QUESTION 163
You have an Azure virtual machine named VM1.
From Azure Security Center, you get the following high-severity recommendation: "Install endpoint protection solutions on virtual machine".
You need to resolve the issue causing the high-severity recommendation.
What should you do?

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

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

QUESTION 164
You have an Azure subscription that contains a virtual network. The virtual network contains the subnets shown in the following table.

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

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

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

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

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

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

QUESTION 165
SIMULATION
You need to ensure that web11597200 is protected from malware by using Microsoft Antimalware for Virtual Machines and is scanned every Friday at 01:00.
To complete this task, sign in to the Azure portal.
Answer:
You need to install and configure the Microsoft Antimalware extension on the virtual machine named web11597200.
1. In the Azure portal, type **Virtual Machines** in the search box, select **Virtual Machines** from the search results then select **web11597200**. Alternatively, browse to Virtual Machines in the left navigation pane.
2. In the properties of web11597200, click on **Extensions.**
3. Click the **Add** button to add an **Extension.**
4. Scroll down the list of extensions and select **Microsoft Antimalware.**
5. Click the **Create** button. This will open the settings pane for the **Microsoft Antimalware Extension.**
6. In the **Scan day** field, select **Friday.**
7. In the **Scan time** field, enter **60.** The scan time is measured in minutes after midnight so 60 would be 01:00, 120 would be 02:00 etc.
8. Click the **OK** button to save the configuration and install the extension.

QUESTION 166
SIMULATION
You need to ensure that the events in the NetworkSecurityGroupRuleCounter log of the VNET01-Subnet0-NSG network security group (NSG) are stored in the logs11597200 Azure Storage account for 30 days.
To complete this task, sign in to the Azure portal.
Answer:
You need to configure the diagnostic logging for the NetworkSecurityGroupRuleCounter log.
1. In the Azure portal, type **Network Security Groups** in the search box, select **Network Security Groups** from the search results then select **VNET01-Subnet0-NSG**. Alternatively, browse to Network Security Groups in the left navigation pane.
2. In the properties of the Network Security Group, click on **Diagnostic Settings.**
3. Click on the **Add diagnostic setting** link.
4. Provide a name in the **Diagnostic settings name** field. It doesn't matter what name you provide for the exam.
5. In the **Log** section, select **NetworkSecurityGroupRuleCounter**.
6. In the **Destination details** section, select **Archive to a storage account.**
7. In the **Storage account** field, select the **logs11597200** storage account.
8. In the **Retention (days)** field, enter **30.**
9. Click the **Save** button to save the changes.

QUESTION 167
SIMULATION
A user named Debbie has the Azure app installed on her mobile device.
You need to ensure that debbie@contoso.com is alerted when a resource lock is deleted.
To complete this task, sign in to the Azure portal.
Answer:
You need to configure an alert rule in Azure Monitor.
1. Type **Monitor** into the search box and select **Monitor** from the search results.
2. Click on **Alerts.**
3. Click on **+New Alert Rule.**
4. In the **Scope** section, click on the **Select resource** link.
5. In the **Filter by resource type** box, type **locks** and select **Management locks (locks)** from the filtered results.

6. Select the subscription then click the **Done** button.
7. In the **Condition** section, click on the **Select condition** link.
8. Select the **Delete management locks** condition the click the **Done** button.
9. In the **Action group** section, click on the **Select action group** link.
10. Click the **Create action group** button to create a new action group.
11. Give the group a name such as Debbie Mobile App (it doesn't matter what name you enter for the exam) then click the **Next: Notifications >** button.
12. In the **Notification type** box, select the **Email/SMS message/Push/Voice** option.
13. In the **Email/SMS message/Push/Voice** window, tick the **Azure app Push Notifications** checkbox and enter **debbie@contoso.com** in the **Azure account email field.**
14. Click the **OK** button to close the window.
15. Enter a name such as Debbie Mobile App in the notification name box.
16. Click the **Review & Create** button then click the **Create** button to create the action group.
17. Back in the **Create alert rule window**, in the **Alert rule details** section, enter a name such as **Management lock deletion** in the **Alert rule name** field.
18. Click the **Create alert rule** button to create the alert rule.

QUESTION 168
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?

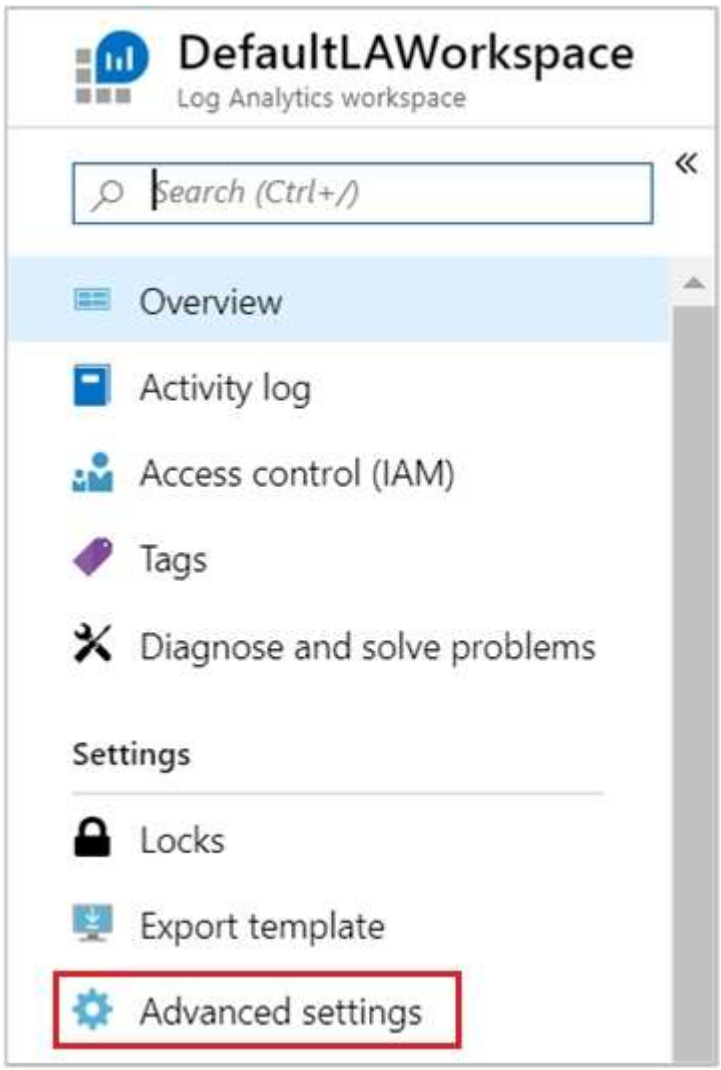
A. Azure Storage Explorer
B. SQL query editor in Azure
C. File Explorer in Windows
D. Azure Security Center

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

Note:
There are several versions of this question in the exam. The questions in the exam have two different correct answers:
1. Azure Storage Explorer
2. AZCopy
Other incorrect answer options you may see on the exam include the following:
1. Azure Monitor
2. The Security & Compliance admin center
3. Azure Cosmos DB explorer
4. Azure Monitor
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-metrics?toc=%2fazure%2fstorage%2fblobs%2ftoc.json
https://docs.microsoft.com/en-us/azure/storage/common/storage-explorers

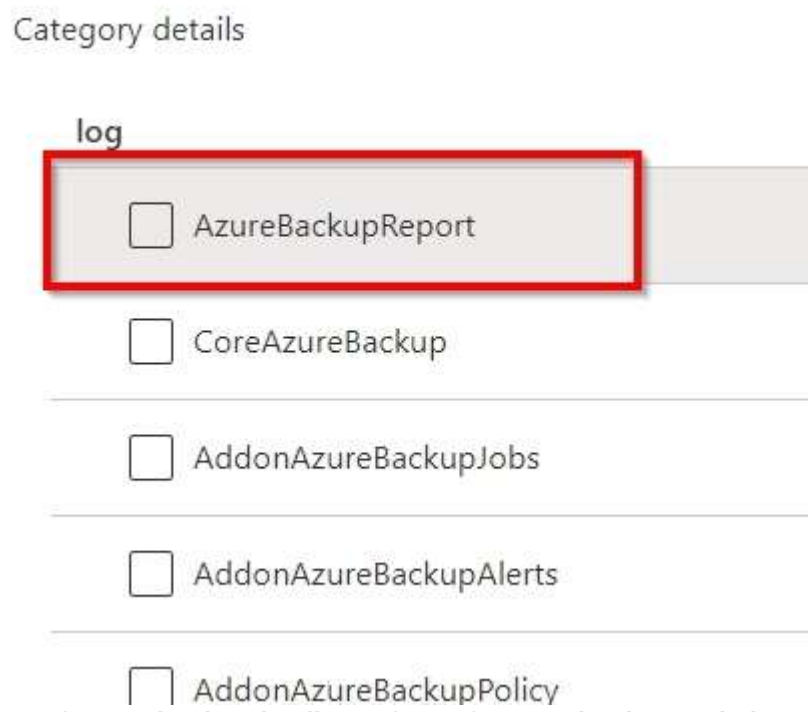
QUESTION 169
SIMULATION
You plan to connect several Windows servers to the WS11641655 Azure Log Analytics workspace.
You need to ensure that the events in the System event logs are collected automatically to the workspace after you connect the Windows servers.
To complete this task, sign in to the Azure portal and modify the Azure resources.
Answer:
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**.



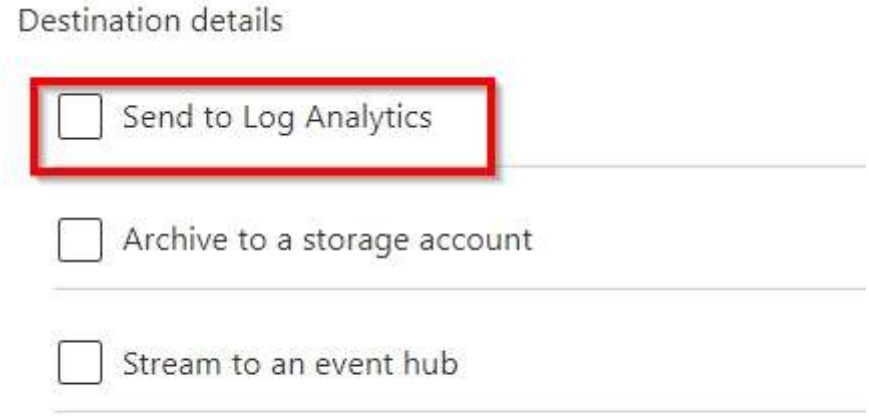
2. Select **Data**, and then select **Windows Event Logs**.
3. You add an event log by typing in the name of the log. Type **System** and then select the plus sign **+**.
4. In the table, check the severities **Error** and **Warning**. (for this question, select all severities to ensure that ALL logs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

QUESTION 170
SIMULATION

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.
Answer:
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.**



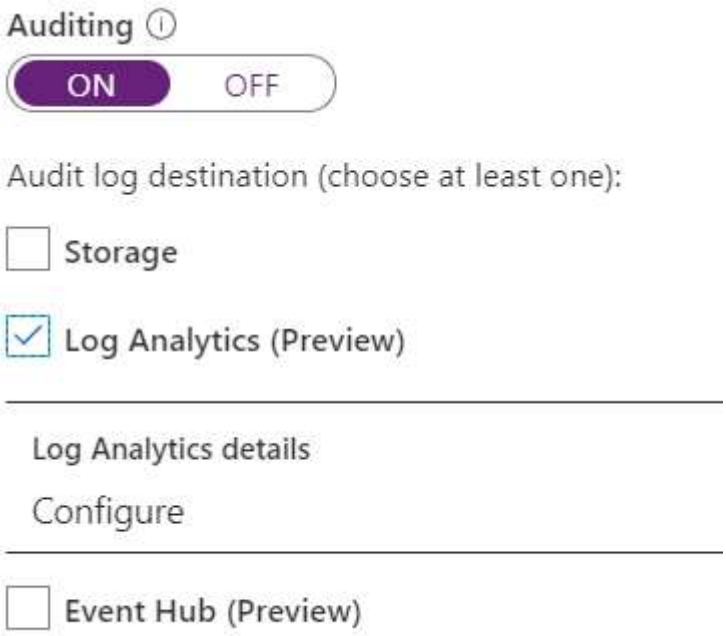
6. In the **Destination details** section, select **Send to log analytics**



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

QUESTION 171
SIMULATION
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.
Answer:
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.**



4. Select the **WS11641655** Azure Log Analytics workspace.
5. Click **Save** to save the changes.

QUESTION 172
SIMULATION
You need to configure a weekly backup of an Azure SQL database named Homepage. The backup must be retained for eight weeks.
To complete this task, sign in to the Azure portal.
Answer:
You need to configure the backup policy for the Azure SQL database.
1. In the Azure portal, type **Azure SQL Database** in the search box, select **Azure SQL Database** from the search results then select **Homepage**. Alternatively, browse to Azure SQL Database in the left navigation pane.
2. Select the server hosting the **Homepage** database and click on **Manage backups.**
3. Click on **Configure policies.**
4. Ensure that the **Weekly Backups** option is ticked.
5. Configure the **How long would you like weekly backups to be retained** option to **8 weeks.**
6. Click **Apply** to save the changes.

QUESTION 173
SIMULATION
You need to ensure that when administrators deploy resources by using an Azure Resource Manager template, the deployment can access secrets in an Azure key vault named KV11597200.
To complete this task, sign in to the Azure portal.
Answer:
You need to configure an option in the Advanced Access Policy of the key vault.
1. In the Azure portal, type **Azure Key Vault** in the search box, select **Azure Key Vault** from the search results then select the key vault named KV11597200. Alternatively, browse to Azure Key Vault in the left navigation pane.
2. In the properties of the key vault, click on **Advanced Access Policies.**
3. Tick the checkbox labelled **Enable access to Azure Resource Manager for template deployment.**
4. Click **Save** to save the changes.

QUESTION 174
SIMULATION
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.
Answer:
You need to enable the Web Application Firewall on the Application Gateway.

1. 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.
2. In the properties of the application gateway, click on **Web application firewall.**
3. For the **Tier** setting, select **WAF V2.**
4. In the **Firewall status** section, click the slider to switch to **Enabled.**
5. In the **Firewall mode** section, click the slider to switch to **Prevention.**
6. Click **Save** to save the changes.