SC-200 Q&As

Microsoft Security Operations Analyst

Pass Microsoft SC-200 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/sc-200.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

You have the following environment:

1.

Azure Sentinel

2.

A Microsoft 365 subscription

3.

Microsoft Defender for Identity

4.

An Azure Active Directory (Azure AD) tenant

You configure Azure Sentinel to collect security logs from all the Active Directory member servers and domain controllers.

You deploy Microsoft Defender for Identity by using standalone sensors.

You need to ensure that you can detect when sensitive groups are modified in Active Directory.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Configure the Advanced Audit Policy Configuration settings for the domain controllers.

B. Modify the permissions of the Domain Controllers organizational unit (OU).

C. Configure auditing in the Microsoft 365 compliance center.

D. Configure Windows Event Forwarding on the domain controllers.

Correct Answer: AD

To enable auditing for sensitive groups, you need to configure the Advanced Audit Policy Configuration settings for the domain controllers. This can be done by modifying the Default Domain Controllers Policy in the Group Policy Management Console (GPMC) and enabling the "Audit Detailed Directory Service Replication" policy under "Advanced Audit Policy Configuration\DS Access". This will generate audit events when sensitive groups are modified.

Windows Event Forwarding can be used to forward the audit events generated by the domain controllers to Azure Sentinel for analysis. This involves configuring a subscription on the domain controllers and a collection rule in Azure Sentinel to collect the forwarded events.

Reference: https://docs.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection
https://docs.microsoft.com/en-us/defender-for-identity/configure-event-collection

QUESTION 2

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint and contains a Windows device named Device1.

You need to investigate a suspicious executable file detected on Device1. The solution must meet the following requirements:

1.

Identify the image file path of the file.

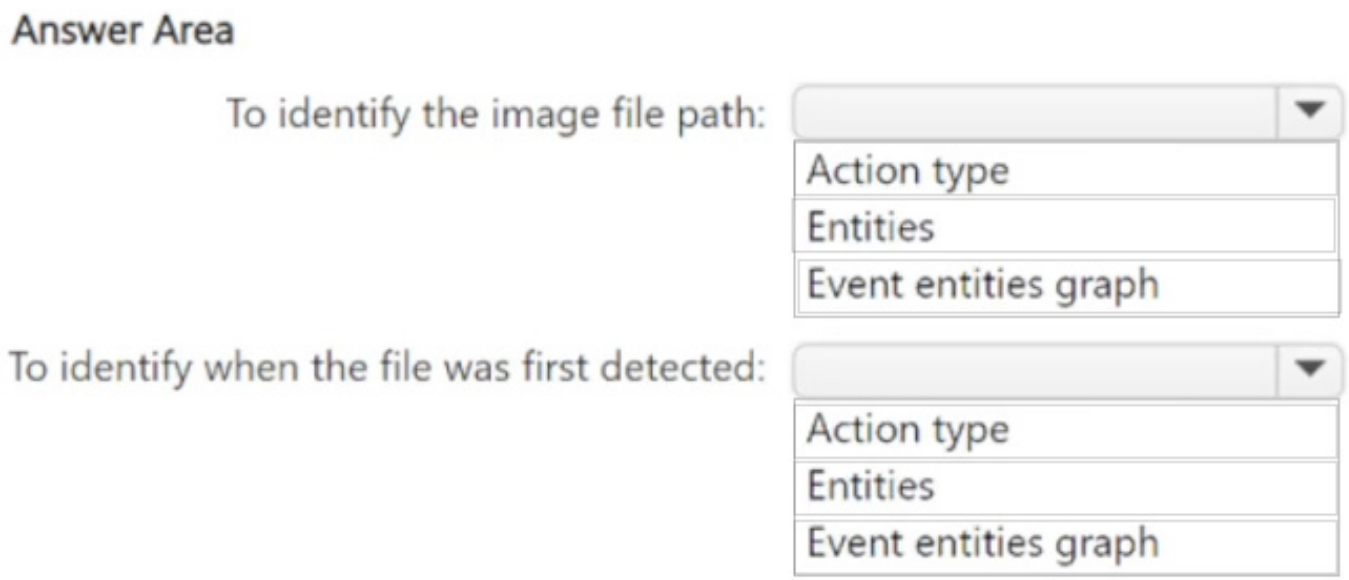
2.

Identify when the file was first detected on Device1.

What should you review from the timeline of the detection event? To answer, select the appropriate options in the answer area.

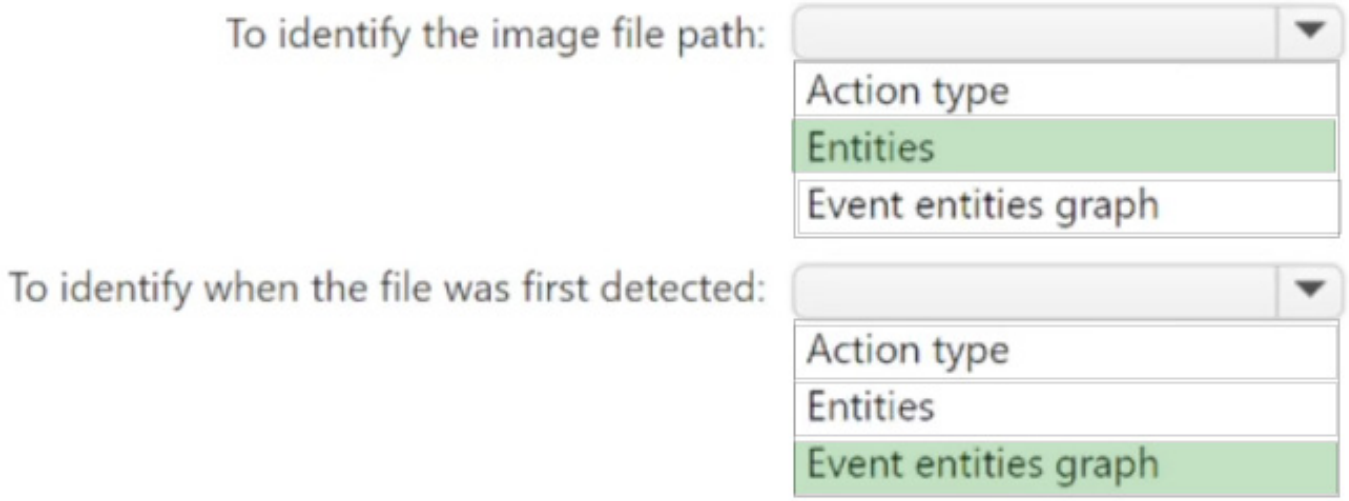
NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Answer Area



QUESTION 3

You have a third-party security information and event management (SIEM) solution.

You need to ensure that the SIEM solution can generate alerts for Azure Active Directory (Azure AD) sign-events in near real time.

What should you do to route events to the SIEM solution?

A. Create an Azure Sentinel workspace that has a Security Events connector.

B. Configure the Diagnostics settings in Azure AD to stream to an event hub.

C. Create an Azure Sentinel workspace that has an Azure Active Directory connector.

D. Configure the Diagnostics settings in Azure AD to archive to a storage account.

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-monitoring

QUESTION 4

HOTSPOT

Your on-premises network contains 100 servers that run Windows Server.

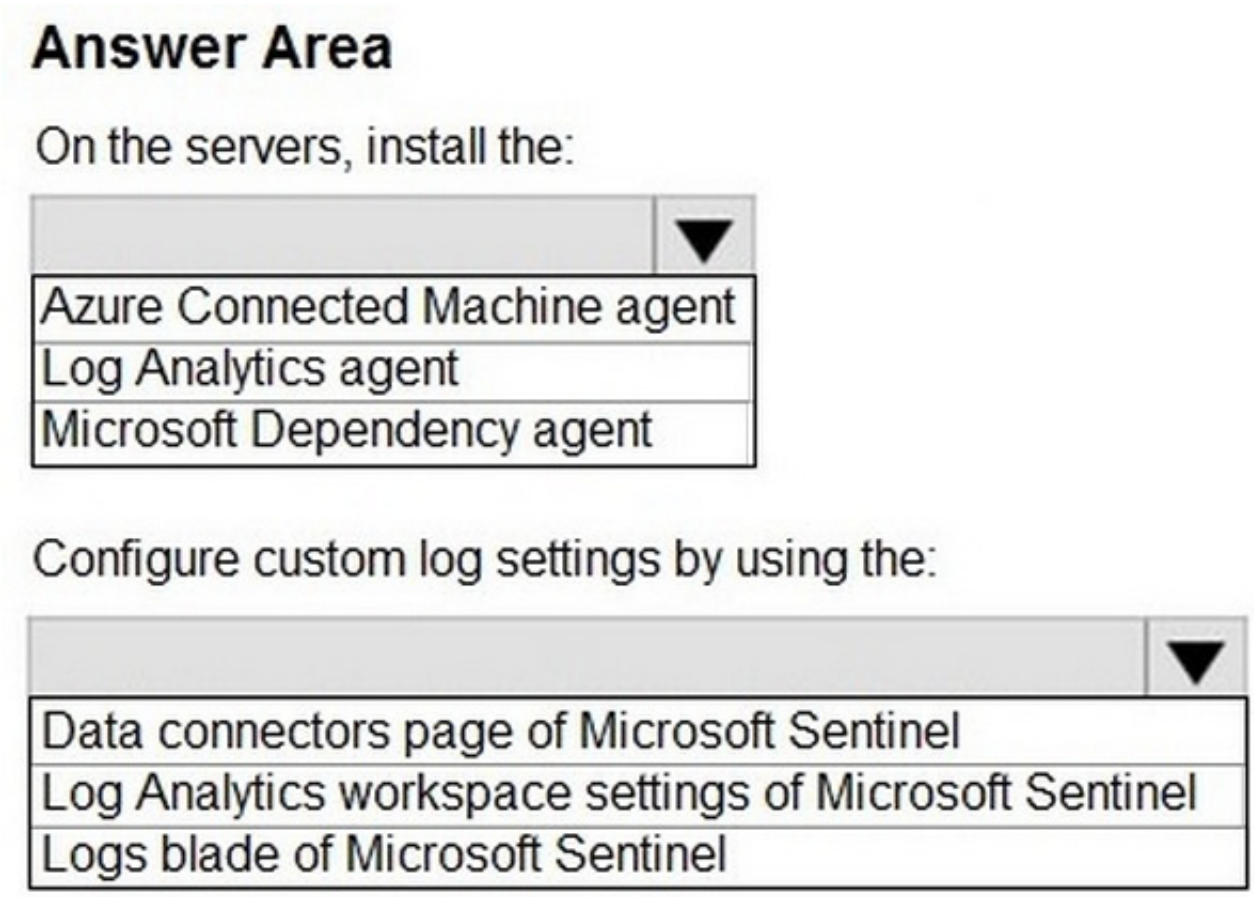
You have an Azure subscription that uses Microsoft Sentinel.

You need to upload custom logs from the on-premises servers to Microsoft Sentinel.

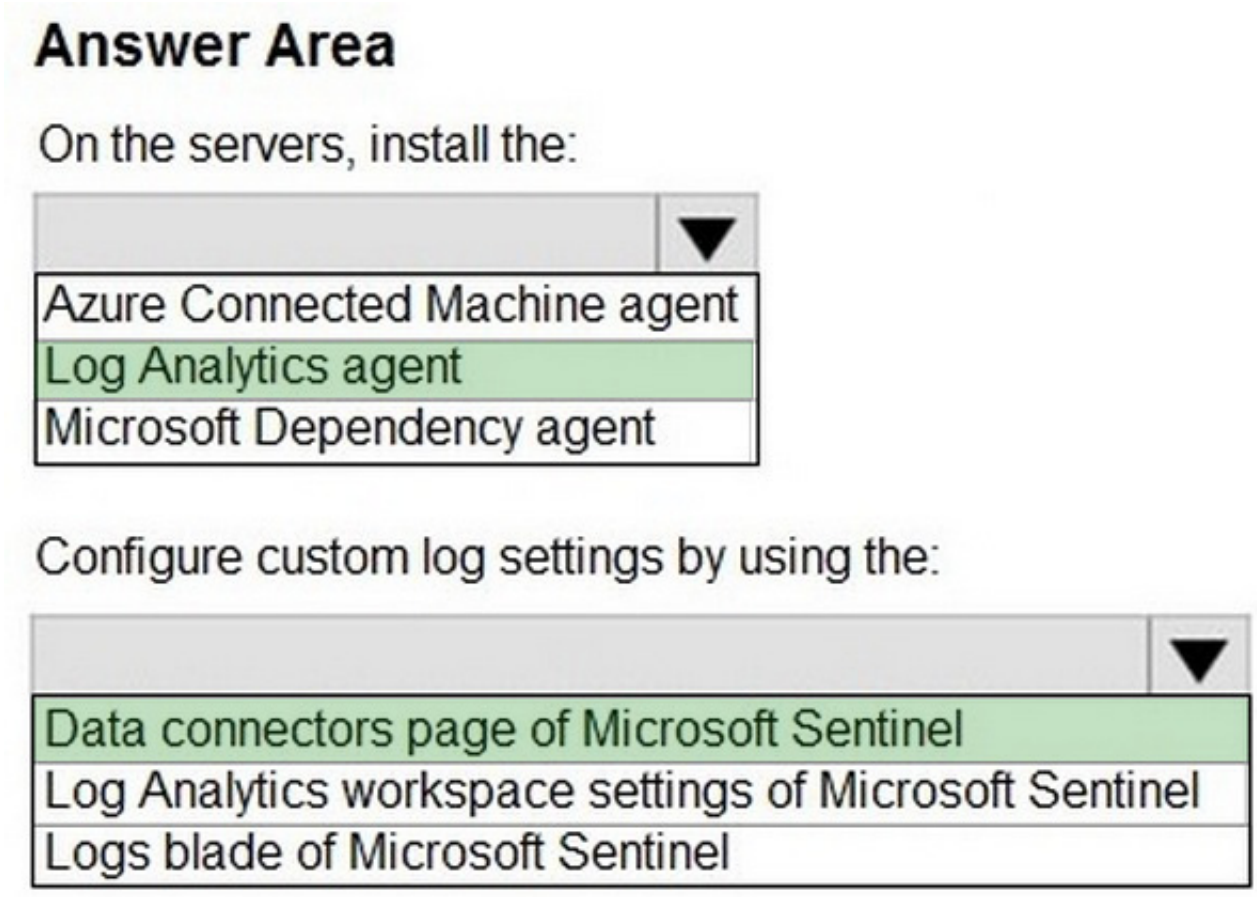
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: Log Analytics agent

Collect data in custom log formats to Microsoft Sentinel with the Log Analytics agent.

Many applications log data to text files instead of standard logging services like Windows Event log or Syslog. You can use the Log Analytics agent to collect data in text files of nonstandard formats from both Windows and Linux computers.

Once collected, you can either parse the data into individual fields in your queries or extract the data during collection to individual fields.

Box 2 Data connectors page of Microsoft Sentinel

Configure the logs to be collected

Many device types have their own data connectors appearing in the Data connectors page in Microsoft Sentinel. Some of these connectors require special additional instructions to properly set up log collection in Microsoft Sentinel. These

instructions can include the implementation of a parser based on a Kusto function.

All connectors listed in Microsoft Sentinel will display any specific instructions on their respective connector pages in the portal, as well as in their sections of the Microsoft Sentinel data connectors reference page.

If your product is not listed in the Data connectors page, consult your vendor\\'s documentation for instructions on configuring logging for your device.

Reference:

https://learn.microsoft.com/en-us/azure/sentinel/connect-custom-logs

QUESTION 5

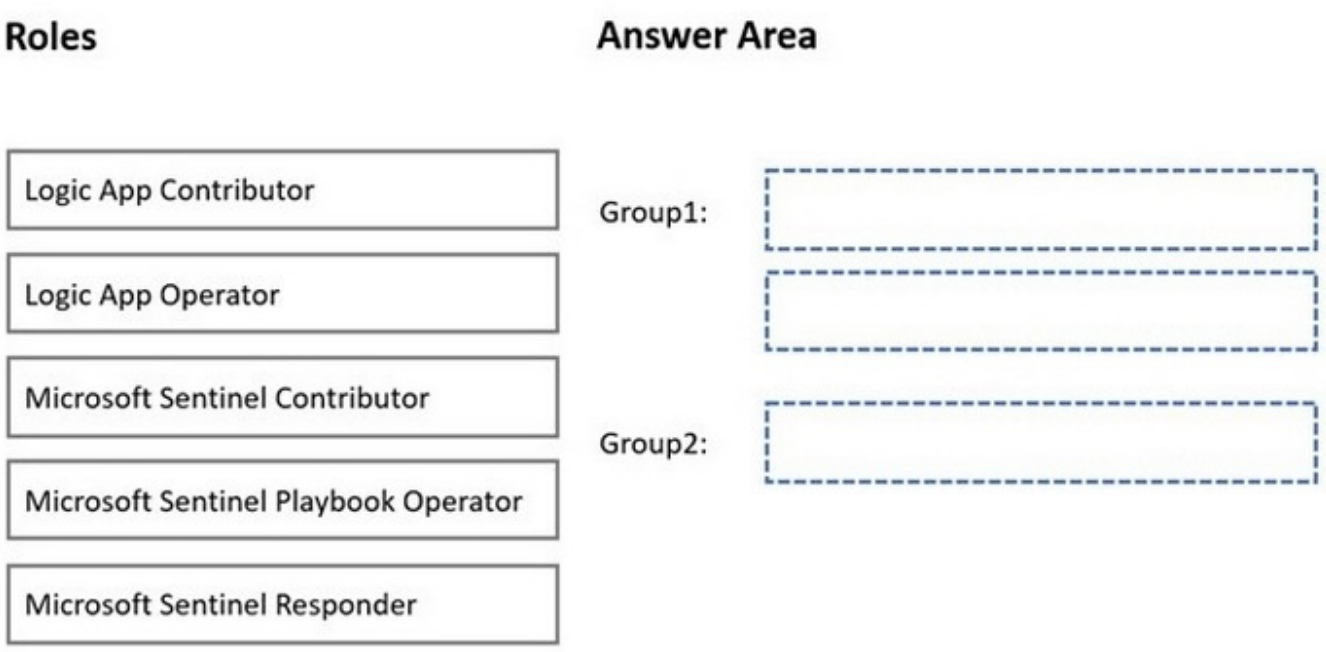
DRAG DROP

You need to assign role-based access control (RBAC) roles to Group1 and Group2 to meet the Microsoft Sentinel requirements and the business requirements.

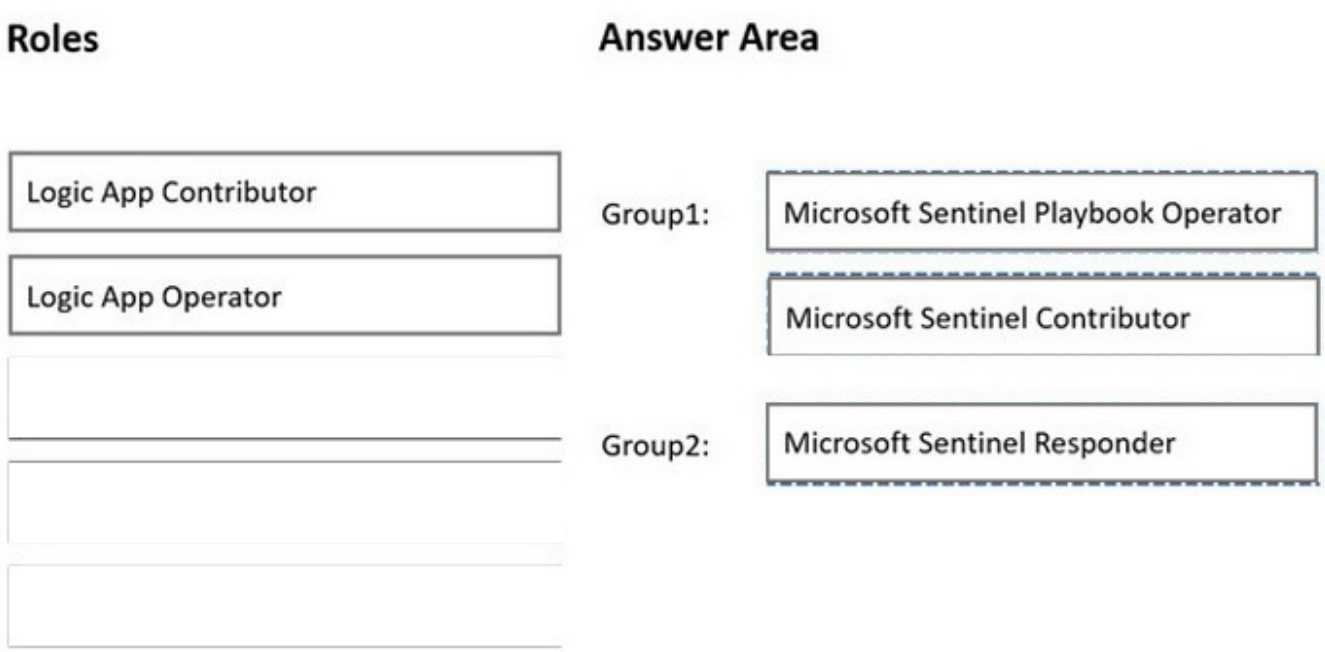
Which role should you assign to each group? To answer, drag the appropriate roles to the correct groups. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Box 1: Microsoft Sentinel Playbook Operator

Microsoft Sentinel Playbook Operator can list, view, and manually run playbooks.

Note: The fabrikam.com forest contains two global groups named Group1 and Group2.

Fabrikam identifies the following Microsoft Sentinel requirements:

Ensure that the members of Group1 can create and run playbooks.

Box 2: Microsoft Sentinel Contributor

Ensure that the members of Group1 can manage analytics rules.

Microsoft Sentinel Contributor can, in addition to the below (Microsoft Sentinel Reader +Microsoft Sentinel Responder), create and edit workbooks, analytics rules, and other Microsoft Sentinel resources.

Box 3: Microsoft Sentinel Responder

Ensure that the members of Group2 can manage incidents.

Microsoft Sentinel Reader can view data, incidents, workbooks, and other Microsoft Sentinel resources. Microsoft Sentinel Responder can, in addition to the above, manage incidents (assign, dismiss, etc.). Reference:

https://learn.microsoft.com/en-us/azure/sentinel/roles