

Exam Questions az-500

Microsoft Azure Security Technologies

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



NEW QUESTION 1

- (Exam Topic 4)

You are collecting events from Azure virtual machines to an Azure Log Analytics workspace. You plan to create alerts based on the collected events

You need to identify which Azure services can be used to create the alerts.

Which two services should you identify? Each correct answer presents a complete solution NOTE: Each correct selection is worth one point.

- A. Azure Monitor
- B. Azure Security Center
- C. Azure Analytics Services
- D. Azure Sentinel
- E. Azure Advisor

Answer: AD

Explanation:

<https://docs.microsoft.com/en-us/azure/analysis-services/analysis-services-overview>

NEW QUESTION 2

- (Exam Topic 4)

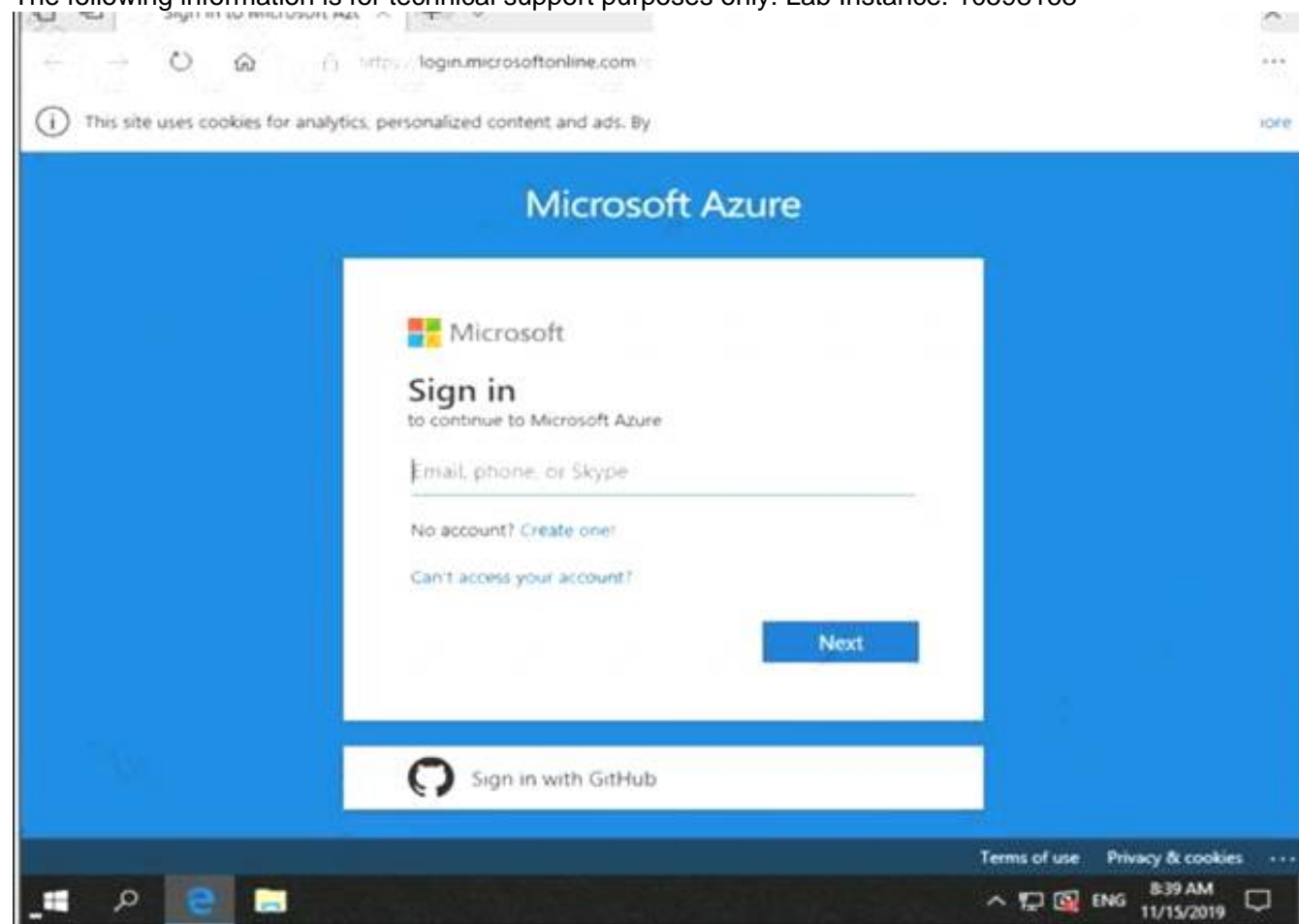
Use the following login credentials as needed:

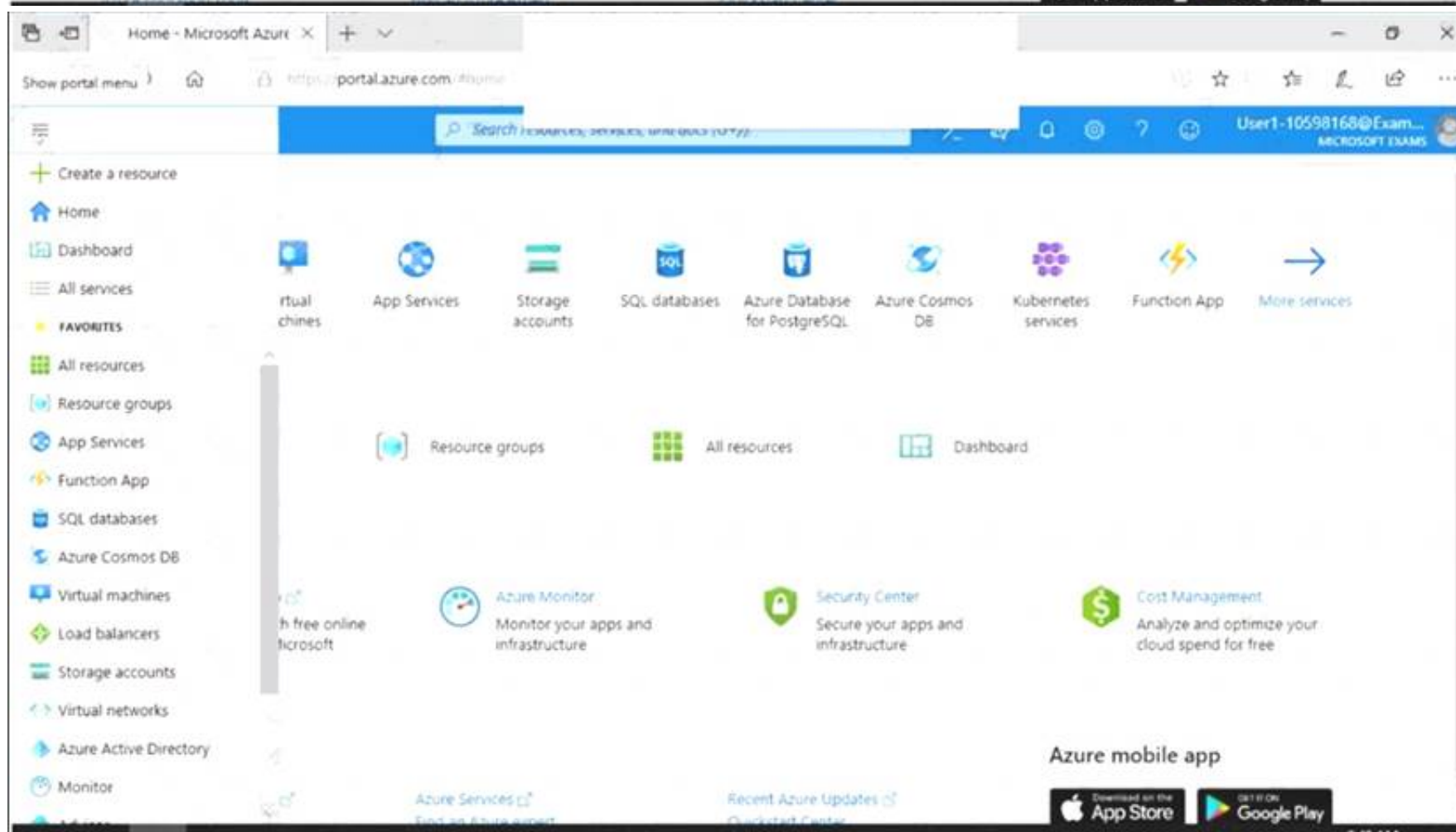
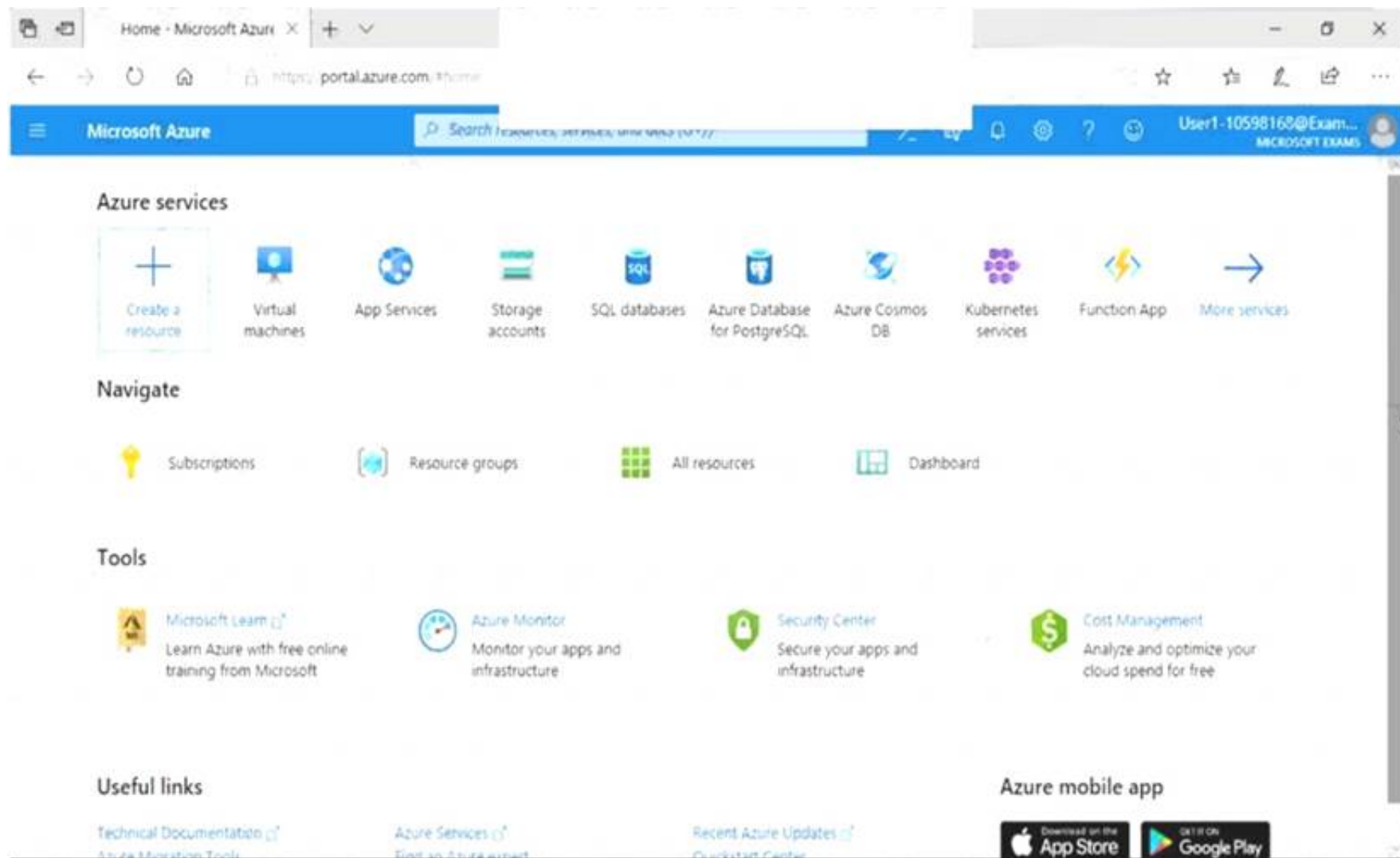
To enter your username, place your cursor in the Sign in box and click on the username below.

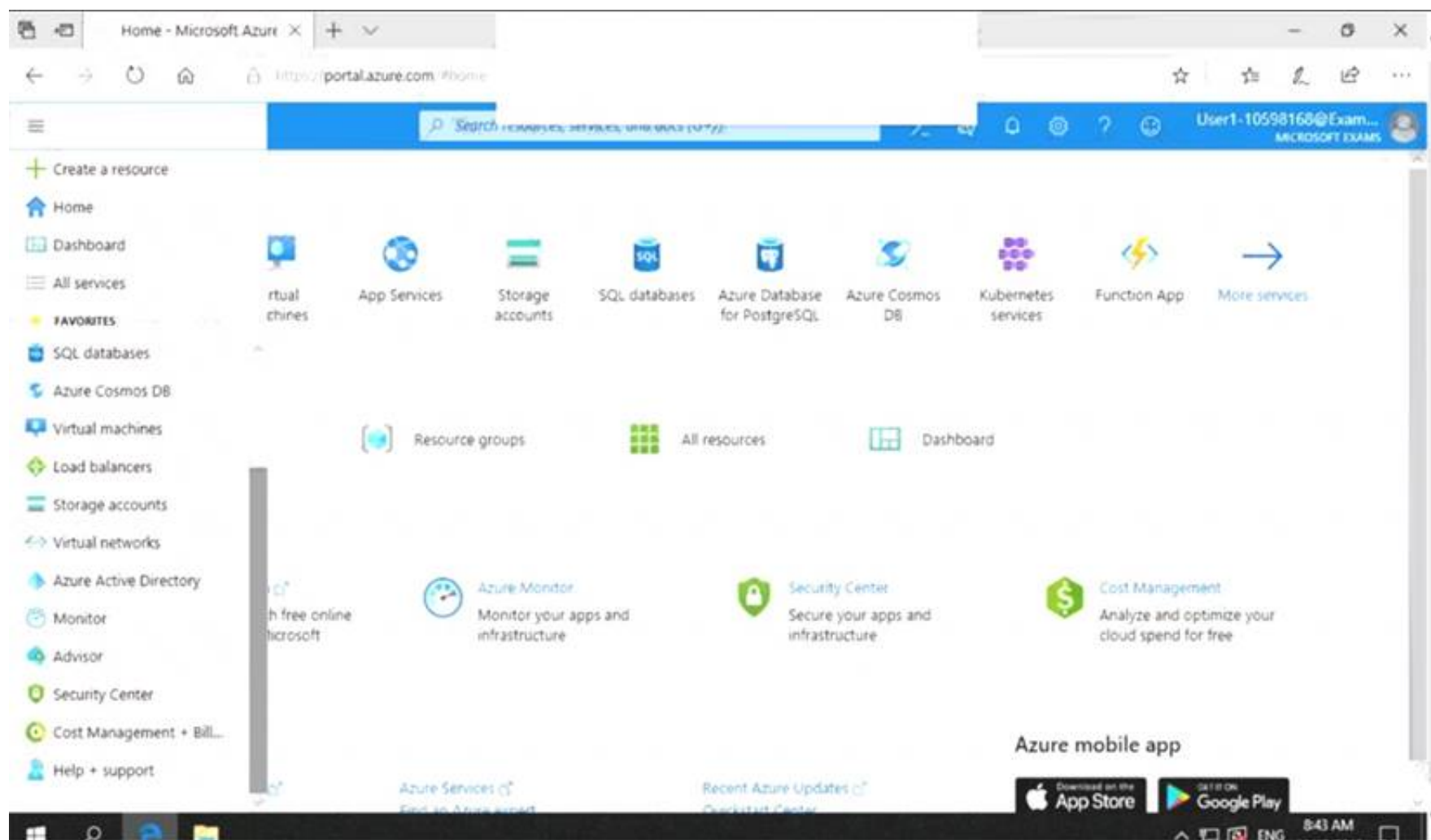
To enter your password, place your cursor in the Enter password box and click on the password below. Azure Username: User1-10598168@ExamUsers.com

Azure Password: Ag1Bh9!#Bd

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







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

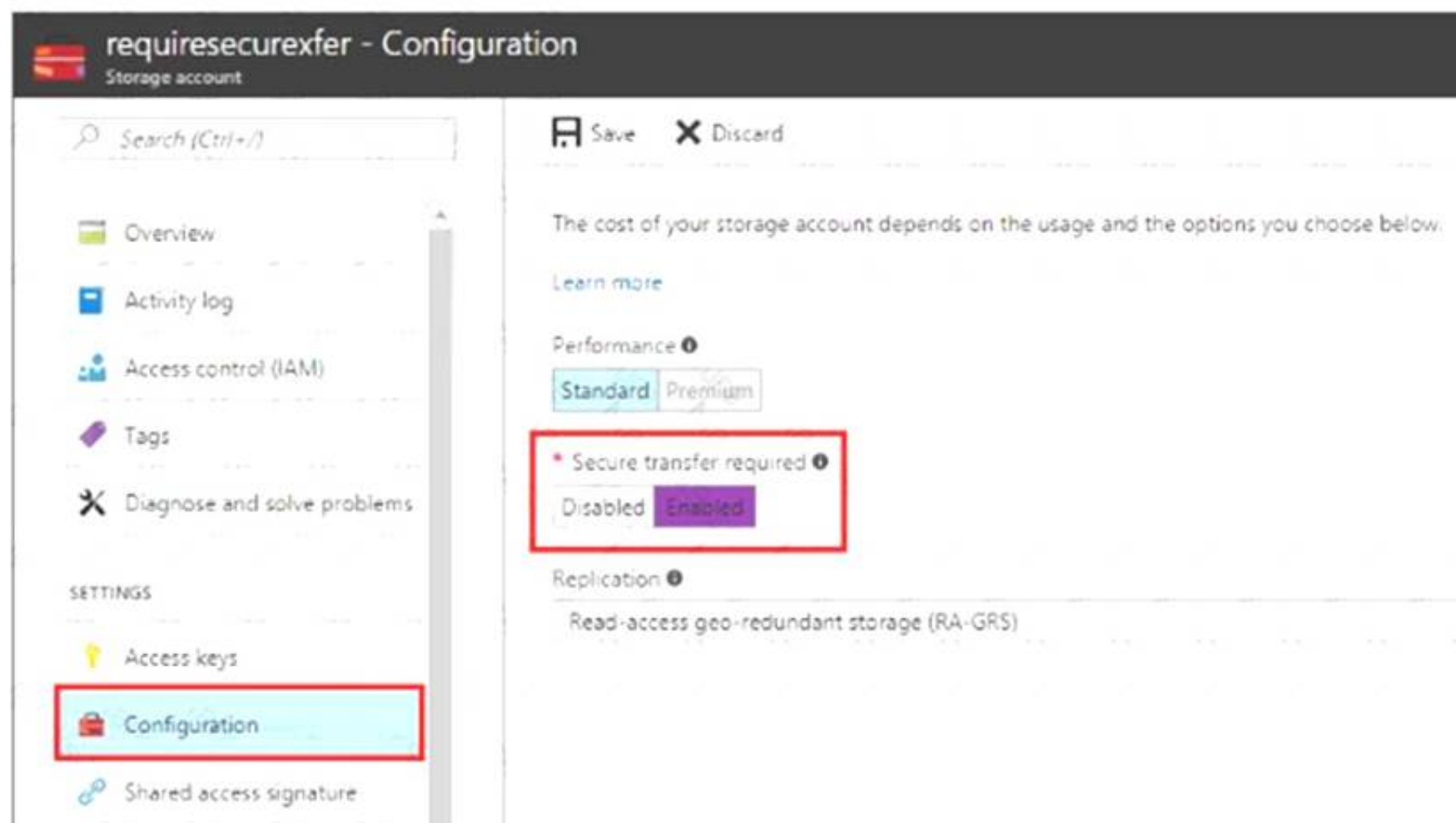
- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The "Secure transfer required" feature is now supported in Azure Storage account. This feature enhances the security of your storage account by enforcing all requests to your account through a secure connection. This feature is disabled by default.

- * 1. In Azure Portal select you Azure Storage account rg1lod10598168n1.
- * 2. Select Configuration, and Secure Transfer required.



Reference:

<https://techcommunity.microsoft.com/t5/Azure/quot-Secure-transfer-required-quot-is-available-in-Azure-Storag>

NEW QUESTION 3

- (Exam Topic 4)

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

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

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

Custom smart lockout

Lockout threshold ⓘ ✓

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 4

- (Exam Topic 4)

You have an Azure subscription that contains 100 virtual machines. Azure Diagnostics is enabled on all the virtual machines.

You are planning the monitoring of Azure services in the subscription. You need to retrieve the following details:

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

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

NOTE: Each correct selection is worth one point.

Settings

Answer Area

Activity log

Logs

Metrics

Service Health

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box1: Activity log

Azure activity logs provide insight into the operations that were performed on resources in your subscription. Activity logs were previously known as “audit logs” or “operational logs,” because they report control-plane events for your subscriptions.

Activity logs help you determine the “what, who, and when” for write operations (that is, PUT, POST, or DELETE).

Box 2: Logs

Log Integration collects Azure diagnostics from your Windows virtual machines, Azure activity logs, Azure Security Center alerts, and Azure resource provider logs. This integration provides a unified dashboard for all your assets, whether they're on-premises or in the cloud, so that you can aggregate, correlate, analyze, and alert for security events.

References:

<https://docs.microsoft.com/en-us/azure/security/azure-log-audit>

NEW QUESTION 5

- (Exam Topic 4)

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 6

- (Exam Topic 4)

You need to configure a virtual network named VNET2 to meet the following requirements:

➤ Administrators must be prevented from deleting VNET2 accidentally.

➤ Administrators must be able to add subnets to VNET2 regularly.

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

- A. Mastered
- B. Not Mastered

Answer: A

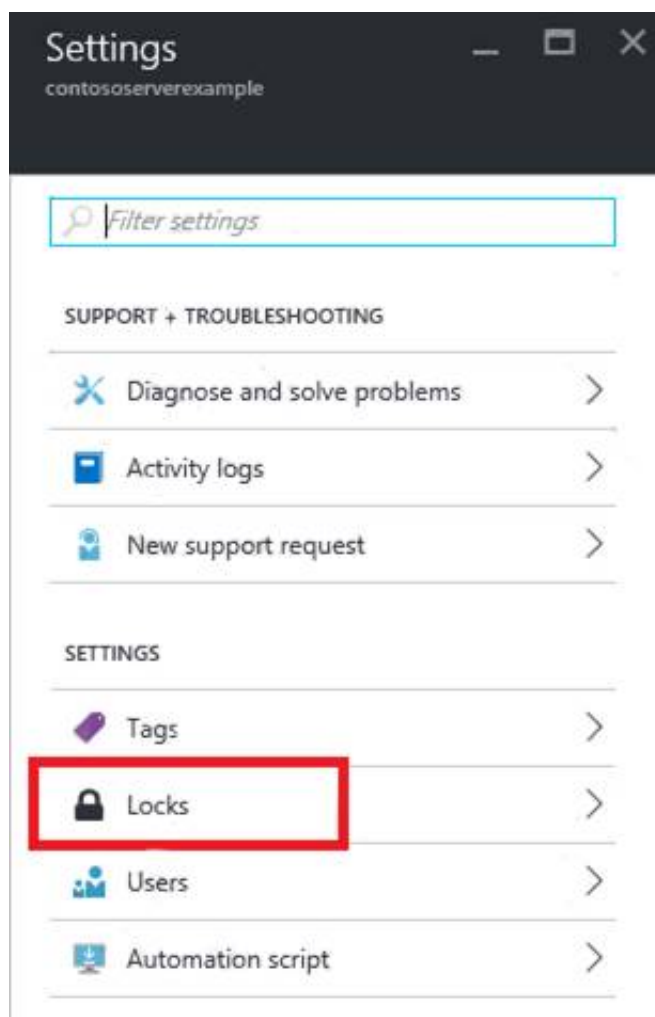
Explanation:

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

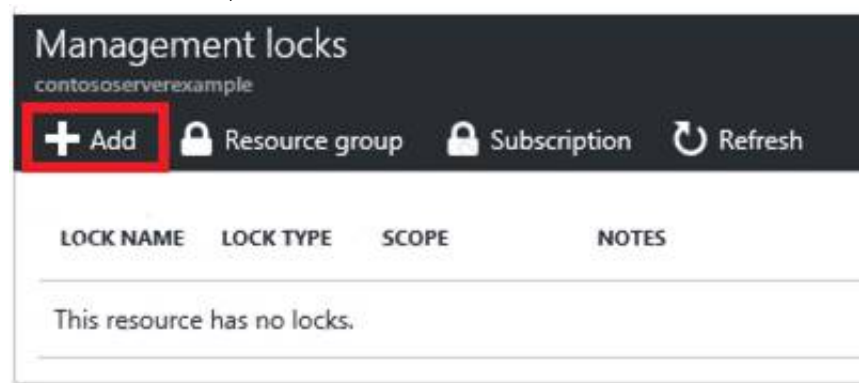
Note: In Azure, the term resource refers to an entity managed by Azure. For example, virtual machines, virtual networks, and storage accounts are all referred to as Azure resources.

* 1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET2. Alternatively, browse to Virtual Networks in the left navigation pane.

* 2. In the Settings blade for virtual network VNET2, select Locks.



* 3. To add a lock, select Add.



* 4. For Lock type select Delete lock, and click OK Reference:

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

NEW QUESTION 7

- (Exam Topic 4)

You have Azure Resource Manager templates that you use to deploy Azure virtual machines.

You need to disable unused Windows features automatically as instances of the virtual machines are provisioned.

What should you use?

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

Answer: B

Explanation:

You can use Azure Automation State Configuration to manage Azure VMs (both Classic and Resource Manager), on-premises VMs, Linux machines, AWS VMs, and on-premises physical machines.

Note: Azure Automation State Configuration provides a DSC pull server similar to the Windows Feature DSCService so that target nodes automatically receive configurations, conform to the desired state, and report back on their compliance. The built-in pull server in Azure Automation eliminates the need to set up and maintain your own pull server. Azure Automation can target virtual or physical Windows or Linux machines, in the cloud or on-premises.

References:

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

NEW QUESTION 8

- (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 9

- (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 10

- (Exam Topic 4)

You onboard Azure Sentinel. You connect Azure Sentinel to Azure Security Center.

You need to automate the mitigation of incidents in Azure Sentinel. The solution must minimize administrative effort.

What should you create?

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

Answer: B

NEW QUESTION 10

- (Exam Topic 4)

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant and a user named User1.

The App registrations settings for the tenant are configured as shown in the following exhibit.

App registrations

Users can register applications ⓘ

☐ Yes ☒ No

You plan to deploy an app named App1.

You need to ensure that User1 can register App1 in Azure AD. The solution must use the principle of least privilege.

Which role should you assign to User1?

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 15

- (Exam Topic 4)

You have three on-premises servers named Server1, Server2, and Server3 that run Windows Server1 and Server2 and located on the Internal network. Server3 is located on the premises network. All servers have access to Azure.

From Azure Sentinel, you install a Windows firewall data connector.

You need to collect Microsoft Defender Firewall data from the servers for Azure Sentinel. What should you do?

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 17

- (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.

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

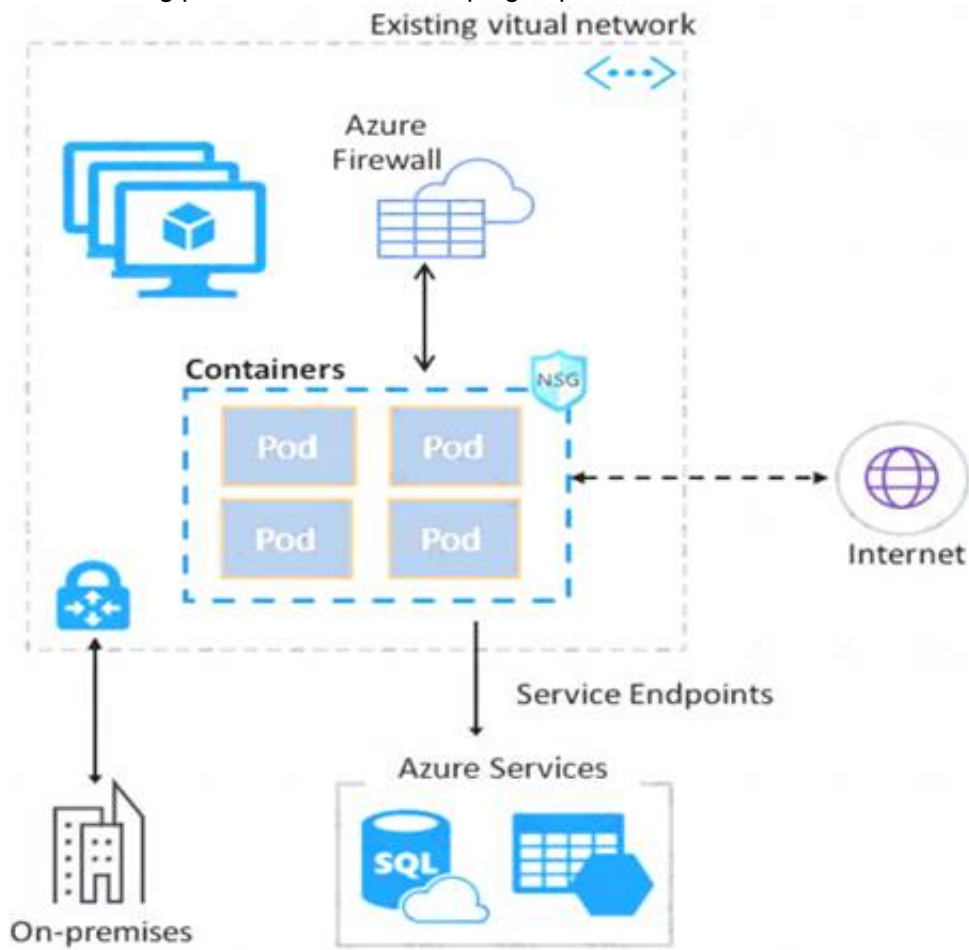
Answer: C

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 22

- (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 23

- (Exam Topic 4)

You have an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry. You need to use automatically generated service principal for the AKS cluster to authenticate to the Azure Container Registry.

What should you create?

- A. a secret in Azure Key Vault
- B. a role assignment
- C. an Azure Active Directory (Azure AD) user
- D. an Azure Active Directory (Azure AD) group

Answer: B

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal>

NEW QUESTION 25

- (Exam Topic 4)

You are troubleshooting a security issue for an Azure Storage account. You enable the diagnostic logs for the storage account.

What should you use to retrieve the diagnostics logs?

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

Answer: A

Explanation:

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

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

References:

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

NEW QUESTION 26

- (Exam Topic 4)

You have an Azure environment.

You need to identify any Azure configurations and workloads that are non-compliant with ISO 27001:2013 standards.

What should you use?

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

Answer: B

NEW QUESTION 30

- (Exam Topic 4)

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

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

You have an Azure subscription named Sub1.

You have an Azure Storage account named sa1 in a resource group named RG1.

Users and applications access the blob service and the file service in sa1 by using several shared access signatures (SASs) and stored access policies.

You discover that unauthorized users accessed both the file service and the blob service. You need to revoke all access to sa1.

Solution: You regenerate the Azure storage account access keys. Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

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

NEW QUESTION 33

- (Exam Topic 4)

You have an Azure web app named webapp1.

You need to configure continuous deployment for webapp1 by using an Azure Repo. What should you create first?

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

Answer: B

NEW QUESTION 34

- (Exam Topic 4)

You plan to connect several Windows servers to the WS11641655 Azure Log Analytics workspace.

You need to ensure that the events in the System event logs are collected automatically to the workspace after you connect the Windows servers.

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

- A. Mastered
- B. Not Mastered

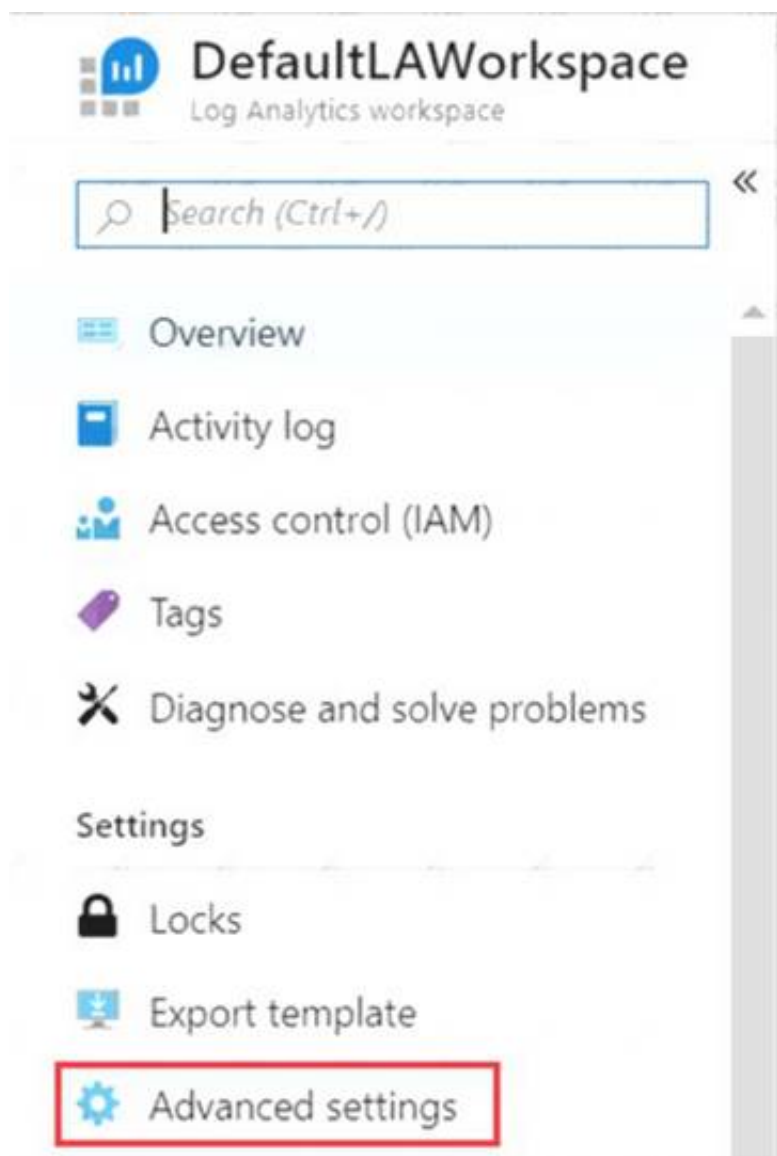
Answer: A

Explanation:

Azure Monitor can collect events from the Windows event logs or Linux Syslog and performance counters that you specify for longer term analysis and reporting, and take action when a particular condition is detected. Follow these steps to configure collection of events from the Windows system log and Linux Syslog, and several common performance counters to start with.

Data collection from Windows VM

* 1. In the Azure portal, locate the WS11641655 Azure Log Analytics workspace then select Advanced settings.



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

NEW QUESTION 37

- (Exam Topic 4)

You have an Azure subscription that contains an Azure SQL database named DB1 in the East US Azure region. You create the storage accounts shown in the following table.

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

You plan to enable auditing for DB1.

Which storage accounts can you use as the auditing destination for DB1?

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

Answer: C

NEW QUESTION 42

- (Exam Topic 4)

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

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

You have an Azure subscription named Subscription2 that contains the following resources:

- > An Azure Sentinel workspace
- > An Azure Event Grid instance

You need to ingest the CEF messages from the NVAs to Azure Sentinel. NOTE: Each correct selection is worth one point.

Answer Area

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

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

NEW QUESTION 47

- (Exam Topic 4)

You have an Azure subscription that uses Microsoft Sentinel.

You need to create a Microsoft Sentinel notebook that will use the Guided Investigation - Anomaly Lookup template.

What should you create first?

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

Answer: A

NEW QUESTION 52

- (Exam Topic 4)

You have an Azure subscription that contains the storage accounts shown in the following, table.

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

You enable Microsoft Defender for Storage.

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

Answer Area

Monitored storage services:

Protected storage accounts:

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Monitored storage services:

Protected storage accounts:

NEW QUESTION 57

- (Exam Topic 4)

You have an Azure subscription named Sub1.

In Azure Security Center, you have a workflow automation named WF1. WF1 is configured to send an email message to a user named User1. You need to modify WF1 to send email messages to a distribution group named Alerts. What should you use to modify WF1?

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

Answer: C

Explanation:

Reference:

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

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

NEW QUESTION 58

- (Exam Topic 4)

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

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

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

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

Solution: You create a policy definition and assignments that are scoped to resource groups. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

References:

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

NEW QUESTION 61

- (Exam Topic 4)

You have been tasked with configuring an access review, which you plan to assigned to a new collection of reviews. You also have to make sure that the reviews can be reviewed by resource owners.

You start by creating an access review program and an access review control. You now need to configure the Reviewers.

Which of the following should you set Reviewers to?

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

Answer: C

Explanation:

In the Reviewers section, select either one or more people to review all the users in scope. Or you can select to have the members review their own access. If the resource is a group, you can ask the group owners to review.

Graphical user interface, application Description automatically generated with medium confidence



Reference:

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

NEW QUESTION 62

- (Exam Topic 4)

You have an Azure subscription that contains four Azure SQL managed instances.

You need to evaluate the vulnerability of the managed instances to SQL injection attacks. What should you do first?

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

Answer: B

NEW QUESTION 63

- (Exam Topic 4)

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has an Active Directory forest with a single domain, named weylaindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.

You have been tasked with integrating Active Directory and the Azure AD tenant. You intend to deploy Azure AD Connect.

Your strategy for the integration must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.

Solution: You recommend the use of password hash synchronization and seamless SSO. Does the solution meet the goal?

A. Yes

B. No

Answer: B

NEW QUESTION 68

- (Exam Topic 4)

You need to ensure that the audit logs from the SQLdb1 Azure SQL database are 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 SQL in the search box, select SQL databases from the search results then select SQLdb1. Alternatively, browse to SQL databases in the left navigation pane.

* 2. In the properties of SQLdb1, scroll down to the Security section and select Auditing.

* 3. Turn auditing on if it isn't already, tick the Log Analytics checkbox then click on Configure.

Auditing ⓘ

☒ ON ☐ OFF

Audit log destination (choose at least one):

☐ Storage

☒ Log Analytics (Preview)

Log Analytics details

Configure

☐ Event Hub (Preview)

* 4. Select the WS11641655 Azure Log Analytics workspace.

* 5. Click Save to save the changes.

NEW QUESTION 70

- (Exam Topic 4)

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has an Active Directory forest with a single domain, named weylaindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.

You have been tasked with integrating Active Directory and the Azure AD tenant. You intend to deploy Azure AD Connect.

Your strategy for the integration must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.

Solution: You recommend the use of federation with Active Directory Federation Services (AD FS). Does the solution meet the goal?

A. Yes

B. No

Answer: B

Explanation:

A federated authentication system relies on an external trusted system to authenticate users. Some companies want to reuse their existing federated system investment with their Azure AD hybrid identity solution. The maintenance and management of the federated system falls outside the control of Azure AD. It's up to the organization by using the federated system to make sure it's deployed securely and can handle the authentication load.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta>

NEW QUESTION 71

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.

You need to ensure that User1 can create and manage administrative units. The solution must use the principle of least privilege.

Which role should you assign to User1?

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

Answer: A

NEW QUESTION 76

- (Exam Topic 4)

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

Name	Days to retain deleted vaults	Purge protection	Permission model
KeyVault1	10	Enabled	Azure role-based access control (Azure RBAC)
KeyVault2	15	Disabled	Azure role-based access control (Azure RBAC)

The subscription contains the users shown in the following table.

Name	Role	Assigned to
Admin1	Key Vault Contributor	KeyVault1
Admin2	Key Vault Secrets Officer	KeyVault2
Admin3	Key Vault Administrator	KeyVault1

On June 1, you perform the following actions:

- Delete a key named key1 from KeyVault1.
- Delete a secret named secret 1 from KeyVault2.

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

Statements	Yes	No
Admin1 can recover key1 on June 5.	<input type="radio"/>	<input type="radio"/>
Admin2 can purge secret1 on June 12.	<input type="radio"/>	<input type="radio"/>
Admin3 can recover key1 on June 17.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Yes Yes No

NEW QUESTION 81

- (Exam Topic 4)

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

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

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

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

You need to configure auditing for SQL1.

Which storage accounts and Log Analytics workspaces can you use as the audit log destination? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Storage accounts that can be used as the audit log destination:

Storage1 only

Storage2 only

Storage1 and Storage2 only

Storage1, Storage2, and Storage3

Log Analytics workspaces that can be used as the audit log destination:

Analytics1 only

Analytics1 and Analytics2 only

Analytics1 and Analytics3 only

Analytics1, Analytics2, and Analytics3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Answer Area

Storage accounts that can be used as the audit log destination:

Storage1 only

Storage2 only

Storage1 and Storage2 only

Storage1, Storage2, and Storage3

Log Analytics workspaces that can be used as the audit log destination:

Analytics1 only

Analytics1 and Analytics2 only

Analytics1 and Analytics3 only

Analytics1, Analytics2, and Analytics3

NEW QUESTION 85

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

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

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

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

- 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 87

- (Exam Topic 4)

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

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

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

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

Solution: You deploy an Azure AD Application Proxy. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.

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

- Create Azure Virtual Network.
- Create a custom DNS server in the Azure Virtual Network.
- Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.
- Configure forwarding between the custom DNS server and your on-premises DNS server.

Reference:

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

NEW QUESTION 92

- (Exam Topic 4)

You have an Azure subscription that contains a storage account named storage1 and several virtual machines. The storage account and virtual machines are in the same Azure region. The network configurations of the virtual machines are shown in the following table.

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

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

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

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

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

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
VM1 can connect to storage1.	<input type="radio"/>	<input type="radio"/>
VM2 can connect to storage1.	<input type="radio"/>	<input type="radio"/>
VM3 can connect to storage1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: No

VNet1 has a service endpoint configure for Azure Storage. However, the Azure storage does not allow access from VNet1 or the public IP address of VM1.

Box 2: Yes

VNet2 does not have a service endpoint configured. However, the Azure storage allows access from the public IP address of VM2.

Box 3: No

Azure storage allows access from VNet3. However, VNet3 does not have a service endpoint for Azure storage. The Azure storage also does not allow access from the public IP of VM3.

NEW QUESTION 93

- (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

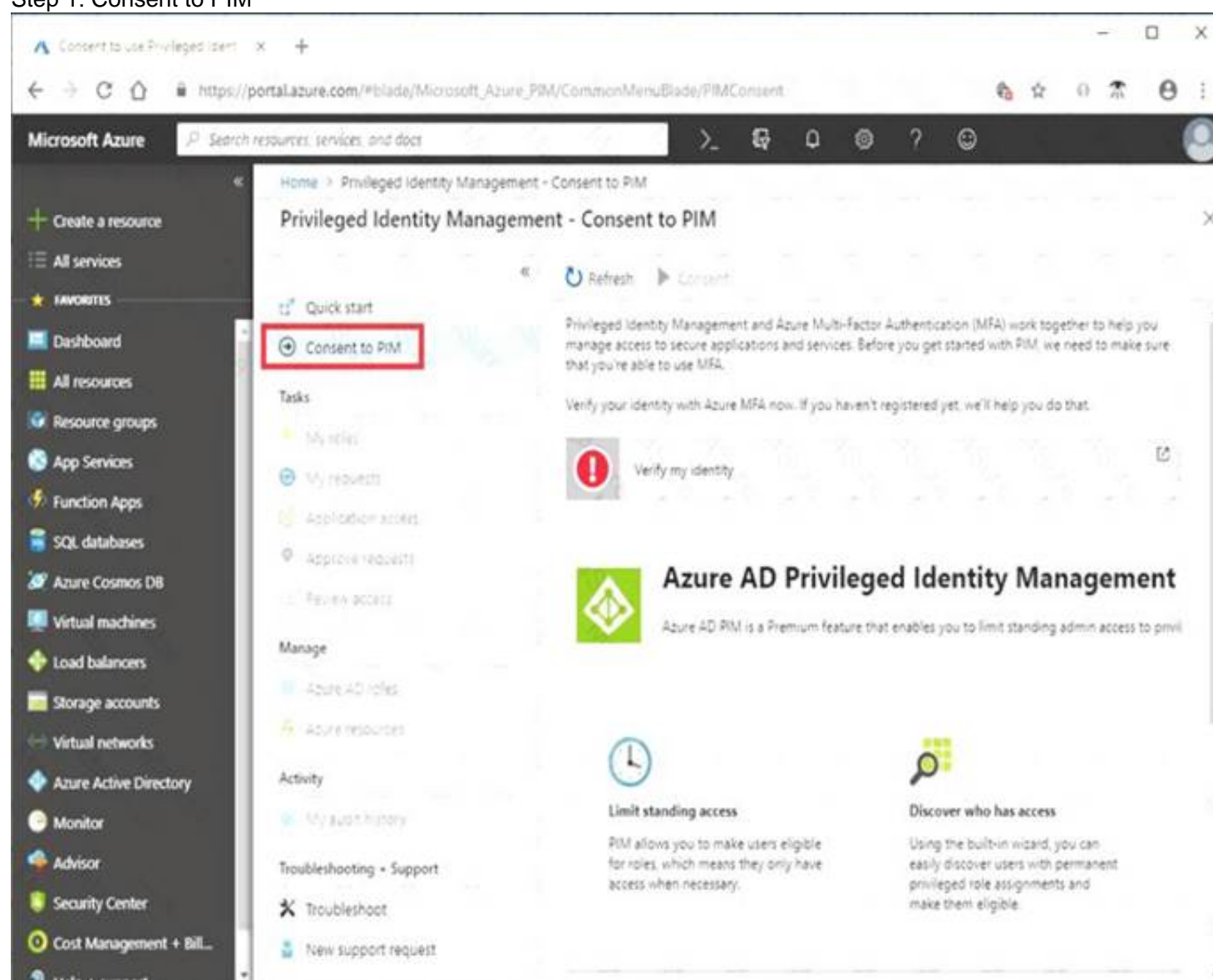


- A. Mastered
 B. Not Mastered

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 94

- (Exam Topic 4)

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

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

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

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

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

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

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

Answer Area

Statements	Yes	No
User1 can set Purge protection to Enable for Vault1.	<input type="radio"/>	<input type="radio"/>
User2 can configure firewalls and virtual networks for Vault1.	<input type="radio"/>	<input type="radio"/>
User3 can add access policies to Vault1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can set Purge protection to Enable for Vault1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can configure firewalls and virtual networks for Vault1.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can add access policies to Vault1.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 95

- (Exam Topic 4)

You have an Azure subscription that contains an Azure key vault named KeyVault1 and the virtual machines shown in the following table.

Name	Private IP address	Public IP address	Connected to
VM1	10.7.0.4	51.144.245.152	VNET1/Default
VM2	10.8.0.4	104.45.9.227	VNET2/Default

You set the Key Vault access policy to Enable access to Azure Disk Encryption for volume encryption. KeyVault1 is configured as shown in the following exhibit.

Save Discard

Allow access from:

☐ All networks ☒ Selected networks

Configure network access control for your key vault. [Learn More](#)

Virtual networks:

+ Add existing virtual networks

+ Add new virtual network

VIRTUAL NETWORK	SUBNET	RESOURCE GROUP	SUBSCRIPTION
VNET1	default	RG1	...

Firewall:

IPv4 ADDRESS OR CIDR

IPv4 address or CIDR ...

Exception:

Allow trusted Microsoft services to bypass this firewall?

☒ Yes ☐ No

This setting is related to firewall only. In order to access this key vault, the trusted service must also be given explicit permissions in the Access policies section.

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

Statements	Yes	No
From VM1, users can manage the keys and secrets stored in KeyVault1.	<input type="radio"/>	<input type="radio"/>
From VM2, users can manage the keys and secrets stored in KeyVault1.	<input type="radio"/>	<input type="radio"/>
VM2 can use KeyVault for Azure Disk Encryption	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
From VM1, users can manage the keys and secrets stored in KeyVault1.	<input checked="" type="radio"/>	<input type="radio"/>
From VM2, users can manage the keys and secrets stored in KeyVault1.	<input checked="" type="radio"/>	<input type="radio"/>
VM2 can use KeyVault for Azure Disk Encryption	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 96

- (Exam Topic 4)

You have an Azure subscription that contains a resource group named RG1 and the network security groups (NSGs) shown in the following table.

Name	Location	Flow logs status
NSG1	West Europe	Off
NSG2	West Europe	Off

You create the Azure policy shown in the following exhibit.

Basics	Parameters	Remediation	Non-compliance messages	Review + create
Basics				
Scope			Azure Pass - Sponsorship/RG1	
Exclusions			Azure Pass - Sponsorship/RG1/NSG1	
Policy definition			Flow logs should be enabled for every network security group	
Assignment name			Flow logs should be enabled for every network security group	
Description			Description1	
Policy enforcement			Enabled	
Assigned by			Admin1	
Parameters				
effect			Audit	
Remediation				
Create managed identity			Yes	
Managed identity location			westeurope	
Create a remediation task			No	
Non-compliance messages				
Default non-compliance message			Message1	

You assign the policy to RG1.
What will occur if you assign the policy to NSG1 and NSG2?

- A. Flow logs will be enabled for NSG1 and NSG2.
- B. Flow logs will be enabled for NSG2 only.
- C. Flow logs will be disabled for NSG1 and NSG2.
- D. Flow logs will be enabled for NSG1 only.

Answer: B

NEW QUESTION 100

- (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 10 on-premises servers that run Windows Server 2019.

You plan to implement Azure Security Center vulnerability scanning for the servers. What should you install on the servers first?

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 104

- (Exam Topic 4)

Your 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 109

- (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 112

- (Exam Topic 4)

You have a hybrid configuration of Azure Active Directory (Azure AD). You have an Azure SQL Database instance that is configured to support Azure AD authentication.

Database developers must connect to the database instance and authenticate by using their on-premises Active Directory account.

You need to ensure that developers can connect to the instance by using Microsoft SQL Server Management Studio. The solution must minimize authentication prompts.

Which authentication method should you recommend?

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

Answer: D

Explanation:

References:

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

NEW QUESTION 114

- (Exam Topic 4)

You have two Azure virtual machines in the East US2 region as shown in the following table.

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

You deploy and configure an Azure Key vault.

You need to ensure that you can enable Azure Disk Encryption on VM1 and VM2.

What should you modify on each virtual machine? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

VM1: ▼

☐ The operating system version
 ☐ The tier
 ☐ The type

VM2: ▼

☐ The operating system version
 ☐ The tier
 ☐ The type

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

VM1: The Tier

The Tier needs to be upgraded to standard.

Disk Encryption for Windows and Linux IaaS VMs is in General Availability in all Azure public regions and Azure Government regions for Standard VMs and VMs with Azure Premium Storage.

VM2: the operating system

References:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/generation-2#generation-1-vs-generation-2-ca>

NEW QUESTION 115

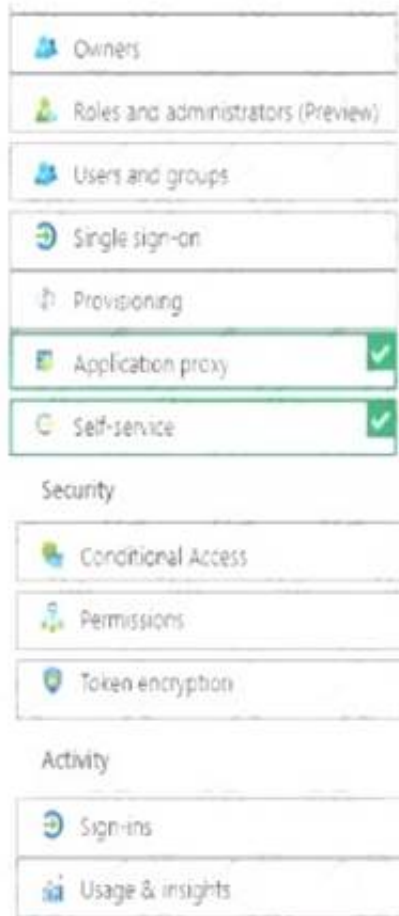
- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that contains two users named User1 and User2 and a registered app named App1.

You create an app-specific role named Role1.

You need to assign Role1 to User1 and enable User2 to request access to App1.

Which two settings should you modify? To answer select the appropriate settings in the answer area NOTE: Each correct selection is worth one pant.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application Description automatically generated

NEW QUESTION 120

- (Exam Topic 4)

You are configuring an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry.

You need to use the auto-generated service principal to authenticate to the Azure Container Registry. What should you create?

- A. an Azure Active Directory (Azure AD) group
- B. an Azure Active Directory (Azure AD) role assignment
- C. an Azure Active Directory (Azure AD) user
- D. a secret in Azure Key Vault

Answer: B

Explanation:

When you create an AKS cluster, Azure also creates a service principal to support cluster operability with other Azure resources. You can use this auto-generated service principal for authentication with an ACR registry. To do so, you need to create an Azure AD role assignment that grants the cluster's service principal access to the container registry.

References:

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

NEW QUESTION 121

- (Exam Topic 4)

You have an Azure subscription named Sub1.

In Azure Security Center, you have a security playbook named Play1. Play1 is configured to send an email message to a user named User1.

You need to modify Play1 to send email messages to a distribution group named Alerts. What should you use to modify Play1?

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

Answer: D

Explanation:

You can change an existing playbook in Security Center to add an action, or conditions. To do that you just need to click on the name of the playbook that you want to change, in the Playbooks tab, and Logic App Designer opens up.

References:

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

NEW QUESTION 126

- (Exam Topic 4)

You have an Azure Storage account named storage1 that has a container named container1. You need to prevent the blobs in container1 from being modified.

What should you do?

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

Answer: B

Explanation:

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

NEW QUESTION 128

- (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 129

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

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 133

- (Exam Topic 3)

You need to perform the planned changes for OU2 and User1.

Which tools should you use? To answer, drag the appropriate tools to the correct resources. Each tool may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Tools	Answer Area
The Azure portal	OU2: Tool
Azure AD Connect	User1: Tool
The Active Directory admin center	
Active Directory Sites and Services	
Active Directory Users and Computers	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Table Description automatically generated

NEW QUESTION 136

- (Exam Topic 3)

You need to meet the technical requirements for the finance department users. Which CAPolicy1 settings should you modify?

- A. Cloud apps or actions
- B. Conditions
- C. Grant
- D. Session

Answer: D

Explanation:

Reference:

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

NEW QUESTION 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:	<div><div></div><div>0</div><div>1</div><div>2</div><div>3</div></div>
Workspaces:	<div><div></div><div>0</div><div>1</div><div>2</div><div>3</div></div>

- 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 140

- (Exam Topic 2)

You are evaluating the security of VM1, VM2, and VM3 in Sub2.

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

Answer Area

Statements	Yes	No
From the Internet, you can connect to the web server on VM1 by using HTTP.	<input type="radio"/>	<input type="radio"/>
From the Internet, you can connect to the web server on VM2 by using HTTP.	<input type="radio"/>	<input type="radio"/>
From the Internet, you can connect to the web server on VM3 by using HTTP.	<input type="radio"/>	<input type="radio"/>

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
From the Internet, you can connect to the web server on VM1 by using HTTP.	<input checked="" type="radio"/>	<input type="radio"/>
From the Internet, you can connect to the web server on VM2 by using HTTP.	<input type="radio"/>	<input checked="" type="radio"/>
From the Internet, you can connect to the web server on VM3 by using HTTP.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 141

- (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 144

- (Exam Topic 1)
You need to configure SQLDB1 to meet the data and application requirements.
Which three actions should you recommend be performed in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

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

In SQLDB1, create contained database users.

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

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

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

Answer Area

<

>

↑

↓

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
From the Azure portal, create an Azure AD administrator for LitwareSQLServer1 Connect to SQLDB1 by using SSMS
In SQLDB1, create contained database users <https://www.youtube.com/watch?v=pEPyPsGEevw>

NEW QUESTION 147

- (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 152

- (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.

Passing Certification Exams Made Easy

visit - <https://www.2PassEasy.com>

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 154

- (Exam Topic 1)

You need to ensure that you can meet the security operations requirements. What should you do first?

- A. Turn on Auto Provisioning in Security Center.
 B. Integrate Security Center and Microsoft Cloud App Security.
 C. Upgrade the pricing tier of Security Center to Standard.
 D. Modify the Security Center workspace configuration.

Answer: C

Explanation:

The Standard tier extends the capabilities of the Free tier to workloads running in private and other public clouds, providing unified security management and threat protection across your hybrid cloud workloads. The Standard tier also adds advanced threat detection capabilities, which uses built-in behavioral analytics and machine learning to identify attacks and zero-day exploits, access and application controls to reduce exposure to network attacks and malware, and more.

Scenario: Security Operations Requirements

Litware must be able to customize the operating system security configurations in Azure Security Center.

References:

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

NEW QUESTION 156

- (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 158

- (Exam Topic 4)

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

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

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

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

Solution: You create a policy initiative and assignments that are scoped to resource groups. Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Instead use a management group.

Management groups in Microsoft Azure solve the problem of needing to impose governance policy on more than one Azure subscription simultaneously.

Reference:

<https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-managementgroups>

NEW QUESTION 161

- (Exam Topic 4)

You have an Azure Storage account that contains a blob container named container1 and a client application named App1.

You need to enable App1 access to container1 by using Azure Active Directory (Azure AD) authentication.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

From Azure AD:

	▼
Register App1.	
Create an access package.	
Implement an application proxy.	
Modify the authentication methods.	

From the storage account:

	▼
Add a private endpoint.	
Regenerate the access key.	
Configure Access control (IAM).	
Generate a shared access signature (SAS).	

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Reference:

<https://azure.microsoft.com/en-in/blog/announcing-the-preview-of-aad-authentication-for-storage/> <https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/storage/common/storage-auth-aad-rbac-portal>

NEW QUESTION 165

- (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 170

- (Exam Topic 4)

You need to ensure that connections through an Azure Application Gateway named Homepage-AGW are inspected for malicious requests. To complete this task, sign in to the Azure portal. You do not need to wait for the task to complete.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

You need to enable the Web Application Firewall on the Application Gateway.

In the Azure portal, type Application gateways in the search box, select Application gateways from the search results then select the gateway named Homepage-AGW. Alternatively, browse to Application Gateways in the left navigation pane.

In the properties of the application gateway, click on Web application firewall. For the Tier setting, select WAF V2.

In the Firewall status section, click the slider to switch to Enabled. In the Firewall mode section, click the slider to switch to Prevention. Click Save to save the changes.

NEW QUESTION 173

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant. The tenant contains users that are assigned Azure AD Premium Plan 2 licenses.

You have an partner company that has a domain named The fabrikam.com domain contains a user named user'. User' has an email address of userl@fabrikam.com.

You to provide User1 with to the resources in the tenant The solution must meet the following requirements: ➤ user1 must be able to sign in by using the userl@fabrikam.com credentials

- You must be able to grant User1 access to the resources in the tenant
- Administrative effort must be minimized.

What should you do?

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

Answer: B

NEW QUESTION 176

- (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/azurerm.keyvault/set-azurekeyvaultsecretattribute

NEW QUESTION 180

- (Exam Topic 4)

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

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

Azure AD Privileged Identity Management (PIM) is enabled for the tenant. In PIM, the Password Administrator role has the following settings:

- > Maximum activation duration (hours): 2
- > Send email notifying admins of activation: Disable
- > Require incident/request ticket number during activation: Disable
- > Require Azure Multi-Factor Authentication for activation: Enable
- > Require approval to activate this role: Enable
- > Selected approver: Group1

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

Name	Assignment type
User1	Active
User2	Eligible
user3	Eligible

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

Statements	Yes	No
When User1 signs in, the user is assigned the Password Administrator role automatically.	<input type="radio"/>	<input type="radio"/>
User2 can request to activate the Password Administrator role.	<input type="radio"/>	<input type="radio"/>
If User3 wants to activate the Password Administrator role, the user can approve their own request.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

YES (Already active)

YES (The user will be prompted for MFA regardless the MFA Status of the user) NO (Even the user is included in the group, a user can't approve itself)

https://docs.microsoft.com/es-es/azure/active-directory/privileged-identity-management/pim-deployment-plan (Require approval section)

NEW QUESTION 184

- (Exam Topic 4)

You create a new Azure subscription that is associated to a new Azure Active Directory (Azure AD) tenant. You create one active conditional access policy named Portal Policy. Portal Policy is used to provide access to the Microsoft Azure Management cloud app.

The Conditions settings for Portal Policy are configured as shown in the Conditions exhibit. (Click the Conditions tab.)

Portal Policy [X]

Info [i] Delete [X]

Name: Portal Policy

Assignments

Users and groups [i]
All users

Cloud apps [i]
1 app included

Conditions [i]
1 condition selected

Access controls

Grant [i]
2 controls selected

Session [i]
0 controls selected

Conditions [X]

Info [i]

Device platforms [i]
Not configured

Locations [i]
1 included

Client apps (preview) [i]
Not configured

Device state (preview) [i]
Not configured

Locations [X]

Control user access based on their physical location. [Learn more](#)

Configure [i]
Yes No

Include Exclude

☐ Any location
☐ All trusted locations
☒ Selected locations

Select
Contoso

Contoso ...

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

Portal Policy [X]

Info [i] Delete [X]

Name: Portal Policy

Assignments

Users and groups [i]
All users

Cloud apps [i]
1 app included

Conditions [i]
1 condition selected

Access controls

Grant [i]
2 controls selected

Session [i]
0 controls selected

Grant [X]

Select the controls to be enforced.

☐ Block access
☒ Grant access

☒ Require multi-factor authentication [i]
☐ Require device to be marked as compliant [i]
☐ Require Hybrid Azure AD joined device [i]
☒ Require approved client app [i]
[See list of approved client apps](#)

For multiple controls
☐ Require all the selected controls
☒ Require one of the selected controls

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

Statements	Yes	No
Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	<input type="radio"/>	<input type="radio"/>
Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription.	<input type="radio"/>	<input type="radio"/>
Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 186

- (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 188

- (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 193

- (Exam Topic 4)

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

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

An IP address of 10.1.0.4 is assigned to VM5. VM5 does not have a public IP address. VM5 has just in time (JIT) VM access configured as shown in the following exhibit.

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 198

- (Exam Topic 4)

You have an Azure environment.

You need to identify any Azure configurations and workloads that are non-compliant with ISO 27001 standards. What should you use?

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

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-compliance-dashboard>

NEW QUESTION 200

- (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.

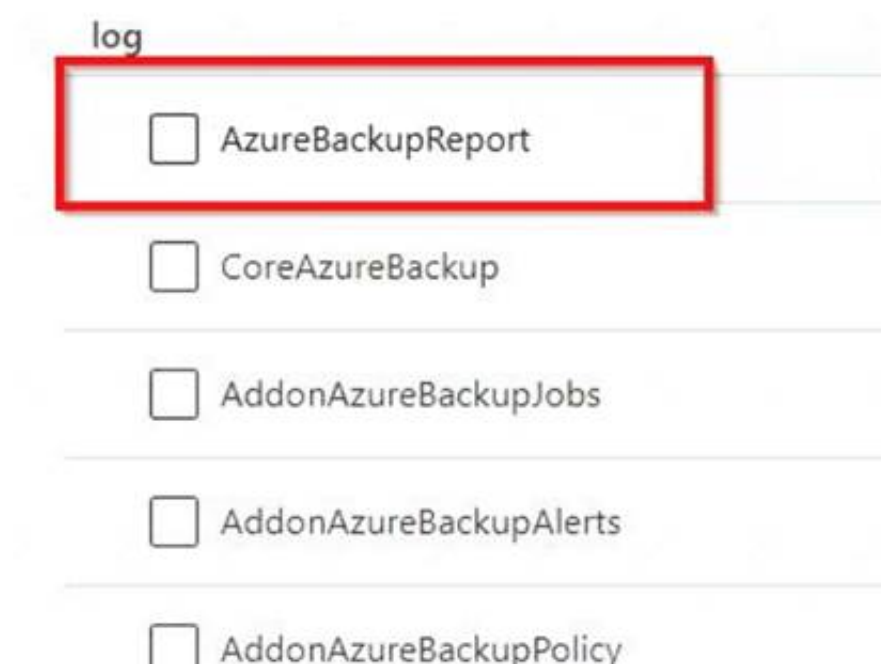
* 2. In the properties of Vault1, scroll down to the Monitoring section and select Diagnostic Settings.

* 3. Click the Add a diagnostic setting link.

* 4. Enter a name in the Diagnostic settings name box.

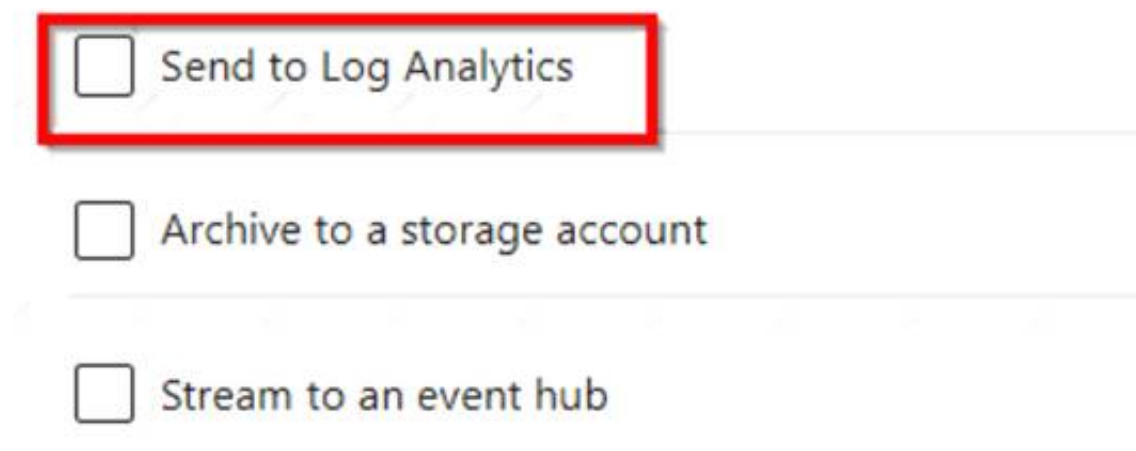
* 5. In the Log section, select AzureBackupReport.

Category details



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

Destination details



* 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 204

- (Exam Topic 4)

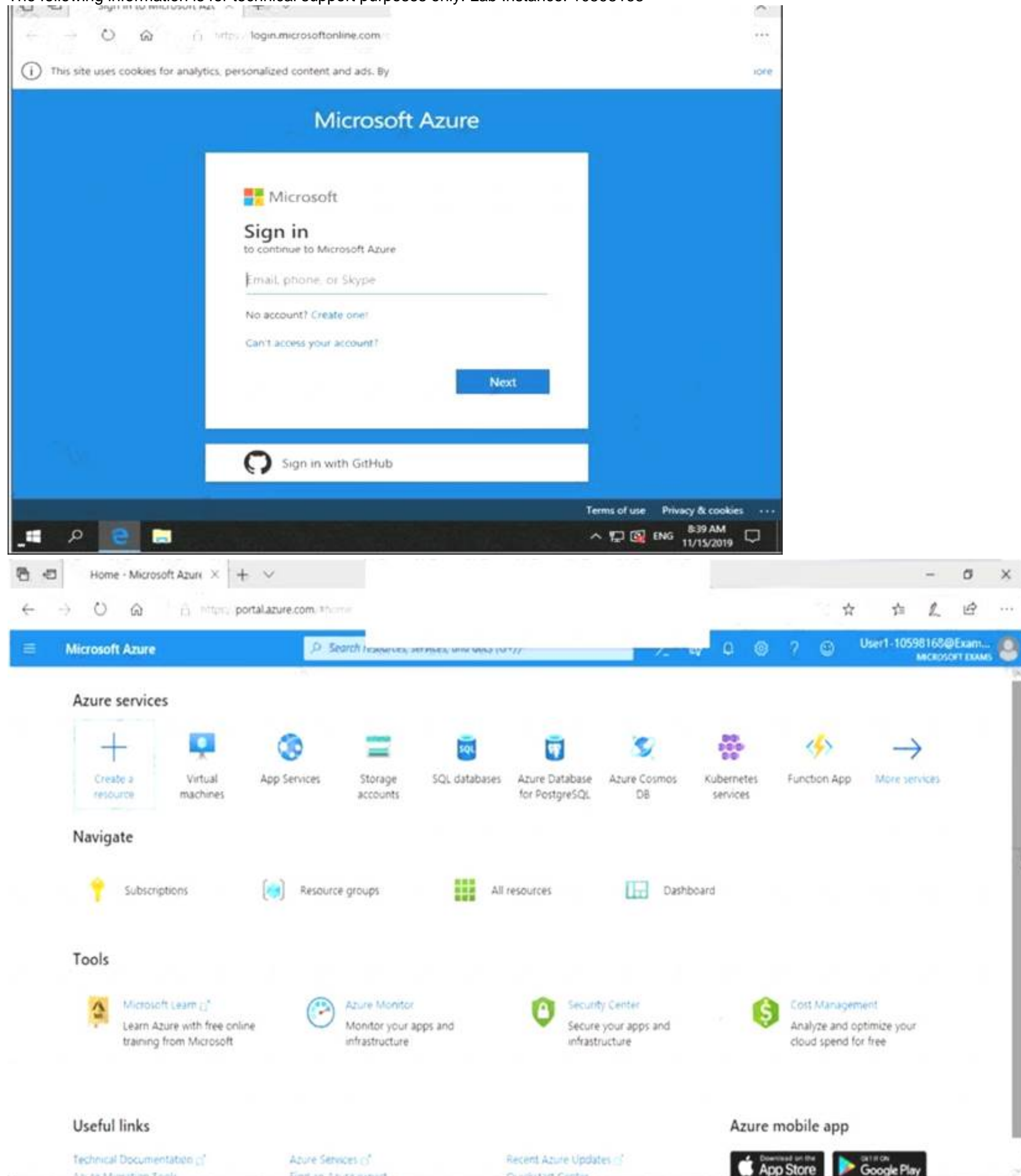
Use the following login credentials as needed:

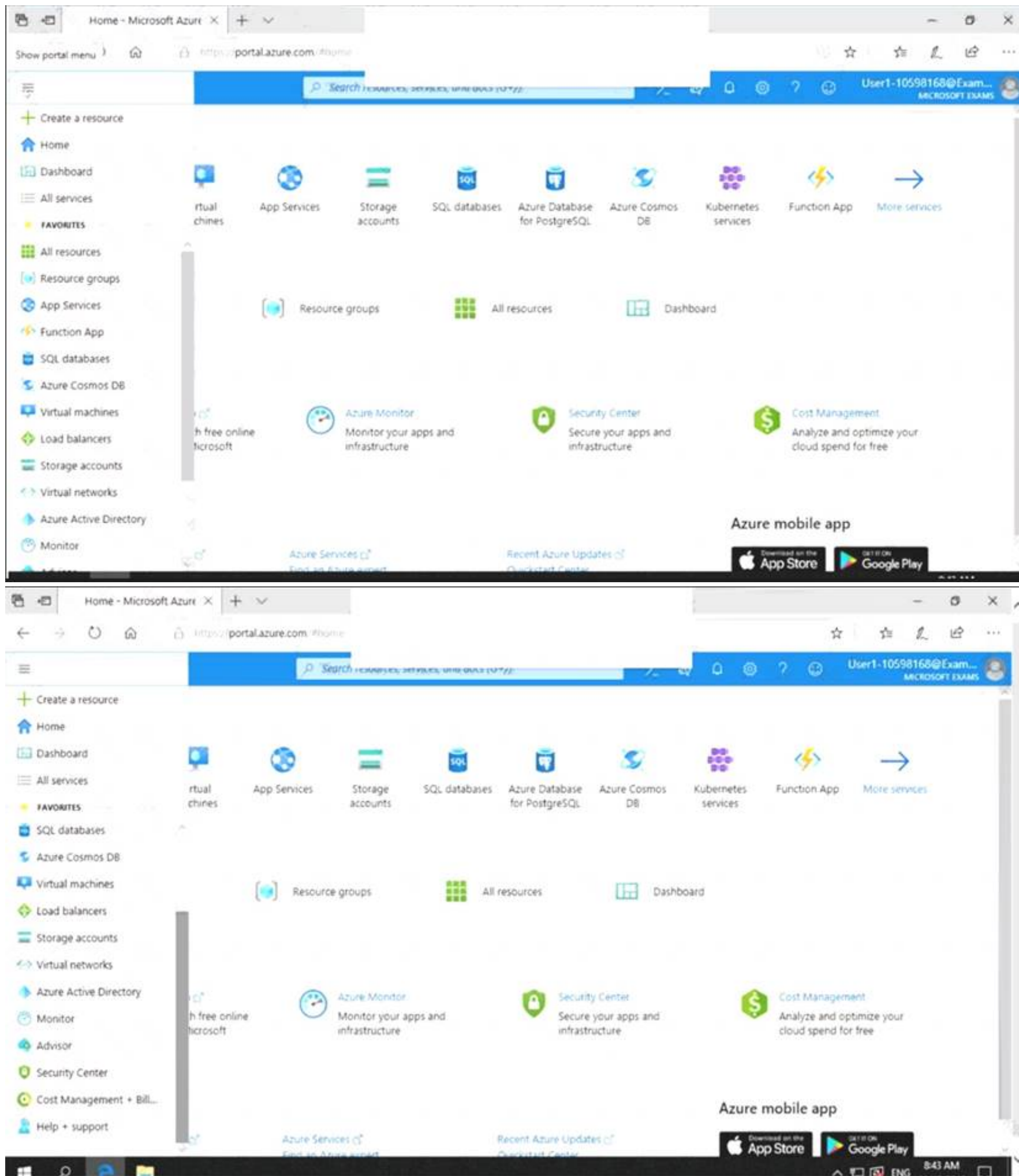
To enter your username, place your cursor in the Sign in box and click on the username below.

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 207

- (Exam Topic 4)

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

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

You have an Azure Subscription. The subscription contains 50 virtual machines that run Windows Server 2012 R2 or Windows Server 2016.

You need to deploy Microsoft Antimalware to the virtual machines. Solution: You connect to each virtual machine and add a Windows feature. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Microsoft Antimalware is deployed as an extension and not a feature. References:

<https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware>

NEW QUESTION 208

- (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 210

- (Exam Topic 4)

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

Name	Role
Admin1	Global administrator
Admin2	Group administrator
Admin3	User administrator

Contoso.com contains a group naming policy. The policy has a custom blocked word list rule that includes the word Contoso.

Which users can create a group named Contoso Sales in contoso.com? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Users who can create a security group named Contoso Sales:

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

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-naming-policy>

NEW QUESTION 212

- (Exam Topic 4)

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

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

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

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

Solution: You create an initiative and an assignment that is scoped to the Tenant Root Group management group.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/overview>

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

NEW QUESTION 214

- (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 217

- (Exam Topic 4)

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

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

You have an Azure Subscription named Sub1.

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

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

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

Solution: You generate new SASs. Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Instead you should create a new stored access policy.

To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access

policy. Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it.

References:

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

NEW QUESTION 219

- (Exam Topic 4)

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

Name	Pattern	Case sensitivity
Condition1	White	On
Condition2	Black	Off

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

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

You need to identify how Azure Information Protection will label files.

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

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

▼

No label

Label1 only

Label2 only

Label1 and Label2

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

▼

No label

Label1 only

Label2 only

Label1 and Label2

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Box 1: Label 2 only

How multiple conditions are evaluated when they apply to more than one label

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

➤ The most sensitive label is applied.

➤ The last sublabel is applied.

Box 2: No Label

Automatic classification applies to Word, Excel, and PowerPoint when documents are saved, and apply to Outlook when emails are sent. Automatic classification does not apply to Microsoft Notepad.

References:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification>

NEW QUESTION 222

- (Exam Topic 4)

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

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

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

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

NOTE: Each correct selection is worth one point.

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 223

- (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 226

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that contains two administrative units named AU1 and AU2.

Users are assigned to the administrative units as shown in the following table.

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

Answer Area

Statements	Yes	No
Admin1 can reset the password of User1.	<input type="radio"/>	<input type="radio"/>
Admin2 can reset the password of User3.	<input type="radio"/>	<input type="radio"/>
Admin3 can reset the password of Admin4.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Admin1 can reset the password of User1.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can reset the password of User3.	<input checked="" type="radio"/>	<input type="radio"/>
Admin3 can reset the password of Admin4.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 227

- (Exam Topic 4)

You have been tasked with applying conditional access policies for your company's current Azure Active Directory (Azure AD). The process involves assessing the risk events and risk levels.

Which of the following is the risk level that should be configured for users that have leaked credentials?

- A. None
 B. Low
 C. Medium
 D. High

Answer: D

Explanation:

These six types of events are categorized in to 3 levels of risks – High, Medium & Low: Table Description automatically generated

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

Reference:

<http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/>

NEW QUESTION 232

- (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 237

- (Exam Topic 4)

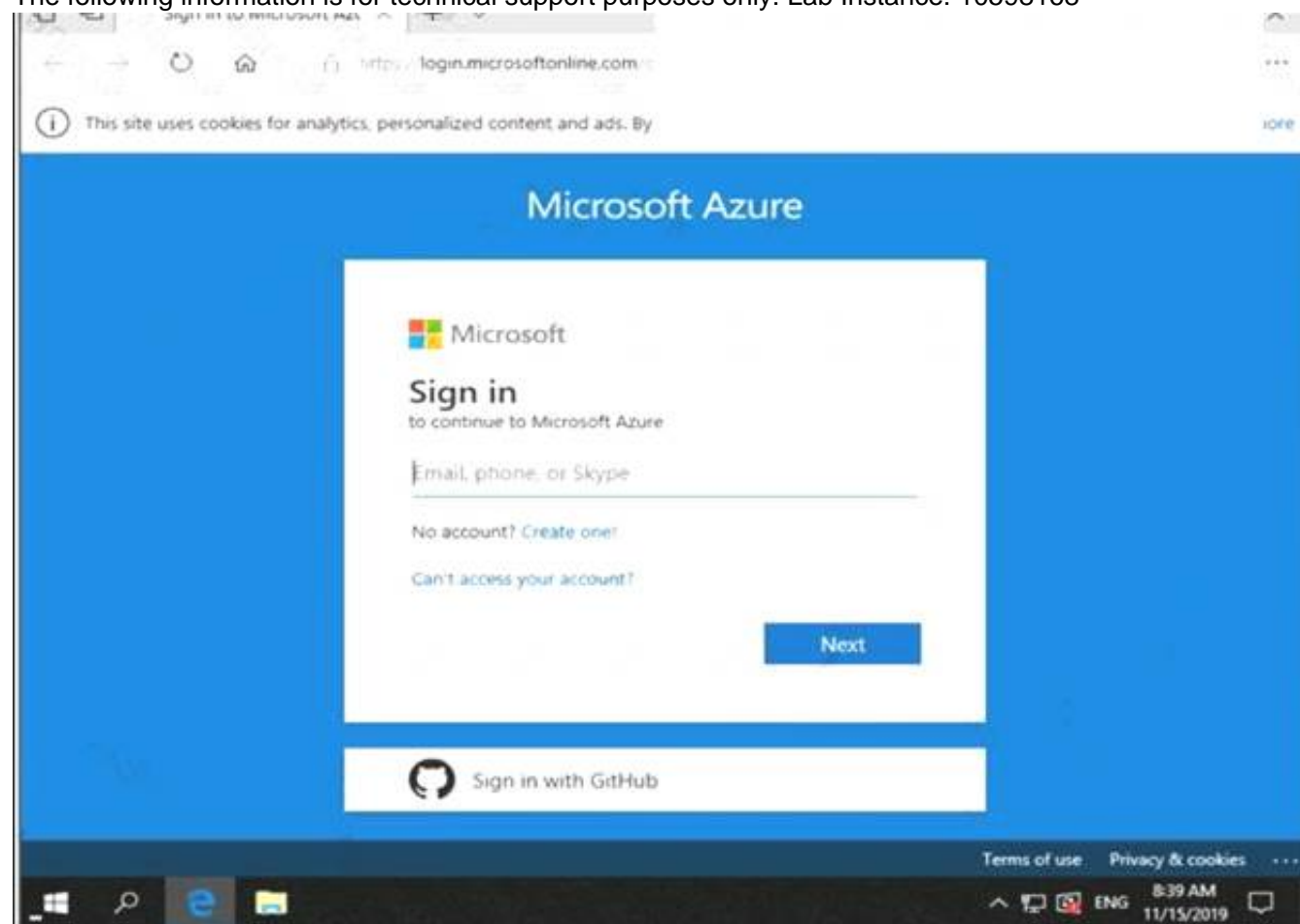
Use the following login credentials as needed:

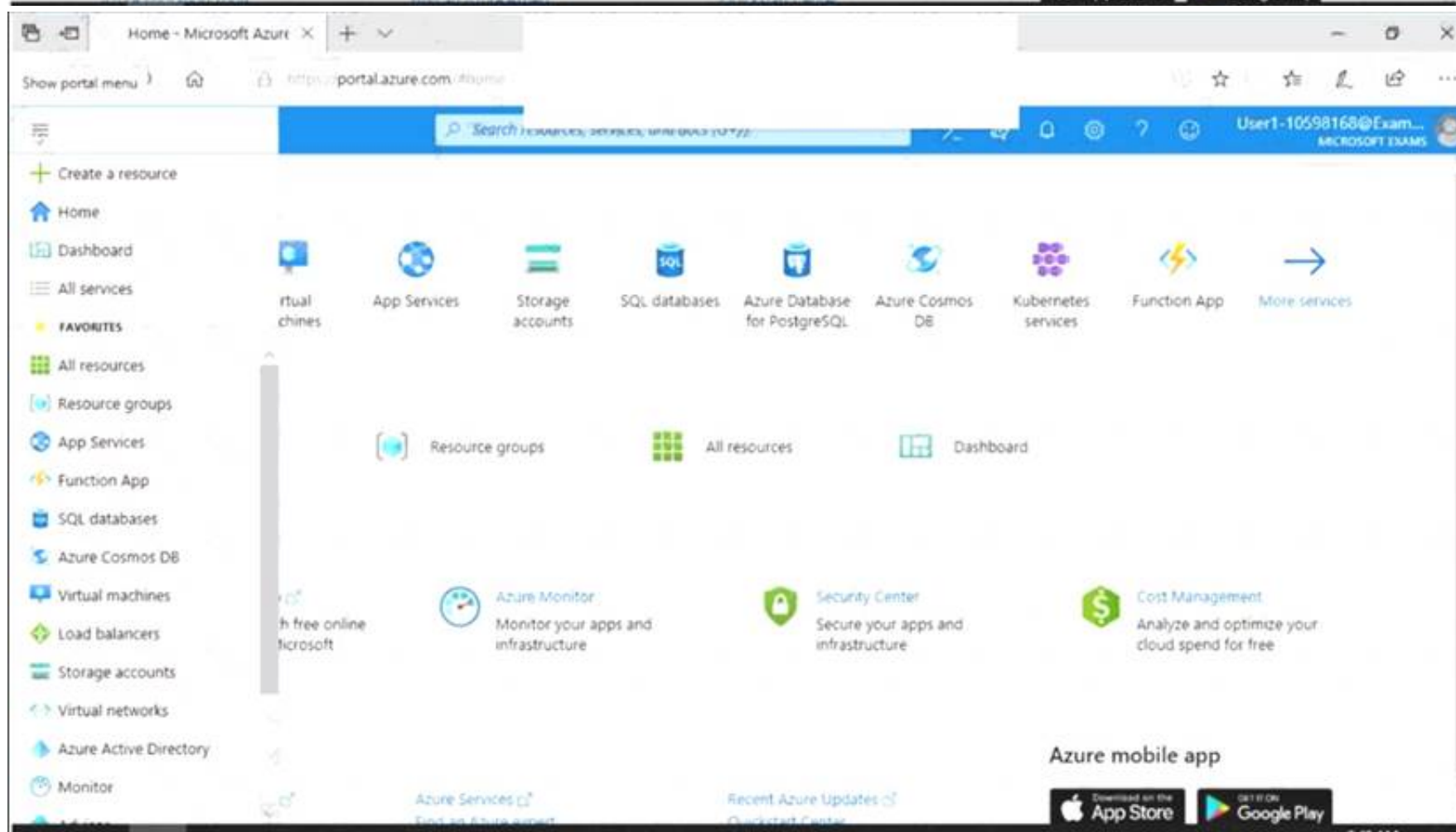
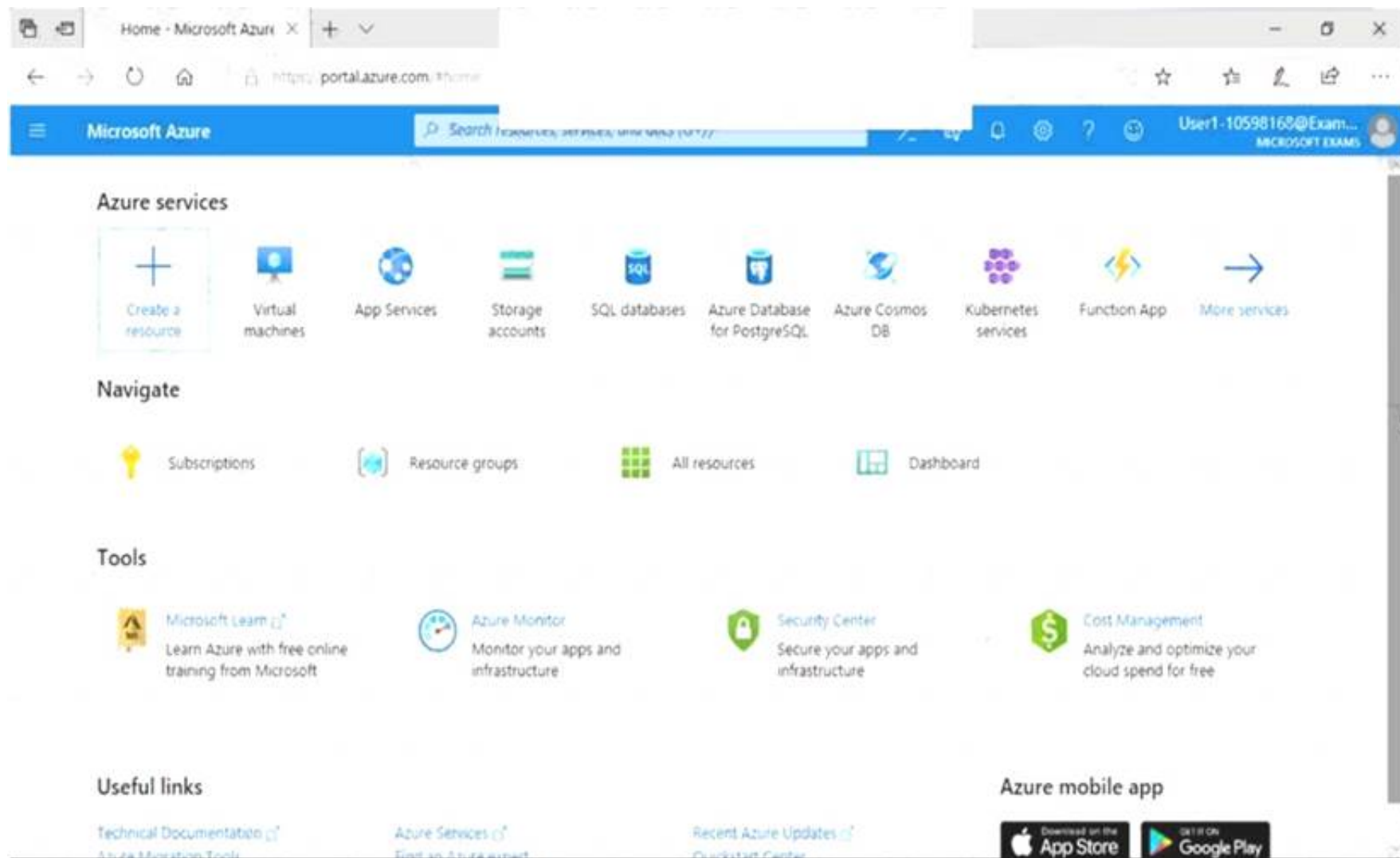
To enter your username, place your cursor in the Sign in box and click on the username below.

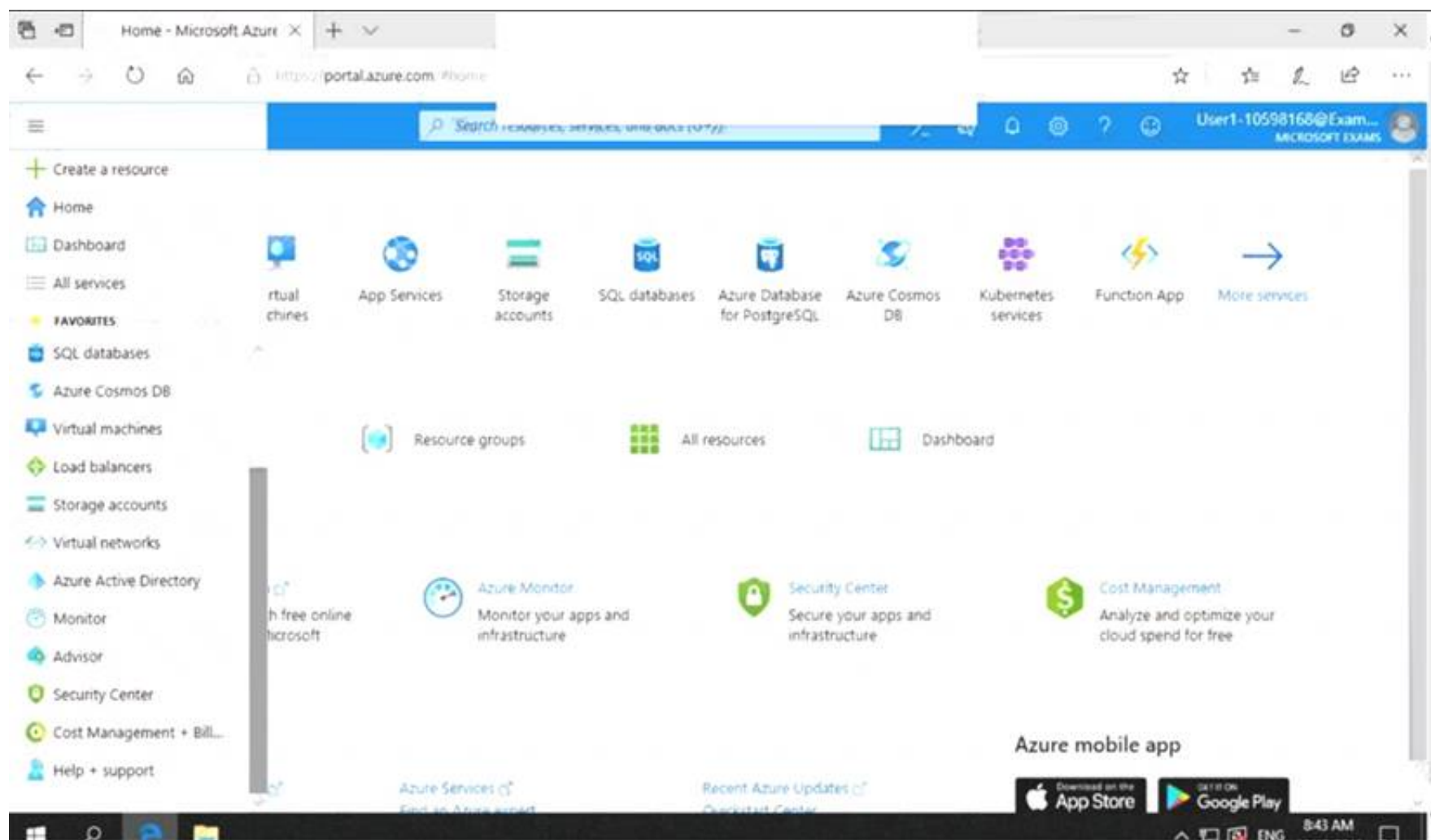
To enter your password, place your cursor in the Enter password box and click on the password below. Azure Username: User1-10598168@ExamUsers.com

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 238

- (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:

A Windows server and a Windows Event Forwarding subscription

Forward events to Microsoft Sentinel by using:

An Azure Log Analytics agent

NEW QUESTION 243

- (Exam Topic 4)

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

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

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

- * Create two application security groups named ASG1 and ASG2 in the West US region.
- * Add the network interface of VM1 to ASG1.

Answer Area

ASG1:

ASG2:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

ASG1:

VM2, VM3, and VM4 only

ASG2:

VM1, VM2, and VM4 only

NEW QUESTION 245

- (Exam Topic 4)

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

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

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

Role settings

Assignment

☐ Allow permanent eligible assignment

Expire eligible assignments after

3 Months

☐ Allow permanent active assignment

Expire active assignments after

1 Month

☒ Require Multi-Factor Authentication on active assignment

☒ Require justification on active assignment

Activation

Activation maximum duration (hours)

8

☒ Require Multi-Factor Authentication on activation

☒ Require justification on activation

☐ Require ticket information on activation

☐ Require approval to activate

Select step in role

No member or group selected

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

Name	Assignment type
User1	Eligible
User2	Active
User3	Active

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

Statements	Yes	No
On May 15, 2019, User1 can activate the Contributor role.	<input type="radio"/>	<input type="radio"/>
On May 15, 2019, User2 can use the Contributor role.	<input type="radio"/>	<input type="radio"/>
On June 15, 2019, User3 can activate the Contributor role.	<input type="radio"/>	<input type="radio"/>

A. Mastered
B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 247

- (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?

Passing Certification Exams Made Easy

visit - https://www.2PassEasy.com

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

Answer: D

NEW QUESTION 248

- (Exam Topic 4)

You suspect that users are attempting to sign in to resources to which they have no access.

You need to create an Azure Log Analytics query to identify failed user sign-in attempts from the last three days. The results must only show users who had more than five failed sign-in attempts.

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

```
let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AccountType == 'User' and EventID == 4625

Summarize failed_login_attempts=
    Count(),
    latest_failed_login=arg_max(TimeGenerated by Account
| where failed_login_attempts > 5
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The following example identifies user accounts that failed to log in more than five times in the last day, and when they last attempted to log in.

```
let timeframe = 1d; SecurityEvent
| where TimeGenerated > ago(1d)
| where AccountType == 'User' and EventID == 4625 // 4625 - failed log in
| summarize failed_login_attempts=count(), latest_failed_login=arg_max(TimeGenerated, Account) by Account
| where failed_login_attempts > 5
| project-away Account1 References:
https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/examples
```

NEW QUESTION 249

- (Exam Topic 4)

You have an Azure Sentinel workspace that contains an Azure Active Directory (Azure AD) connector, an Azure Log Analytics query named Query1 and a playbook named Playbook1.

Query1 returns a subset of security events generated by Azure AD.

You plan to create an Azure Sentinel analytic rule based on Query1 that will trigger Playbook1. You need to ensure that you can add Playbook1 to the new rule.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Create the rule and set the type to:

Fusion
Microsoft Security incident creation
Scheduled

Configure the playbook to include:

A managed connector
A system-assigned managed identity
A trigger
Diagnostic settings

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom> <https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

NEW QUESTION 250

- (Exam Topic 4)

Your network contains an Active Directory forest named contoso.com. You have an Azure Directory (Azure AD) tenant named contoso.com.

You plan to configure synchronization by using the Express Settings installation option in Azure AD Connect. You need to identify which roles and groups are required to perform the planned configurations. The solution must use the principle of least privilege.

Which two roles and groups should you identify? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

Answer: CE

Explanation:

References:

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

NEW QUESTION 251

- (Exam Topic 4)

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

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

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

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

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

- A. Yes
- B. No

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/governance/policy/overview>

NEW QUESTION 254

- (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 256

- (Exam Topic 4)

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com.

The company is developing an application named App1. App1 will run as a service on server that runs Windows Server 2016. App1 will authenticate to contoso.com and access Microsoft Graph to read directory data.

You need to delegate the minimum required permissions to App1.

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

Actions

Grant permissions

Add a delegated permission.

Configure Azure AD Application Proxy.

Add an application permission.

Create an app registration.

Answer Area

⬅

➡

⬆

⬇

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Step 1: Create an app registration

First the application must be created/registered.

Step 2: Add an application permission

Application permissions are used by apps that run without a signed-in user present.

Step 3: Grant permissions

NEW QUESTION 261

- (Exam Topic 4)

You have a Azure subscription that contains an Azure Container Registry named Registry1. The subscription uses the Standard use tier of Azure Security Center.

You upload several container images to Register1.

You discover that vulnerability security scans were not performed

You need to ensured that the images are scanned for vulnerabilities when they are uploaded to Registry1. What should you do?

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

Answer: A

Explanation:

Reference:

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

NEW QUESTION 264

- (Exam Topic 4)

You have an Azure 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 266

- (Exam Topic 4)

You have 10 virtual machines on a single subnet that has a single network security group (NSG). You need to log the network traffic to an Azure Storage account.

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

- A. Install the Network Performance Monitor solution.
- B. Enable Azure Network Watcher.
- C. Enable diagnostic logging for the NSG.

- D. Enable NSG flow logs.
- E. Create an Azure Log Analytics workspace.

Answer: D

Explanation:

A network security group (NSG) enables you to filter inbound traffic to, and outbound traffic from, a virtual machine (VM). You can log network traffic that flows through an NSG with Network Watcher's NSG flow log capability. Steps include:

- Create a VM with a network security group
- Enable Network Watcher and register the Microsoft.Insights provider
- Enable a traffic flow log for an NSG, using Network Watcher's NSG flow log capability
- Download logged data
- View logged data Reference:

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

NEW QUESTION 268

- (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 273

- (Exam Topic 4)

You need to configure an access review. The review will be assigned to a new collection of reviews and reviewed by resource owners.

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

Actions

Create an access review program.

Set Reviewers to Selected users.

Create an access review audit.

Create an access review control.

Set Reviewers to Group owners.

Set Reviewers to Members.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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



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

NEW QUESTION 276

- (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 279

- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Subscription named Sub1. Sub1 contains an Azure virtual machine named VM1 that runs Windows Server 2016.
You need to encrypt VM1 disks by using Azure Disk Encryption.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
Configure secrets for the Azure key vault.	
Create an Azure key vault.	
Run Set-AzureRmStorageAccount.	
Configure access policies for the Azure key vault.	
Run Set-AzureRmVmDiskEncryptionExtension.	

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 281

- (Exam Topic 4)

You have an Azure Container Registry named ContReg1 that contains a container image named image1. You enable content trust for ContReg1. After content trust is enabled, you push two images to ContReg1 as shown in the following table.

Name	Details
image2	Image was pushed with client content trust enabled.
image3	Image was pushed with client content trust disabled.

Which images are trusted images?

- A. image1 and image2 only
 B. image2 only
 C. image1, image2, and image3

Answer: B

Explanation:

Azure Container Registry implements Docker's content trust model, enabling pushing and pulling of signed images.

To push a trusted image tag to your container registry, enable content trust and push the image with docker push.

To work with trusted images, both image publishers and consumers need to enable content trust for their Docker clients. As a publisher, you can sign the images you push to a content trust-enabled registry.

Reference:

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust>

NEW QUESTION 284

- (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 288

- (Exam Topic 4)

You need to ensure that User2-11641655 has all the key permissions for KeyVault11641655. To complete this task, sign in to the Azure portal and modify the Azure resources.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

You need to assign the user the Key Vault Secrets Officer role.

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

NEW QUESTION 290

- (Exam Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 291

- (Exam Topic 4)

You have an Azure subscription that contains the following resources:

- A virtual network named VNET1 that contains two subnets named Subnet1 and Subnet2.
- A virtual machine named VM1 that has only a private IP address and connects to Subnet1.

You need to ensure that Remote Desktop connections can be established to VM1 from the internet.

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

Actions	Answer Area
Configure a network security group (NSG).	
Create a network rule collection.	
Create a NAT rule collection.	
Create a new subnet.	
Deploy Azure Application Gateway.	
Deploy Azure Firewall.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions	Answer Area
Configure a network security group (NSG).	Create a new subnet.
Create a network rule collection.	Deploy Azure Firewall.
Create a NAT rule collection.	Create a NAT rule collection.
Create a new subnet.	
Deploy Azure Application Gateway.	
Deploy Azure Firewall.	

NEW QUESTION 293

- (Exam Topic 4)

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

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

You need to configure authorization access.

Which authorization types can you use for each storage account? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

storage1:

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

storage2:

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

storage3:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/authorize-data-access>

NEW QUESTION 294

- (Exam Topic 4)

You have multiple development teams that will create apps in Azure.

You plan to create a standard development environment that will be deployed for each team.

You need to recommend a solution that will enforce resource locks across the development environments and ensure that the locks are applied in a consistent manner.

What should you include in the recommendation?

- A. an Azure policy
- B. an Azure Resource Manager template
- C. a management group

D. an Azure blueprint

Answer: D

Explanation:

Reference:

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

NEW QUESTION 296

- (Exam Topic 4)

You have an Azure subscription named Sub1 that contains an Azure Storage account named Contosostorage1 and an Azure key vault named Contosokeyvault1.

You plan to create an Azure Automation runbook that will rotate the keys of Contosostorage1 and store them in Contosokeyvault1.

You need to implement prerequisites to ensure that you can implement the runbook.

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

Actions	Answer Area
Run Set-AzureRmKeyVaultAccessPolicy	
Create an Azure Automation account.	
Import PowerShell modules to the Azure Automation account.	
Create a user-assigned managed identity.	
Create a connection resource in the Azure Automation account.	

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Step 1: Create an Azure Automation account

Runbooks live within the Azure Automation account and can execute PowerShell scripts. Step 2: Import PowerShell modules to the Azure Automation account Under 'Assets' from the Azure Automation account Resources section select 'to add in Modules to the runbook. To execute key vault cmdlets in the runbook, we need to add AzureRM.profile and AzureRM.key vault.

Step 3: Create a connection resource in the Azure Automation account

You can use the sample code below, taken from the AzureAutomationTutorialScript example runbook, to authenticate using the Run As account to manage Resource Manager resources with your runbooks. The AzureRunAsConnection is a connection asset automatically created when we created 'run as accounts' above. This can be found under Assets -> Connections. After the authentication code, run the same code above to get all the keys from the vault.

```
$connectionName = "AzureRunAsConnection" try
{
# Get the connection "AzureRunAsConnection "
$servicePrincipalConnection=Get-AutomationConnection -Name $connectionName "Logging in to Azure..."
Add-AzureRmAccount `
-ServicePrincipal `
-TenantId $servicePrincipalConnection.TenantId `
-ApplicationId $servicePrincipalConnection.ApplicationId `
-CertificateThumbprint $servicePrincipalConnection.CertificateThumbprint
}
```

References:

<https://www.rahulpnath.com/blog/accessing-azure-key-vault-from-azure-runbook/>

NEW QUESTION 297

- (Exam Topic 4)

You have a web app named WebApp1.

You create a web application firewall (WAF) policy named WAF1. You need to protect WebApp1 by using WAF1.

What should you do first?

A. Deploy an Azure Front Door.

B. Add an extension to WebApp1.

C. Deploy Azure Firewall.

Answer: A

Explanation:

References:

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

NEW QUESTION 300

- (Exam Topic 4)

You have an Azure subscription named Sub1. Sub1 has an Azure Storage account named Storage1 that contains the resources shown in the following table.

Name	Type
Container1	Blob container
Share1	File share

You generate a shared access signature (SAS) to connect to the blob service and the file service.

Which tool can you use to access the contents in Container1 and Share1 by using the SAS? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Tools for Container1:

☐ Robocopy.exe
 ☐ Azure Storage Explorer
 ☐ File Explorer

Tools for Share1:

☐ Robocopy.exe
 ☐ Azure Storage Explorer
 ☐ File Explorer

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Tools for Container1:

☒ Robocopy.exe
 ☒ Azure Storage Explorer
 ☐ File Explorer

Tools for Share1:

☒ Robocopy.exe
 ☒ Azure Storage Explorer
 ☐ File Explorer

NEW QUESTION 302

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant named Contoso.com and an Azure Service (AKS) cluster AKS1.

You discover that AKS1 cannot be accessed by using accounts from Contoso.com

You need to ensure AKS1 can be accessed by using accounts from Contoso.com The solution must minimize administrative effort.

What should you do first?

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

Answer: A

Explanation:

Reference:

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

NEW QUESTION 304

- (Exam Topic 4)

You have a Microsoft 365 tenant that uses an Azure Active Directory (Azure AD) tenant The Azure AD tenant syncs to an on-premises Active Directory domain by using an instance of Azure AD Connect.

You create a new Azure subscription

You discover that the synced on-premises user accounts cannot be assigned roles in the new subscription. You need to ensure that you can assign Azure and Microsoft 365 roles to the synced Azure AD user accounts. What should you do first?

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

Answer: A

NEW QUESTION 308

- (Exam Topic 4)

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

Name	Connected to	Private IP address	Public IP address
VM1	VNET1/Subnet1	10.1.1.4	13.80.73.87
VM2	VNET2/Subnet2	10.2.1.4	213.199.133.190
VM3	VNET2/Subnet2	10.2.1.5	None

Subnet1 and Subnet2 have a Microsoft.Storage service endpoint configured.

You have an Azure Storage account named storageacc1 that is configured as shown in the following exhibit.

Save
Discard
Refresh

Allow access from

☐ All networks
 ☒ Selected networks

Configure network security for your storage accounts. [Learn more.](#)

Virtual networks

Secure your storage account with virtual networks. [+ Add existing virtual network](#)

[+ Add new virtual network](#)

VIRTUAL NETWORK	SUBNET	ADDRESS RANGE	ENDPOINT STATUS	RESOURCE GROUP	SUBSCRIPTION
No network selected.					

Firewall

Add IP ranges to allow access from the internet on your on-premises networks. [Learn more.](#)

Address Range

13.80.73.87 🗑️

Exceptions

☒ Allow trusted Microsoft services to access this storage account ⓘ
☐ Allow read access to storage logging from any network
☐ Allow read access to storage metrics from any network

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

Statements	Yes	No
From VM1, you can upload a blob to storageacc1.	<input type="radio"/>	<input type="radio"/>
From VM2, you can upload a blob to storageacc1.	<input type="radio"/>	<input type="radio"/>
From VM3 , you can upload a blob to storageacc1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box 1: Yes

The public IP of VM1 is allowed through the firewall.

Box 2: No

The allowed virtual network list is empty so VM2 cannot access storageacc1 directly. The public IP address of VM2 is not in the allowed IP list so VM2 cannot access storageacc1 over the Internet.

Box 3: No

The allowed virtual network list is empty so VM3 cannot access storageacc1 directly. VM3 does not have a public IP address so it cannot access storageacc1 over the Internet.

Reference:

https://docs.microsoft.com/en-gb/azure/storage/common/storage-network-security

NEW QUESTION 312

- (Exam Topic 4)

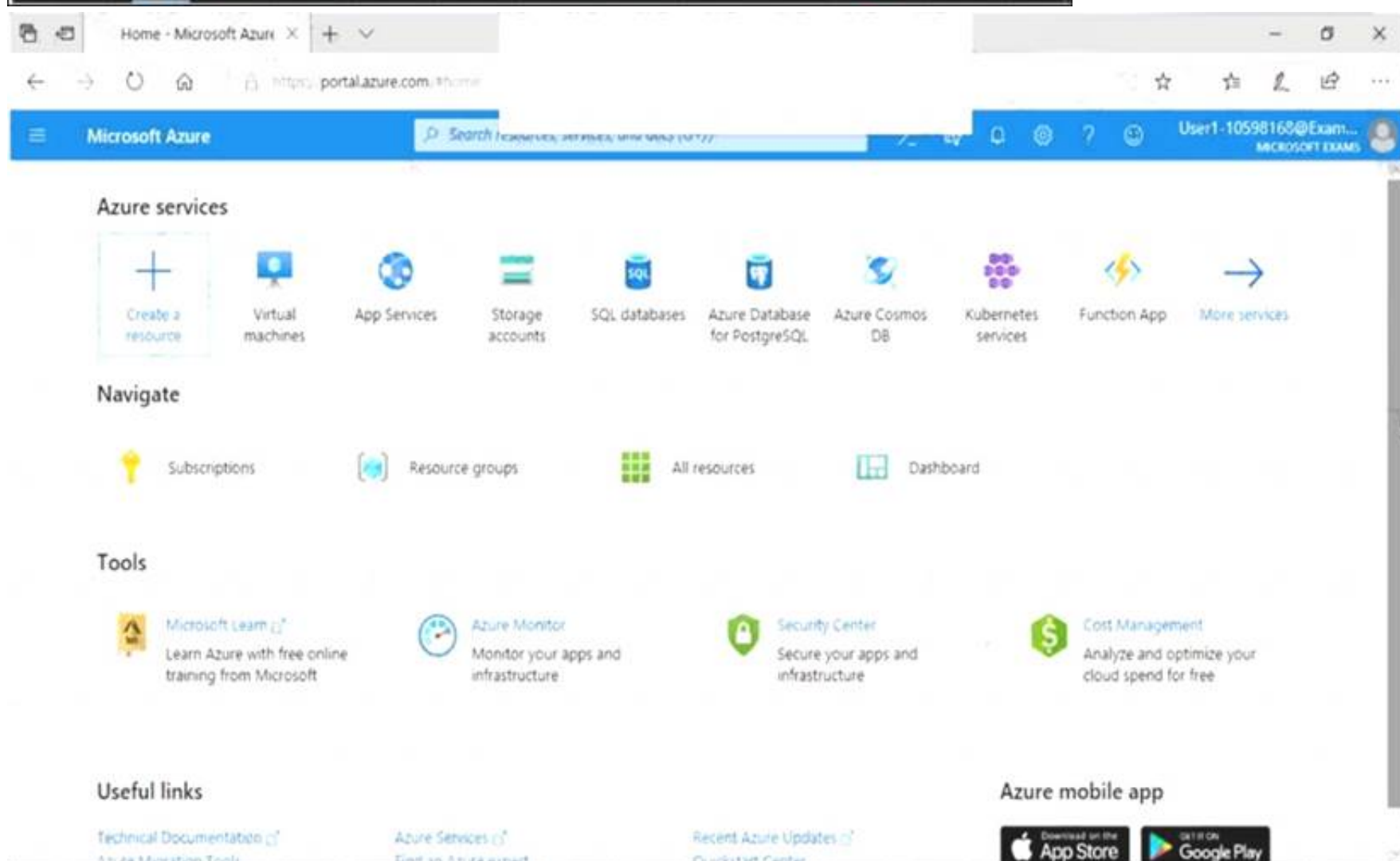
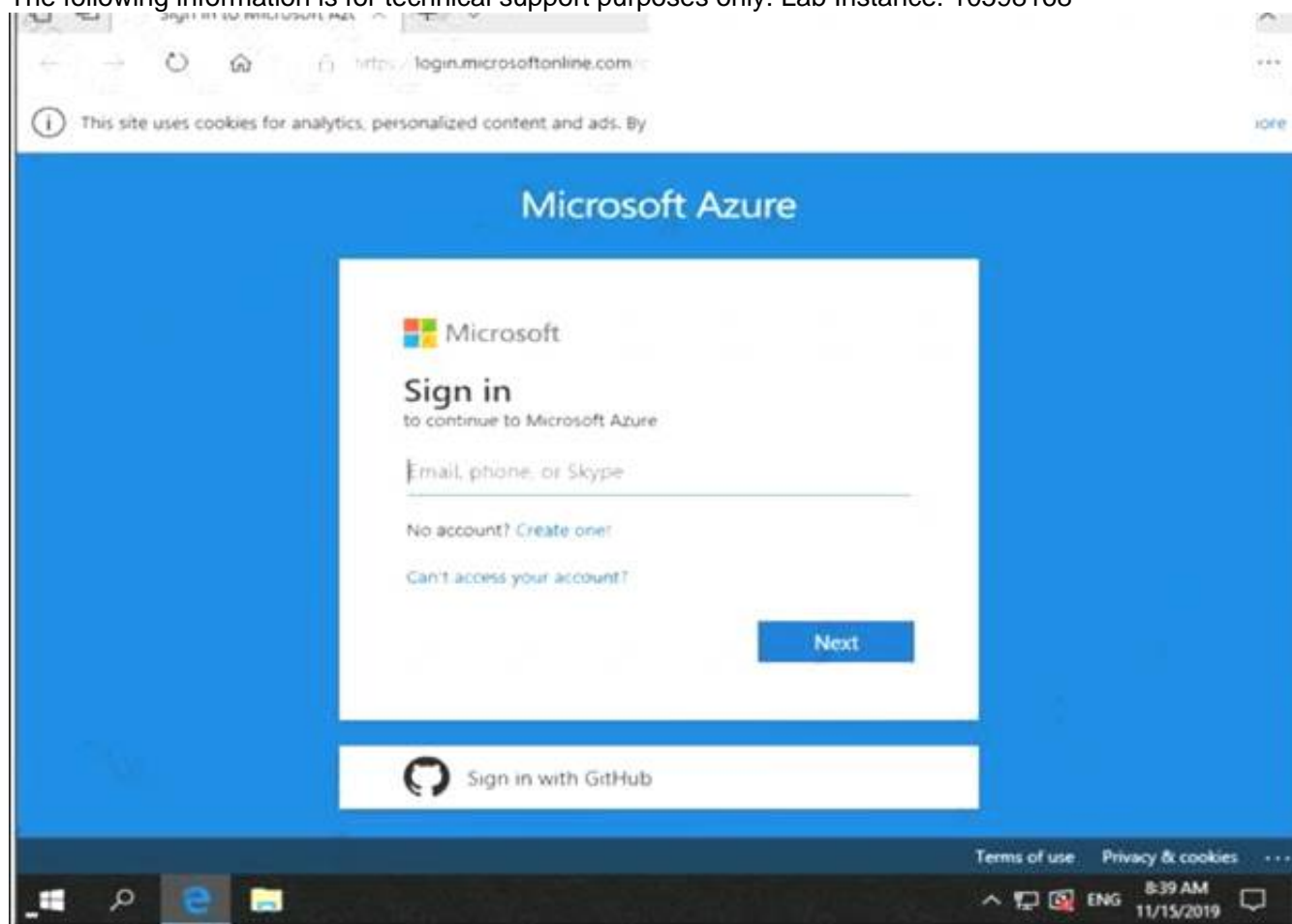
Use the following login credentials as needed:

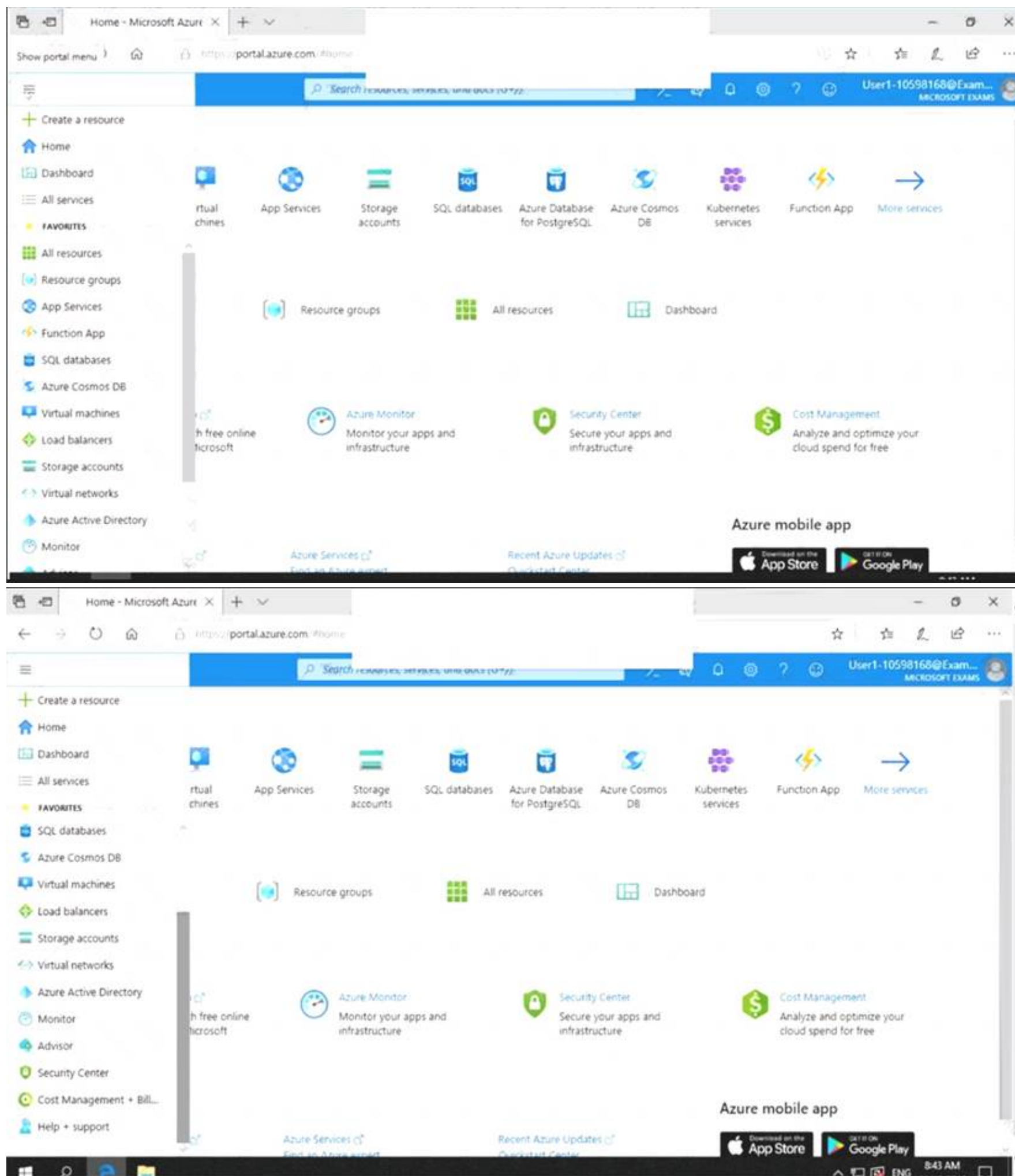
To enter your username, place your cursor in the Sign in box and click on the username below.

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

Azure Password: Ag1Bh9!#Bd

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





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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

- Sign in to the Azure portal.
- In Virtual Machines, select VM1
- In Settings, select Networking.
- In Inbound port rules, check whether the port for RDP is set correctly. The following is an example of the configuration:

Priority: 300 Name: Port_3389

Port(Destination): 3389 Protocol: TCP

Source: Any Destinations: Any Action: Allow Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-nsg-problem>

NEW QUESTION 315

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

az-500 Practice Exam Features:

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