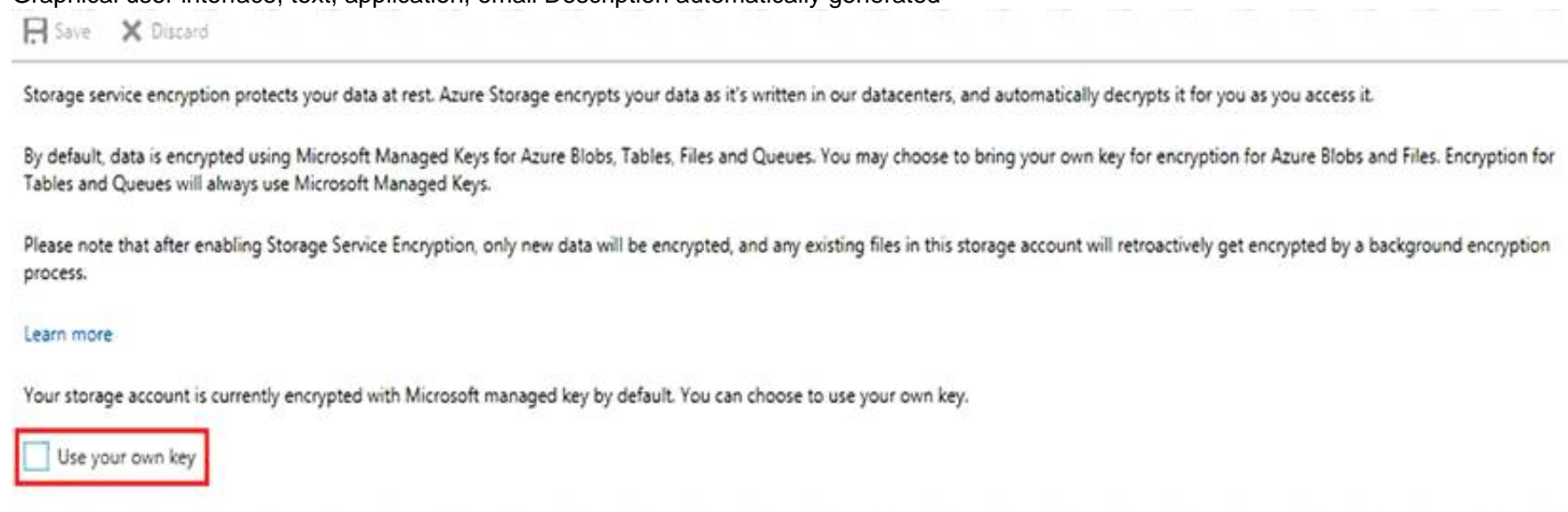
Explanation:

Step 1: To enable customer-managed keys in the Azure portal, follow these steps:

* 1. Navigate to your storage account rg1lod10598168n1

* 2. On the Settings blade for the storage account, click Encryption. Select the Use your own key option, as shown in the following figure.

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



Step 2: Specify a key from a key vault

To specify a key from a key vault, first make sure that you have a key vault that contains a key. To specify a key from a key vault, follow these steps:

* 4. Choose the Select from Key Vault option.

* 5. Choose the key vault KeyVault10598168 containing the key you want to use.

* 6. Choose the key from the key vault.

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

Save

Discard

Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

By default, data is encrypted using Microsoft Managed Keys for Azure Blobs, Tables, Files and Queues. You may choose to bring your own key for encryption for Azure Blobs and Files. Encryption for Tables and Queues will always use Microsoft Managed Keys.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process.

[Learn more](#)

Your storage account is currently encrypted with Microsoft managed key by default. You can choose to use your own key.

☒ Use your own key

Encryption key

☐ Enter key URI

☒ Select from Key Vault

Key Vault

<key-vault>

>

Encryption key

<key>

>

<storage-account> will be granted access to the selected key vault. Both soft delete and purge protection will be enabled on the key vault and cannot be disabled. [Learn more](#)

Reference:

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

NEW QUESTION 213

- (Exam Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 215

- (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:

Never
Always
Only after May 1, 2019

Password2:

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/azurermskeyvault/set-azurekeyvaultsecretattribute>

NEW QUESTION 217

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

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

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

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

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

Statements	Yes	No
User1 can add VM1 to VNET1.	<input type="radio"/>	<input type="radio"/>
User1 can start and stop App1.	<input type="radio"/>	<input type="radio"/>
User1 can start and stop cont1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

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

NEW QUESTION 219

- (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>

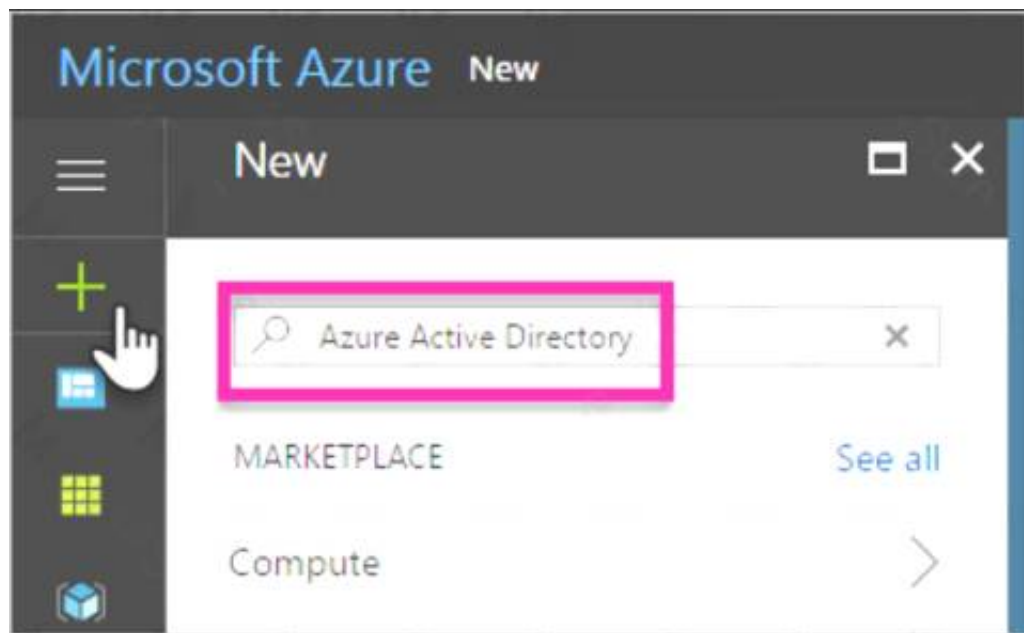
NEW QUESTION 222

- (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).

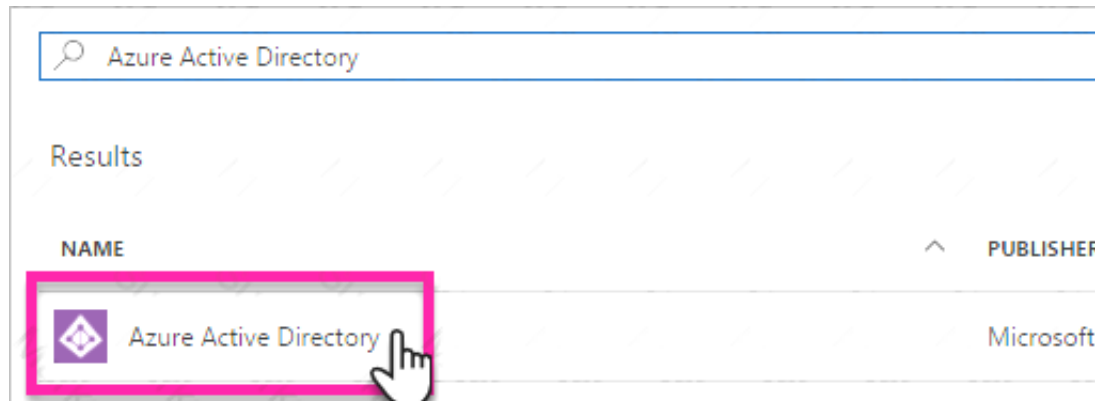
- A. Mastered
- B. Not Mastered

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.

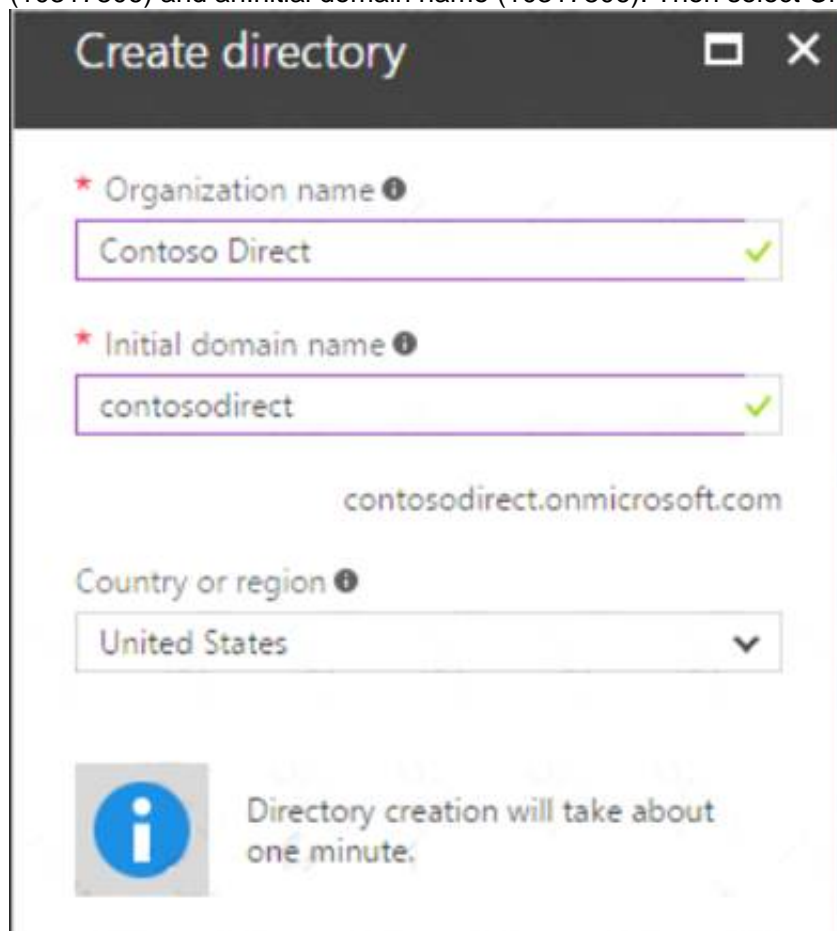


* 4. Select Create.

* 5. Provide an Organization name

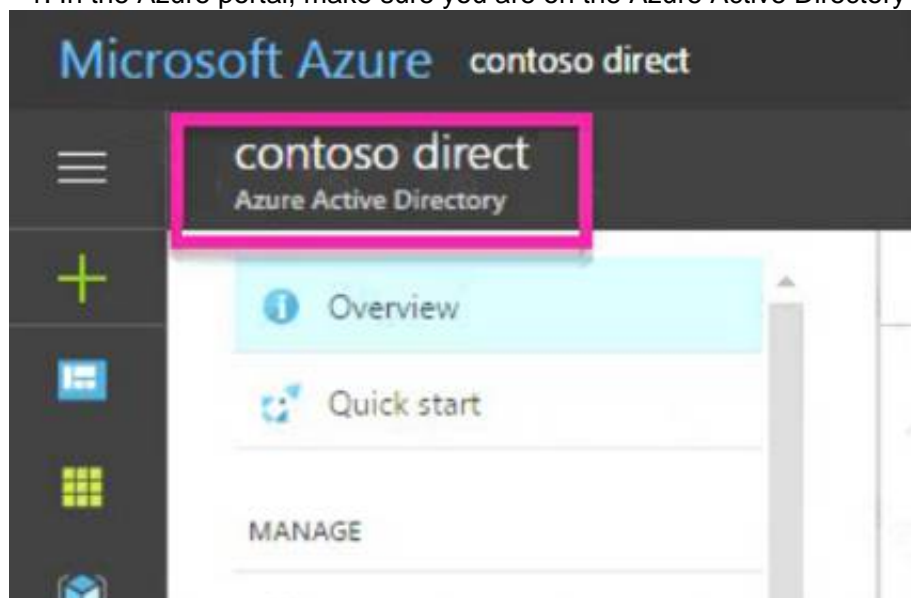
This will create the directory named 10317806.onmicrosoft.com.

(10317806) and an Initial domain name (10317806). Then select Create.

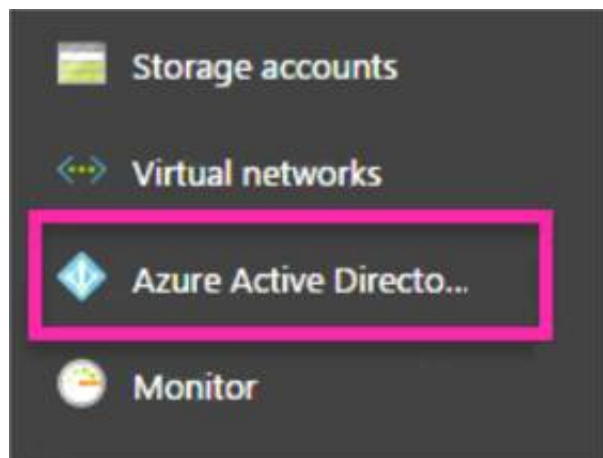


* 6. After directory creation is complete, select the information box to manage your new directory. To create the user:

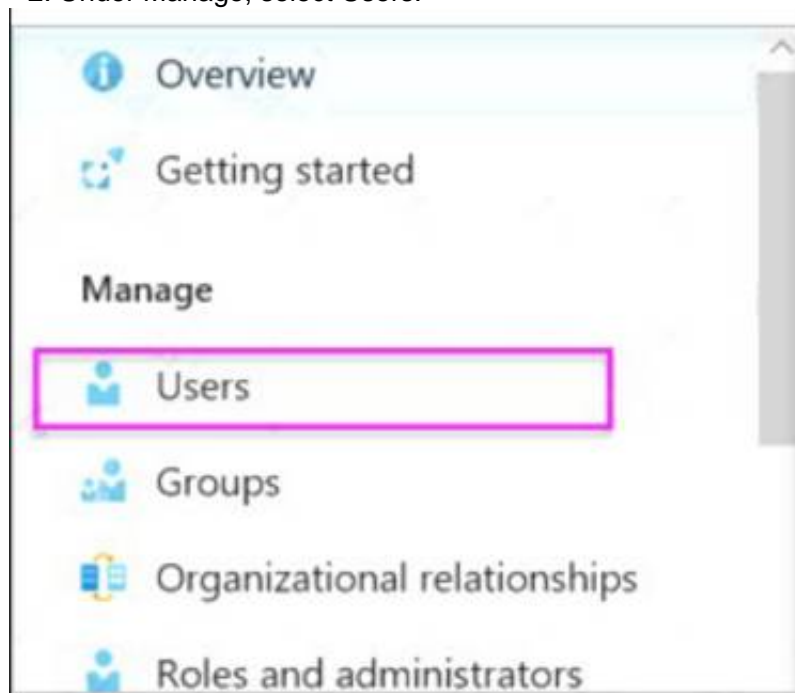
* 1. In the Azure portal, make sure you are on the Azure Active Directory fly out.



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



* 2. Under Manage, select Users.



* 3. Select All users

and then select New user.

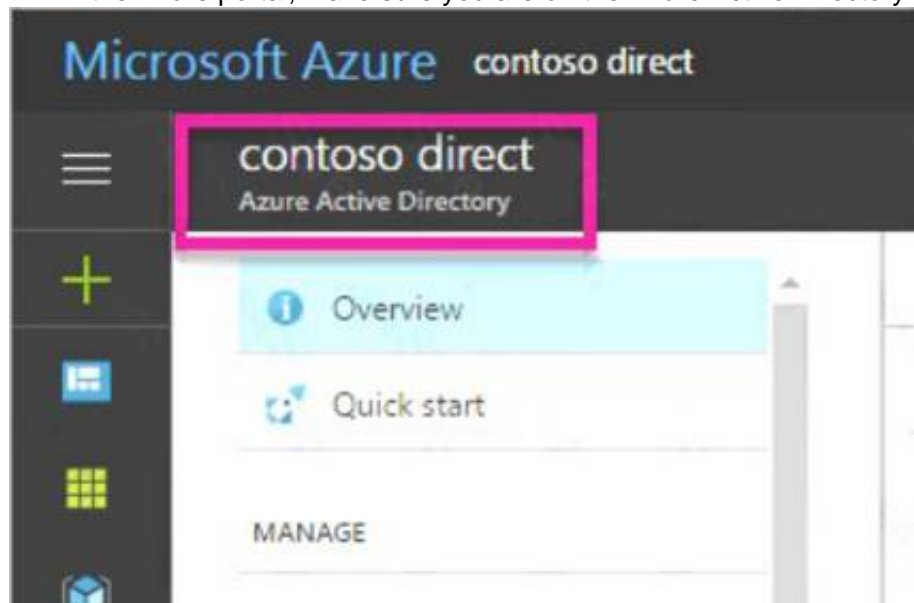
* 4. Provide a Name

and User name

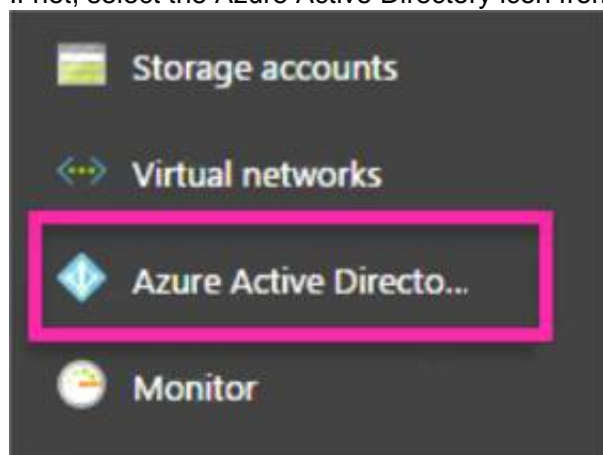
(user10317806) for the user. When you're done, select Create.

To enable MFA:

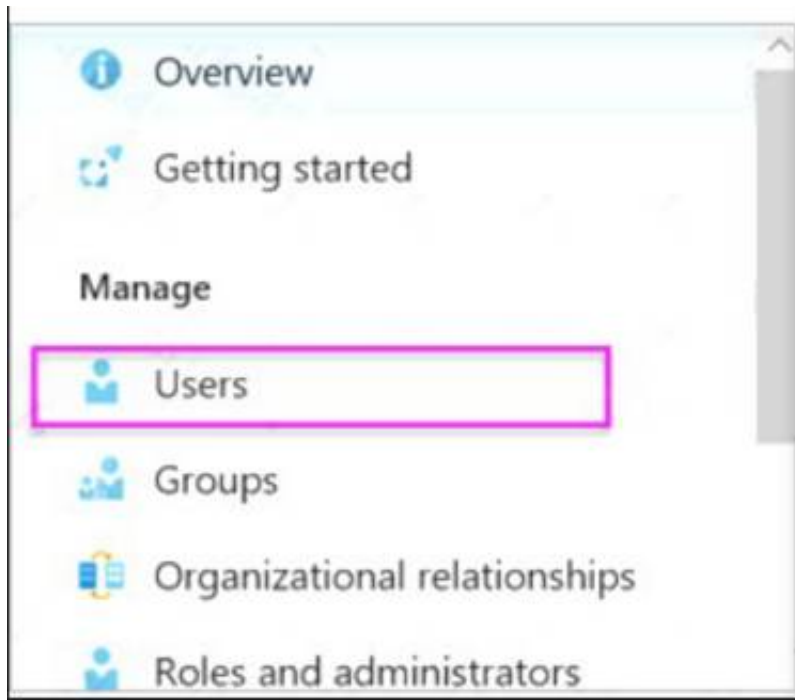
* 1. In the Azure portal, make sure you are on the Azure Active Directory fly out.



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 227

- (Exam Topic 4)

You have a hybrid configuration of Azure Active Directory (Azure AD).

All users have computers that run Windows 10 and are hybrid Azure AD joined.

You have an Azure SQL database that is configured to support Azure AD authentication.

Database developers must connect to the SQL database by using Microsoft SQL Server Management Studio (SSMS) and authenticate by using their on-premises Active Directory account.

You need to tell the developers which authentication method to use to connect to the SQL database from SSMS. The solution must minimize authentication prompts.

Which authentication method should you instruct the developers to use?

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

Answer: C

Explanation:

Azure AD can be the initial Azure AD managed domain. Azure AD can also be an on-premises Active Directory Domain Services that is federated with the Azure AD.

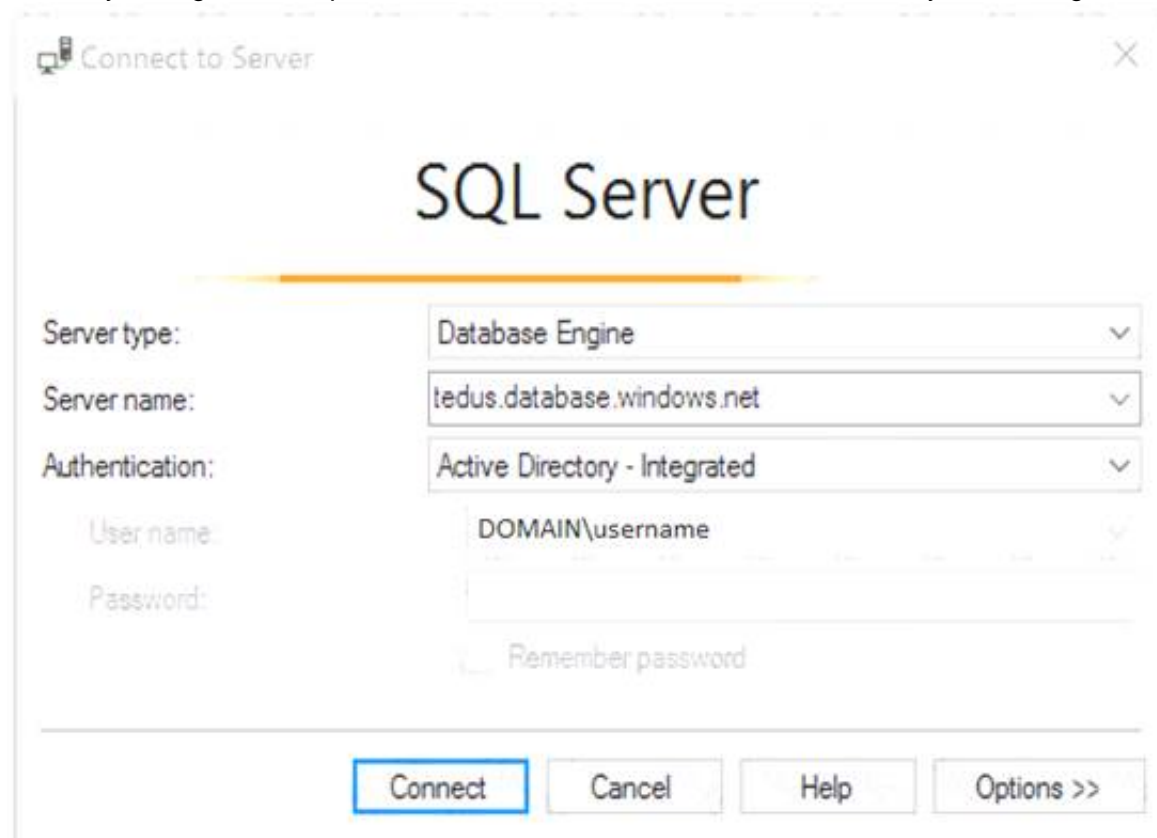
Using an Azure AD identity to connect using SSMS or SSDT

The following procedures show you how to connect to a SQL database with an Azure AD identity using SQL Server Management Studio or SQL Server Database Tools.

Active Directory integrated authentication

Use this method if you are logged in to Windows using your Azure Active Directory credentials from a federated domain.

* 1. Start Management Studio or Data Tools and in the Connect to Server (or Connect to Database Engine) dialog box, in the Authentication box, select Active Directory - Integrated. No password is needed or can be entered because your existing credentials will be presented for the connection.



* 2. Select the Options button, and on the Connection Properties page, in the Connect to database box, type the name of the user database you want to connect to. (The AD domain name or tenant ID" option is only supported for Universal with MFA connection options, otherwise it is greyed out.)

References:

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/sql-database/sql-database-aad-authentication>

NEW QUESTION 232

- (Exam Topic 4)

You need to ensure that a user named user2-12345678 can manage the properties of the virtual machines in the RG1lod12345678 resource group. The solution must use the principle of least privilege.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

- Sign in to the Azure portal.
- Browse to Resource Groups.
- Select the RG1lod12345678 resource group.
- Select Access control (IAM).
- Select Add > role assignment.
- Select Virtual Machine Contributor (you can filter the list of available roles by typing 'virtual' in the search box) then click Next.
- Select the +Select members option and select user2-12345678 then click the Select button.
- Click the Review + assign button twice.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal?tabs=current>

NEW QUESTION 236

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant and a root management group. You create 10 Azure subscriptions and add the subscriptions to the root management group.

You need to create an Azure Blueprints definition that will be stored in the root management group. What should you do first?

- A. Add an Azure Policy definition to the root management group.
- B. Modify the role-based access control (RBAC) role assignments for the root management group.
- C. Create a user-assigned identity.
- D. Create a service principal.

Answer: B

Explanation:

Reference:

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

NEW QUESTION 237

- (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 238

- (Exam Topic 4)

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

Name	Type	Attached to	NSG
NSG1	Network security group (NSG)	VM5	<i>Not applicable</i>
NSG2	Network security group (NSG)	Subnet1	<i>Not applicable</i>
Subnet1	Subnet	<i>Not applicable</i>	<i>Not applicable</i>
VM5	Virtual machine	Subnet1	NSG1

An IP address of 10.1.0.4 is assigned to VM5. VM5 does not have a public IP address.

VM5 has just in time (JIT) VM access configured as shown in the following exhibit.

JIT VM access configuration

VM5

+ Add

Save

Discard

Configure the ports for which the just-in-time VM access will be applicable

Port	Protocol	Allowed source IPs	IP range	Time range (hours)	
3389	Any	Per request	N/A	3 hours	...

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

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

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

Statements	Yes	No
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	<input type="radio"/>	<input type="radio"/>
Remote Desktop access to VM5 is blocked.	<input type="radio"/>	<input type="radio"/>
An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	<input checked="" type="radio"/>	<input type="radio"/>
Remote Desktop access to VM5 is blocked.	<input checked="" type="radio"/>	<input type="radio"/>
An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 240

- (Exam Topic 4)

You need to ensure that the AzureBackupReport log for the Vault1 Recovery Services vault is stored in the WS11641655 Azure Log Analytics workspace. To complete this task, sign in to the Azure portal and modify the Azure resources.

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

* 1. In the Azure portal, type Recovery Services Vaults in the search box, select Recovery Services Vaults from the search results then select Vault1. Alternatively,

browse to Recovery Services Vaults in the left navigation pane.

- * 2. In the properties of Vault1, scroll down to the Monitoring section and select Diagnostic Settings.
- * 3. Click the Add a diagnostic setting link.
- * 4. Enter a name in the Diagnostic settings name box.
- * 5. In the Log section, select AzureBackupReport.

Category details

log

☐ AzureBackupReport

☐ CoreAzureBackup

☐ AddonAzureBackupJobs

☐ AddonAzureBackupAlerts

☐ AddonAzureBackupPolicy

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

Destination details

☐ Send to Log Analytics

☐ Archive to a storage account

☐ Stream to an event hub

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

NEW QUESTION 241

- (Exam Topic 4)

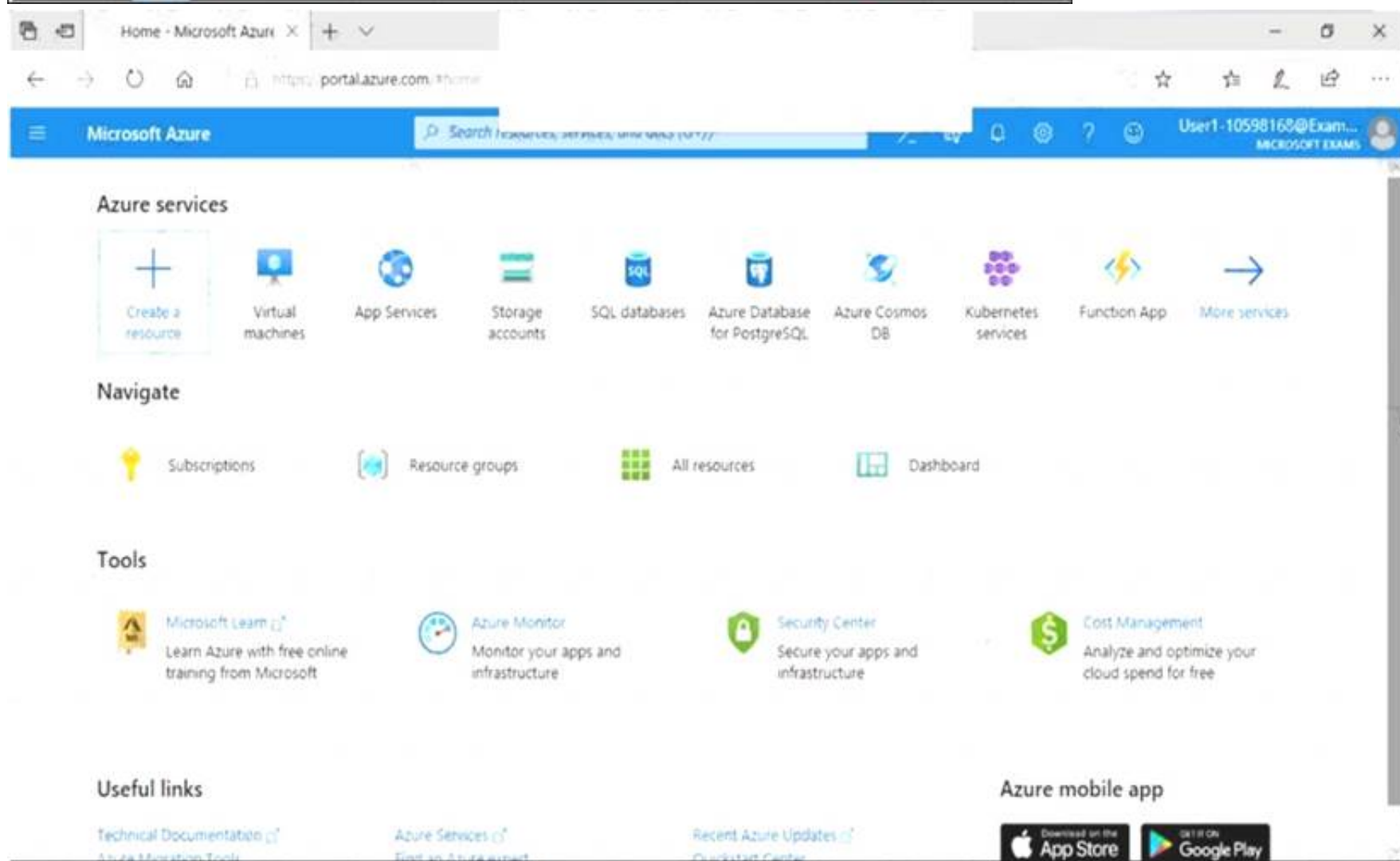
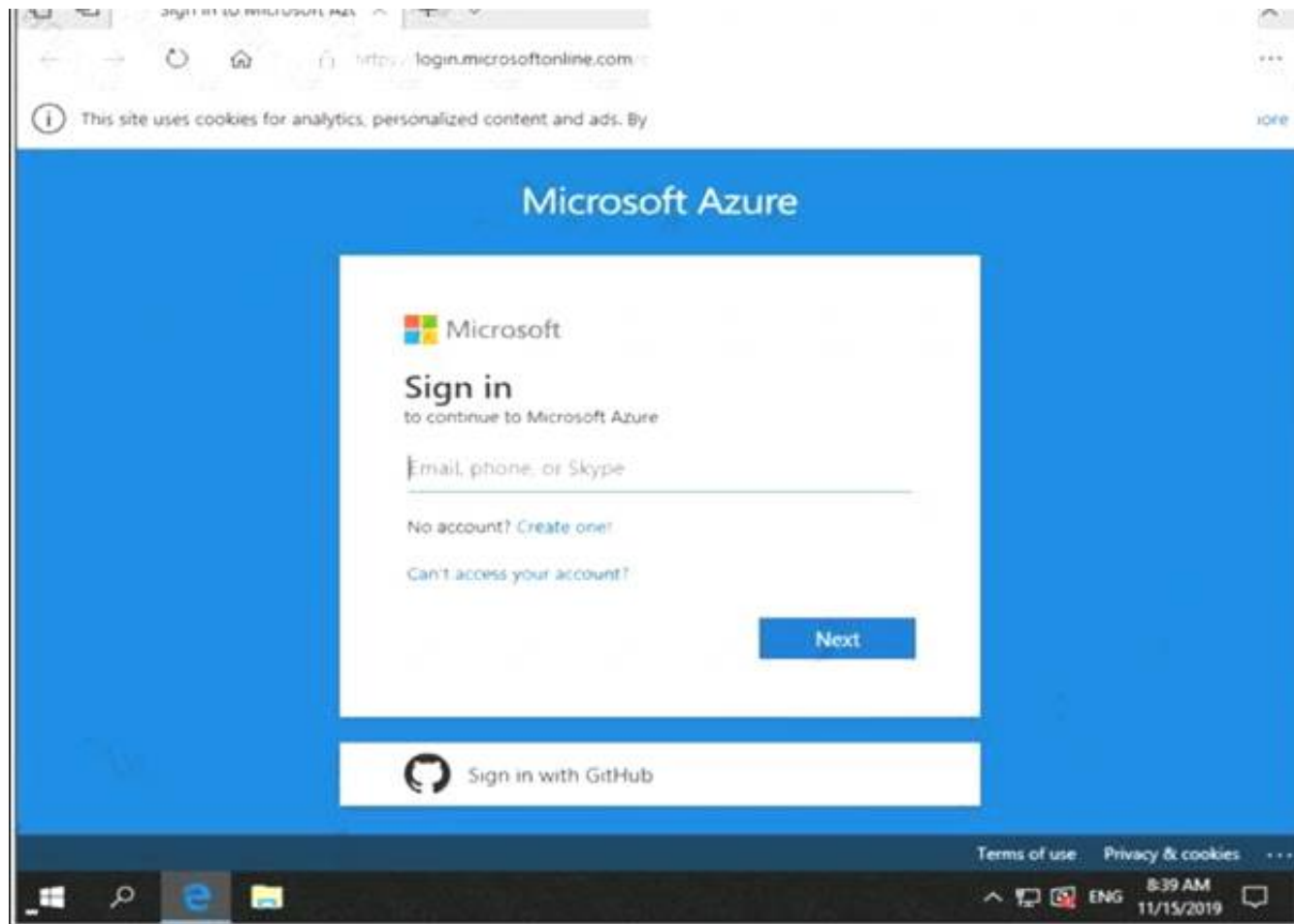
Use the following login credentials as needed:

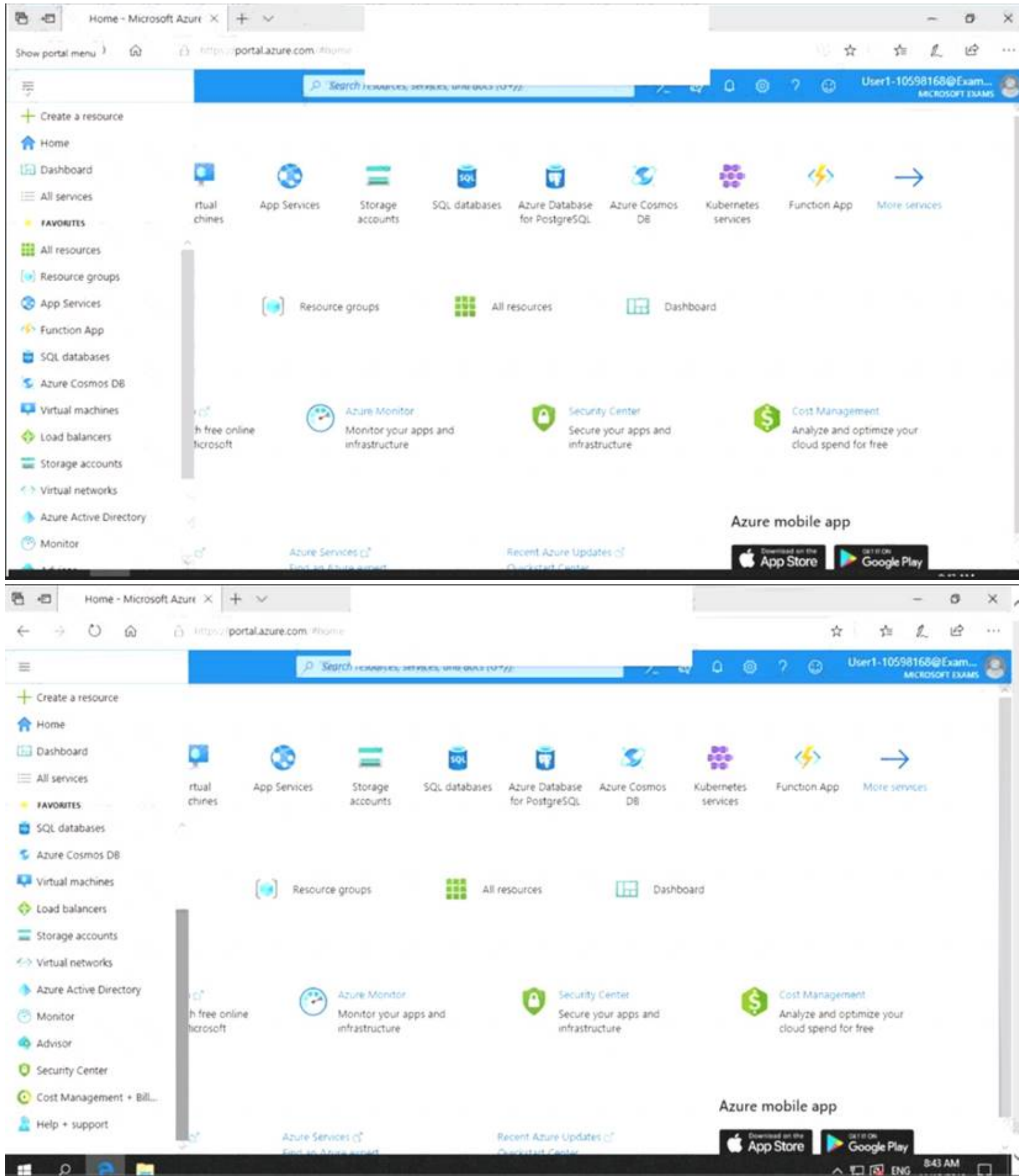
To enter your username, place your cursor in the Sign in box and click on the username below.

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 ensure that a user named user21059868 can manage the properties of the virtual machines in the RG1lod10598168 resource group. The solution must use the principle of least privilege.
 To complete this task, sign in to the Azure portal.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

- * 1. In Azure portal, locate and select the RG1lod10598168 resource group.
- * 2. Click Access control (IAM).
- * 3. Click the Role assignments tab to view all the role assignments at this scope.
- * 4. Click Add > Add role assignment to open the Add role assignment pane.



- * 5. In the Role drop-down list, select the role Virtual Machine Contributor. Virtual Machine Contributor lets you manage virtual machines, but not access to them, and not the virtual network or storage account they're connected to.
- * 6. In the Select list, select user user21059868
- * 7. Click Save to assign the role. Reference:
<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal> <https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-contributor>

NEW QUESTION 245

- (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 250

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

User	Role
User1	AcrPush
User2	AcrPull
User3	AcrImageSigner
User4	Contributor

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

Upload images:

▼

User1 only

User1 and User4 only

User1, User3, and User4

User1, User2, User3, and User4

Download images:

▼

User2 only

User1 and User2 only

User2 ad User4 only

User1, User2, and User4

User1, User2, User3, and User4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: User1 and User4 only

Owner, Contributor and AcrPush can push images. Box 2: User1, User2, and User4

All, except AcrImageSigner, can download/pull images.

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

References:

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

NEW QUESTION 253

- (Exam Topic 4)

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

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

User1 is a member of Group1. Group1 and User2 are assigned the Key Vault Contributor role for Vault1.

On January 1, 2019, you create a secret in Vault1. The secret is configured as shown in the exhibit. (Click the Exhibit tab.)

Create a secret

Upload options

Manual

* Name ⓘ

Password1

* Value

• • • • •

Content type (optional)

Set activation date? ⓘ ☒

Activation Date

2019-03-01



12:00:00 AM

(UTC+02:00) --- Current Time Zone ---

Set expiration Date? ⓘ ☒

Expiration Date

2020-03-01



12:00:00 AM

(UTC+02:00) --- Current Time Zone ---

Enabled?

Yes

No

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

➤ Key Management Operations: Get, List, and Restore

> Cryptographic Operations: Decrypt and Unwrap Key
> Secret Management Operations: Get, List, and Restore
Group1 is assigned an access to Vault1. The policy has the following configurations:
> Key Management Operations: Get and Recover
> Secret Management Operations: List, Backup, and Recover
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Statements	Yes	No
On January 1, 2019, User1 can view the value of Password1.	<input type="radio"/>	<input type="radio"/>
On June 1, 2019, User2 can view the value of Password1.	<input type="radio"/>	<input type="radio"/>
On June 1, 2019, User1 can view the value of Password1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
On January 1, 2019, User1 can view the value of Password1.	<input type="radio"/>	<input checked="" type="radio"/>
On June 1, 2019, User2 can view the value of Password1.	<input checked="" type="radio"/>	<input type="radio"/>
On June 1, 2019, User1 can view the value of Password1.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 256

- (Exam Topic 4)
You have an Azure subscription.
You need to create and deploy an Azure policy that meets the following requirements:

- > When a new virtual machine is deployed, automatically install a custom security extension.
- > Trigger an autogenerated remediation task for non-compliant virtual machines to install the extension. What should you include in the policy? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Definition effect:

▼

Append

DeployIfNotExists

EnforceOPAConstraint

EnforceRegoPolicy

Modify

Assignment remediation task:

▼

A managed identity that has the Contributor role

A managed identity that has the User Access Administrator role

A service principal that has the Contributor role

A service principal that has the User Access Administrator role

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 259

- (Exam Topic 4)

You have an Azure subscription that contains an Azure SQL database named SQL1. You plan to deploy a web app named App1.

You need to provide App1 with read and write access to SQL1. The solution must meet the following requirements:

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

Which type of account should App1 use to access SQL1, and which database roles should you assign to App1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Account type:

Azure Active Directory User
Managed identity
Service Principal

Roles:

db_datawriter only
db_datareader and db_datawriter
db owner only

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/tutorial-connect-msi-sql-database?tabs=windowsclient%2Cd>

NEW QUESTION 262

- (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 264

- (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 265

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 268

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

Configure App1 to authenticate by using a:

Key

Certificate

Passphrase

User-assigned managed identity

System-assigned managed identity

Configure a Key Vault reference for App1 from the:

Extensions blade

General settings tab

TLS/SSL settings blade

Application settings tab

- A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 271

- (Exam Topic 4)
You have an Azure subscription that contains an Azure Sentinel workspace.
Azure Sentinel is configured to ingest logs from several Azure workloads. A third-party service management platform is used to manage incidents.
You need to identify which Azure Sentinel components to configure to meet the following requirements:

- When Azure Sentinel identifies a threat, an incident must be created.
- A ticket must be logged in the service management platform when an incident is created in Azure Sentinel.

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

When Azure Sentinel identifies a threat, an incident must be created:

Analytics

Data connectors

Playbooks

Workbooks

A ticket must be logged in the service management platform when an incident is created in Azure Sentinel:

Analytics

Data connectors

Playbooks

Workbooks

- A. Mastered

B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 275

- (Exam Topic 4)

You have an Azure subscription that uses Azure Active Directory (Azure AD) Privileged Identity Management (PIM).

A PIM user that is assigned the User Access Administrator role reports receiving an authorization error when performing a role assignment or viewing the list of assignments.

You need to resolve the issue by ensuring that the PIM service principal has the correct permissions for the subscription. The solution must use the principle of least privilege.

Which role should you assign to the PIM service principle?

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

Answer: B

NEW QUESTION 278

- (Exam Topic 4)

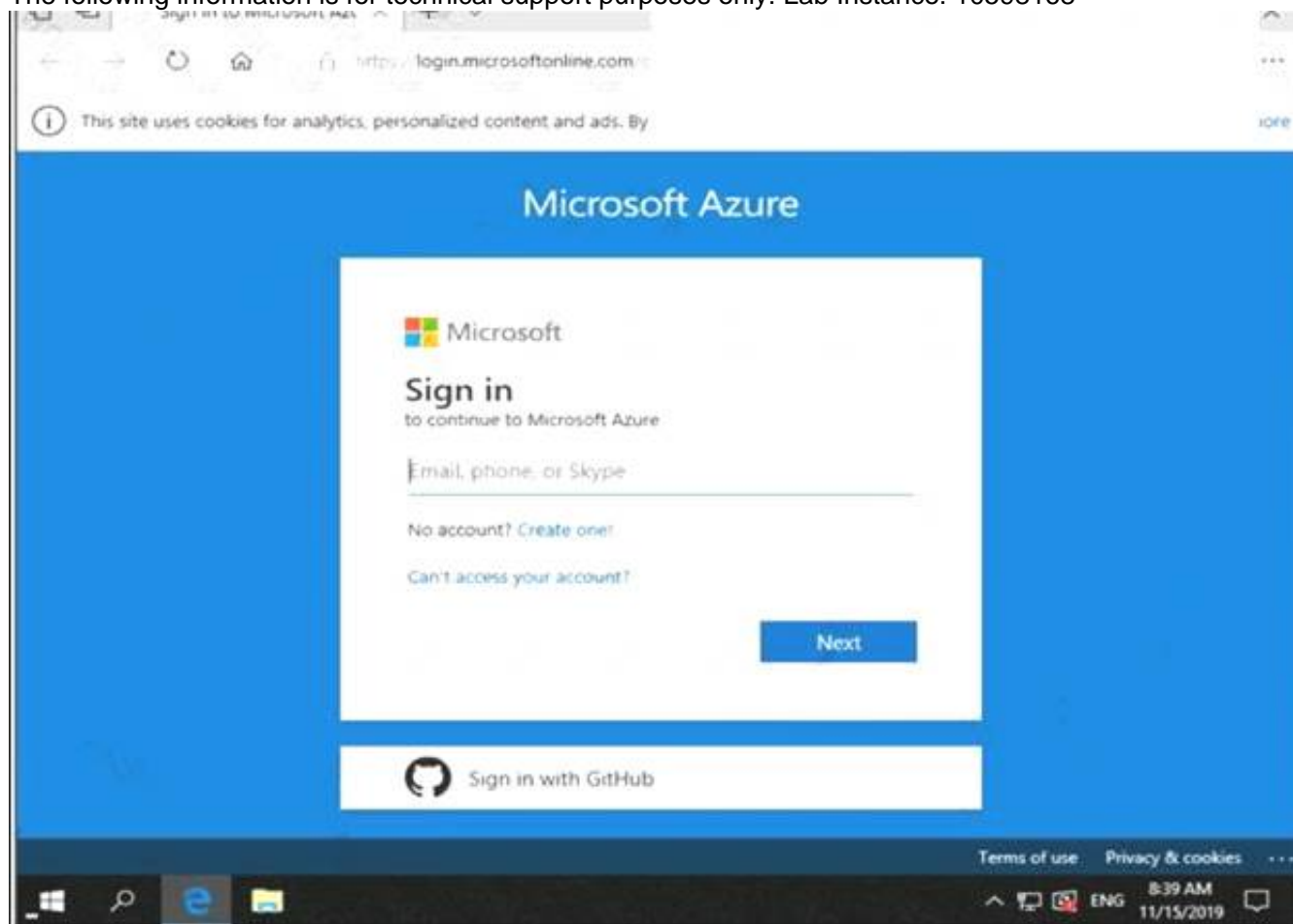
Use the following login credentials as needed:

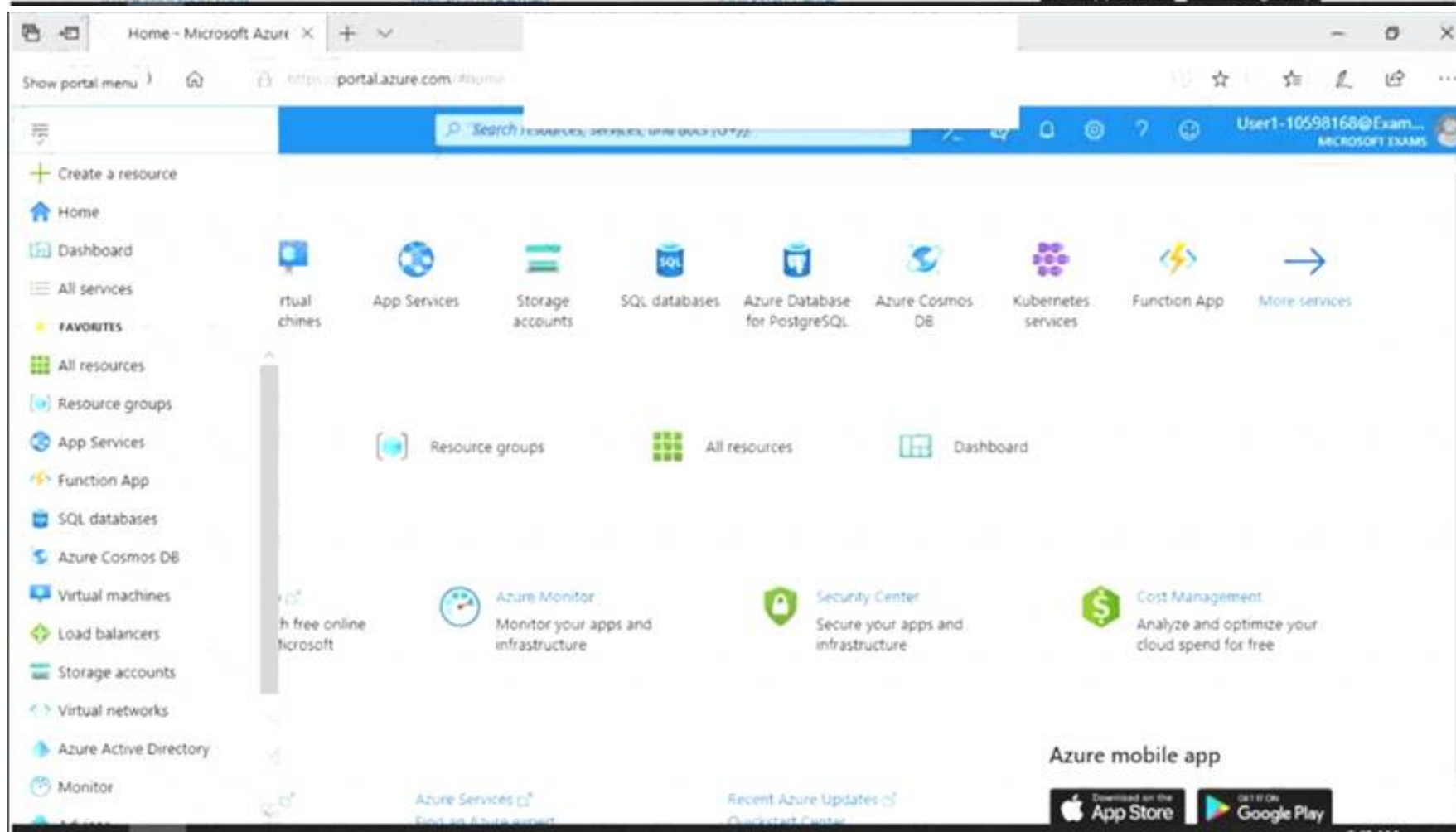
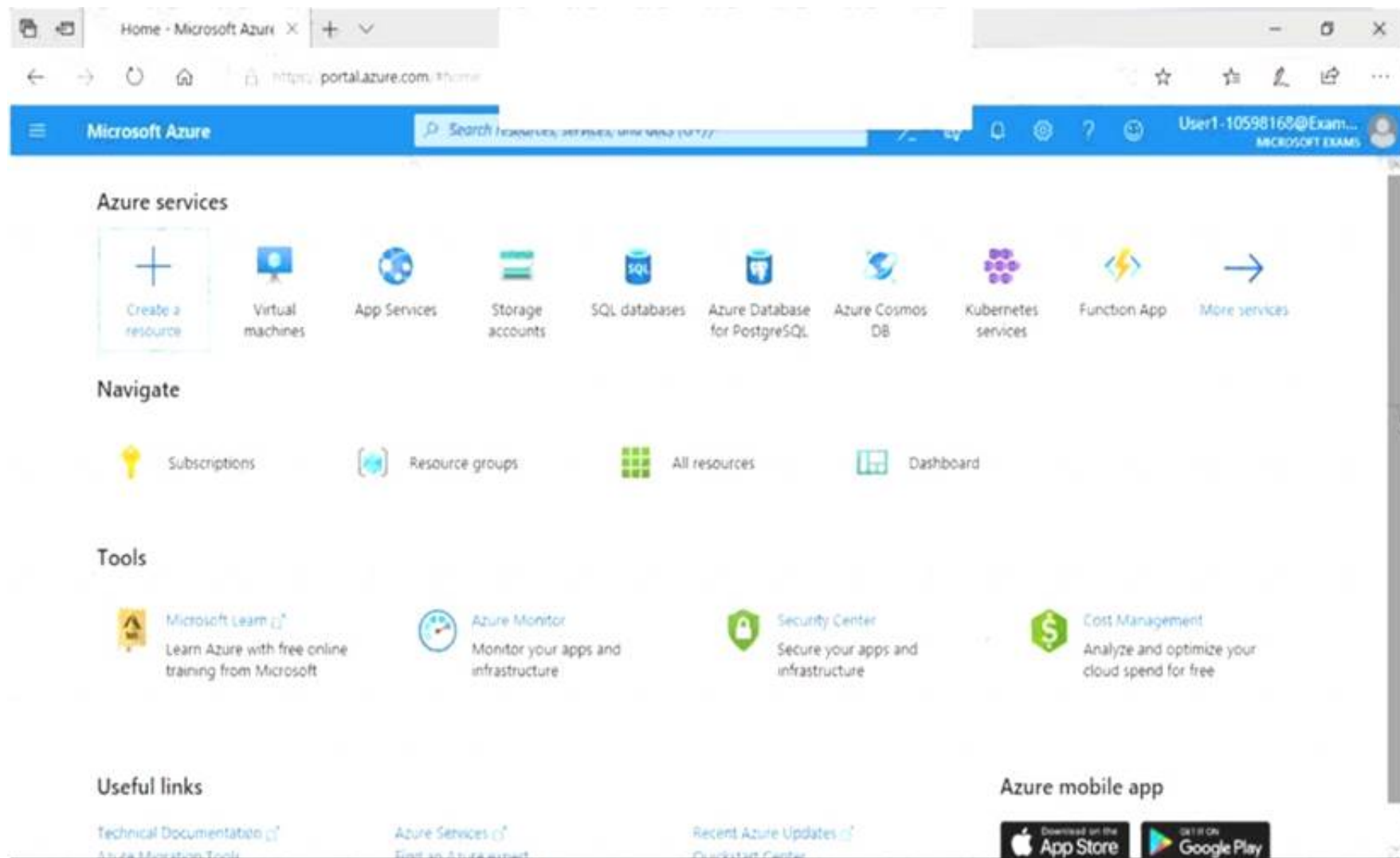
To enter your username, place your cursor in the Sign in box and click on the username below.

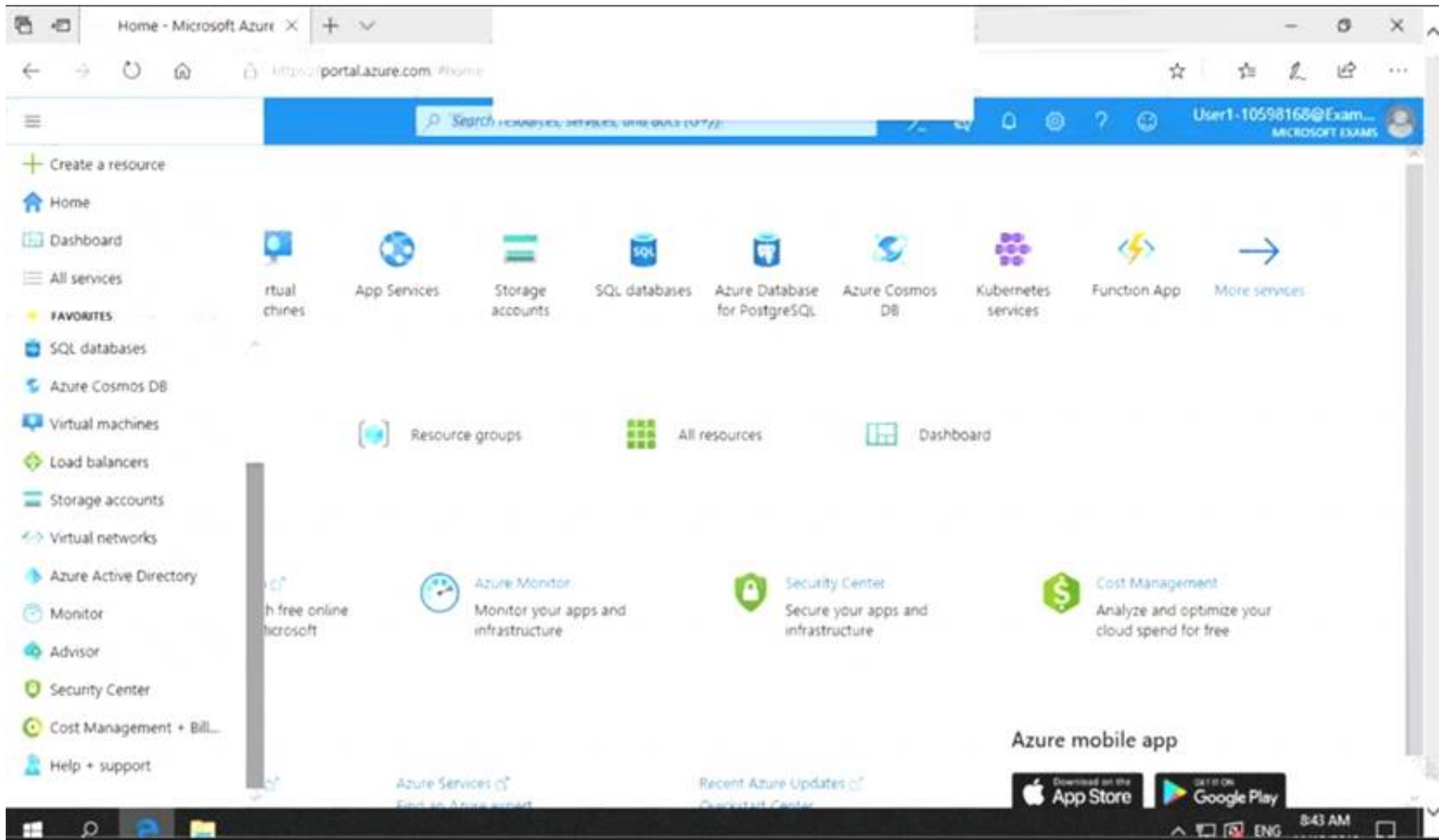
To enter your password, place your cursor in the Enter password box and click on the password below. Azure Username: User1-10598168@ExamUsers.com

Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only: Lab Instance: 10598168







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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Create an alert rule on a metric with the Azure portal

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

Condition

Greater than

* Threshold

60

Period ⓘ

Over the last 5 minutes

Notify via

Email owners, contributors, and readers

☒

Additional administrator email(s)

admin@contoso.com

Webhook ⓘ

http://www.contoso.com/dowork?param

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

NEW QUESTION 280

- (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 284

- (Exam Topic 4)

You have a Microsoft Sentinel deployment.

You need to connect a third-party security solution to the deployment. The third-party solution will send Common Event Format (CEF-formatted messages).

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

Answer Area

Deploy:

Forward events to Microsoft Sentinel by using:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Deploy:

Forward events to Microsoft Sentinel by using:

NEW QUESTION 286

- (Exam Topic 4)

You have an Azure subscription that contains the virtual machines shown in the following table.

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

VNET1, VNET2, and VNET3 are peered with each other. You perform the following actions:

* Create two application security groups named ASG1 and ASG2 in the West US region.

* Add the network interface of VM1 to ASG1.

Answer Area

ASG1:

ASG2:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 289

- (Exam Topic 4)

You need to recommend which virtual machines to use to host App1. The solution must meet the technical requirements for KeyVault1. Which virtual machines should you use?

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

Answer: D

NEW QUESTION 291

- (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 then 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 293

- (Exam Topic 4)

You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant. From the Azure portal, you register an enterprise application.

Which additional resource will be created in Azure AD?

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

Answer: A

Explanation:

Reference:

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

NEW QUESTION 297

- (Exam Topic 4)

You have an Azure subscription named Subscription1 that contains an Azure Active Directory (Azure AD) tenant named contosos.com and a resource group named RG1.

You create a custom role named Role1 for contoso.com.

You need to identify where you can use Role1 for permission delegation. What should you identify?

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

Answer: A

Explanation:

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

NEW QUESTION 302

- (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 303

- (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.	<input type="radio"/>	<input type="radio"/>
An Azure virtual machine on Subnet2 can access data in Contoso1901.	<input type="radio"/>	<input type="radio"/>
A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901.	<input type="radio"/>	<input type="radio"/>

- 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 304

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

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

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

Name	Role
VM1	<ul style="list-style-type: none">Storage Blob Data Reader for storage1Key Vault Reader for Vault1
VM2	<ul style="list-style-type: none">Storage Blob Data Reader for storage1Key Vault Reader for Vault1
VM3	<ul style="list-style-type: none">Storage Blob Data Reader for storage1Key Vault Reader for Vault1Key Vault Reader for Vault2
VM4	<ul style="list-style-type: none">Storage Blob Data Reader for storage1Key Vault Reader for Vault1Key Vault Reader for Vault2

You need to assign managed identities to the virtual machines. The solution must meet the following requirements:

- Assign each virtual machine the required roles.
- Use the principle of least privilege.

What is the minimum number of managed identities required?

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

Answer: B

Explanation:

We have two different sets of required permissions. VM1 and VM2 have the same permission requirements. VM3 and VM4 have the same permission requirements.
A user-assigned managed identity can be assigned to one or many resources. By using user-assigned managed identities, we can create just two managed identities: one with the permission requirements for VM1 and VM2 and the other with the permission requirements for VM3 and VM4.
Reference:
<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

NEW QUESTION 305

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

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

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

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

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

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

Answer: C

Explanation:

Only network interfaces in NVET1, which consists of Subnet11 and Subnet12, can be configured in ASG1, as all network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in.

Reference:

<https://azure.microsoft.com/es-es/blog/applicationsecuritygroups/>

NEW QUESTION 308

- (Exam Topic 4)

Your network contains an Active Directory forest named contoso.com. The forest contains a single domain.

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to deploy Azure AD Connect and to integrate Active Directory and the Azure AD tenant. You need to recommend an integration solution that meets the following requirements:

Ensures that password policies and user logon restrictions apply to user accounts that are synced to the Tenant Minimizes the number of servers required for the solution.

Which authentication method should you include in the recommendation?

- A. federated identity with Active Directory Federation Services (AD FS)
- B. password hash synchronization with seamless single sign-on (SSO)
- C. pass-through authentication with seamless single sign-on (SSO)

Answer: C

Explanation:

* 1. Ensures that password policies and user logon restrictions apply to user accounts that are synced to the tenant

>> Pass-Through Authentication enforce on-premises user account states, password policies, and sign-in hours.

* 2. Minimizes the number of servers required for the solution.

>> Pass-through needs a lightweight agent to be installed one (or more) on-premises servers.

>> PW Hash also require installing Azure AD Connect on your existing DC.

NEW QUESTION 309

- (Exam Topic 4)

You have 15 Azure virtual machines in a resource group named RG1. All virtual machines run identical applications.

You need to prevent unauthorized applications and malware from running on the virtual machines. What should you do?

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

Answer: B

Explanation:

Adaptive application control is an intelligent, automated end-to-end application whitelisting solution from Azure Security Center. It helps you control which applications can run on your Azure and non-Azure VMs (Windows and Linux), which, among other benefits, helps harden your VMs against malware. Security Center uses machine learning to analyze the applications running on your VMs and helps you apply the specific whitelisting rules using this intelligence.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application>

NEW QUESTION 311

- (Exam Topic 4)

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

Actions

Create a management group.

Add the three subscriptions to the management group.

Assign User1 the Global administrator role.

Assign User1 the Owner role for the management group.

Assign User1 the Cost Management Contributor role for the management group.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

Create a management group.

Add the three subscriptions to the management group.

Assign User1 the Global administrator role.

Assign User1 the Owner role for the management group.

Assign User1 the Cost Management Contributor role for the management group.

Assign User1 the Cost Management Contributor role for the management group.

Assign User1 the Global administrator role.

Add the three subscriptions to the management group.

NEW QUESTION 315

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

- An Azure key vault
- An Azure SQL database named Database1
- Two Azure App Service web apps named AppSrv1 and AppSrv2 that are configured to use system-assigned managed identities and access Database1

You need to implement an encryption solution for Database1 that meets the following requirements:

- The data in a column named Discount in Database1 must be encrypted so that only AppSrv1 can decrypt the data.
- AppSrv1 and AppSrv2 must be authorized by using managed identities to obtain cryptographic keys. How should you configure the encryption settings for Database1 To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

To configure the encryption of Database1:

Always Encrypted by using Azure Key Vault.

Always Encrypted by using the Windows Certificate Store.

Transparent Data Encryption (TDE) by using Azure Key Vault integration.

Transparent Data Encryption (TDE) by using Bring Your Own Key (BYOK).

To obtain the cryptographic keys:

Create an access policy in Azure Key Vault.

Generate a key on an HSM device.

Import App Service certificates to AppSrv1 and AppSrv2.

Register an enterprise application in Azure AD.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text Description automatically generated with medium confidence

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/always-encrypted-azure-key-vault-configure?tabs=az>

NEW QUESTION 319

- (Exam Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a hybrid configuration of Azure Active Directory (AzureAD). You have an Azure HDInsight cluster on a virtual network.

You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials. You need to configure the environment to support the planned authentication.

Solution: You create a site-to-site VPN between the virtual network and the on-premises network. Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

You can connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.

Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:

Create Azure Virtual Network.

Create a custom DNS server in the Azure Virtual Network.

Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.

Configure forwarding between the custom DNS server and your on-premises DNS server. References:

<https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network>

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal>

NEW QUESTION 320

- (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 325

- (Exam Topic 4)

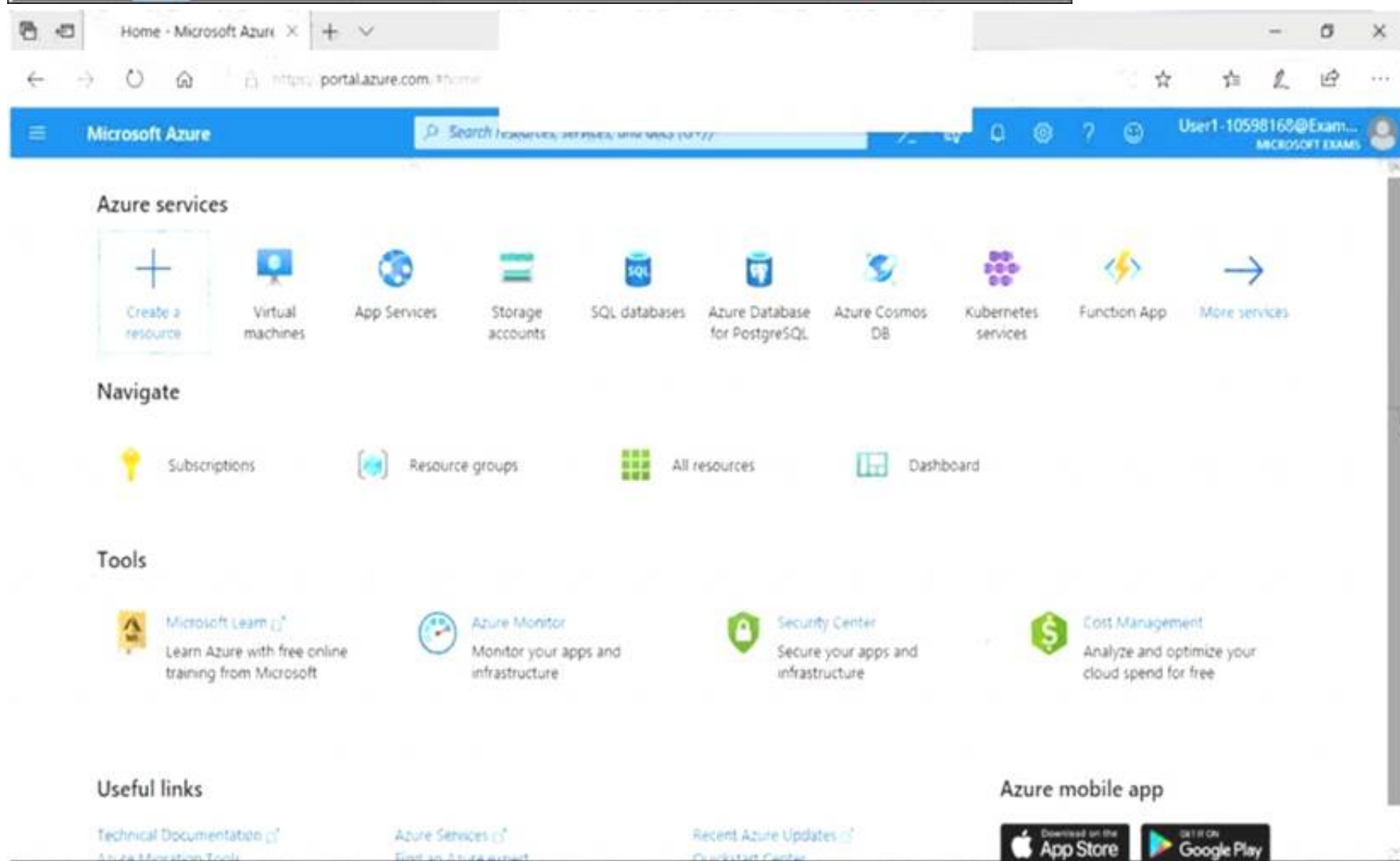
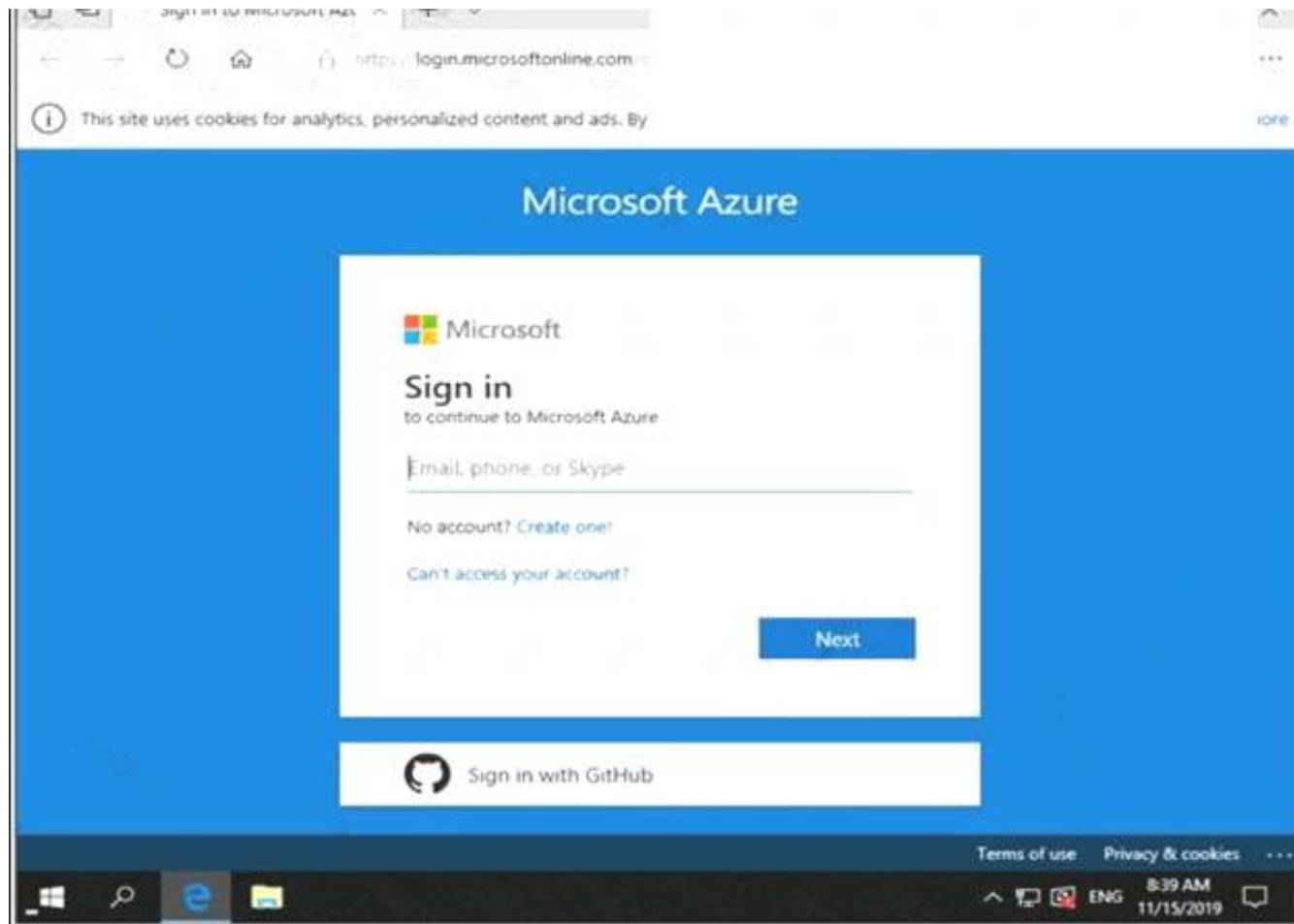
Use the following login credentials as needed:

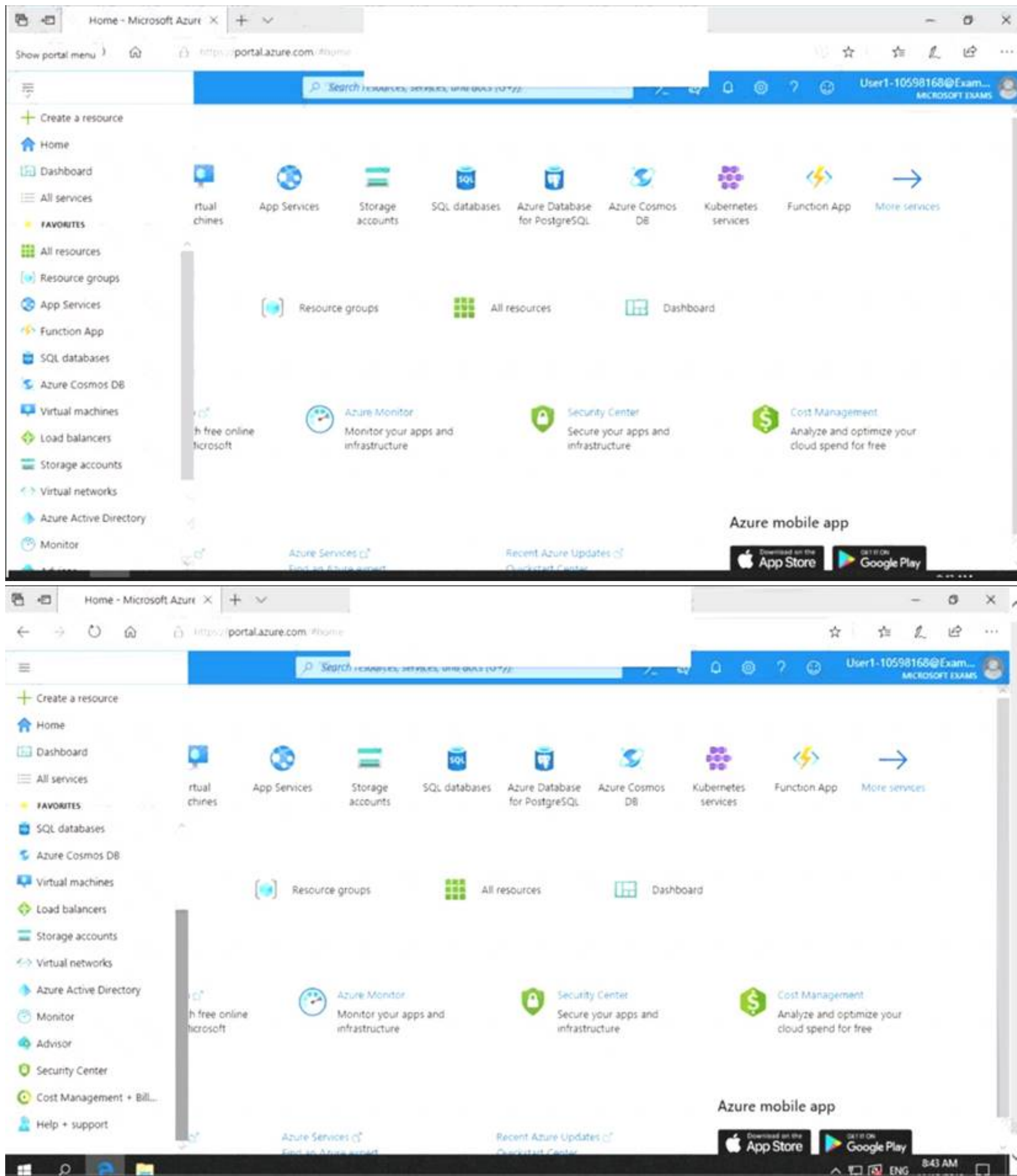
To enter your username, place your cursor in the Sign in box and click on the username below.

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Step 1: To enable customer-managed keys in the Azure portal, follow these steps:

- * 1. Navigate to your storage account rg1lod10598168n1
- * 2. On the Settings blade for the storage account, click Encryption. Select the Use your own key option, as shown in the following figure.

 Save
  Discard

Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

By default, data is encrypted using Microsoft Managed Keys for Azure Blobs, Tables, Files and Queues. You may choose to bring your own key for encryption for Azure Blobs and Files. Encryption for Tables and Queues will always use Microsoft Managed Keys.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process.

[Learn more](#)



Your storage account is currently encrypted with Microsoft managed key by default. You can choose to use your own key.

☐ Use your own key

Step 2: Specify a key from a key vault

To specify a key from a key vault, first make sure that you have a key vault that contains a key. To specify a key from a key vault, follow these steps:

- * 4. Choose the Select from Key Vault option.
- * 5. Choose the key vault KeyVault10598168 containing the key you want to use.
- * 6. Choose the key from the key vault.

 Save
  Discard

Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

By default, data is encrypted using Microsoft Managed Keys for Azure Blobs, Tables, Files and Queues. You may choose to bring your own key for encryption for Azure Blobs and Files. Encryption for Tables and Queues will always use Microsoft Managed Keys.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process.

[Learn more](#)


Your storage account is currently encrypted with Microsoft managed key by default. You can choose to use your own key.

☒ Use your own key

Encryption key
☐ Enter key URI
☒ Select from Key Vault

* Key Vault
 <key-vault>

* Encryption key
 <key>

 <storage-account> will be granted access to the selected key vault. Both soft delete and purge protection will be enabled on the key vault and cannot be disabled. [Learn more](#)

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

NEW QUESTION 329

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

az-500 Practice Exam Features:

- * az-500 Questions and Answers Updated Frequently
- * az-500 Practice Questions Verified by Expert Senior Certified Staff
- * az-500 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * az-500 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The az-500 Practice Test Here](#)