Valid SC-200 Test Materials - Best SC-200 Preparation Materials

P.S. Free 2025 Microsoft SC-200 dumps are available on Google Drive shared by TestBraindump: https://drive.google.com/open?id=1Ralg5XY4Me88Pg8ycnvWXICPR5f4ToYP

All the TestBraindump Microsoft SC-200 practice questions are real and based on actual Microsoft Security Operations Analyst (SC-200) exam topics. The web-based Microsoft Security Operations Analyst (SC-200) practice test is compatible with all operating systems like Mac, IOS, Android, and Windows. Because of its browser-based Microsoft Security Operations Analyst (SC-200) practice exam, it requires no installation to proceed further. Similarly, Chrome, IE, Firefox, Opera, Safari, and all the major browsers support the Microsoft Security Operations Analyst (SC-200) practice test.

Exam SC-200: Microsoft Security Operations Analyst

The Microsoft Security Operations Analyst collaborates with organizational stakeholders to secure information technology systems for the organization. Their goal is to reduce organizational risk by rapidly remediating active attacks in the environment, advising on improvements to threat protection practices, and referring violations of organizational policies to appropriate stakeholders.

Responsibilities include threat management, monitoring, and response by using a variety of security solutions across their environment. The role primarily investigates, responds to, and hunts for threats using Microsoft Azure Sentinel, Azure Defender, Microsoft 365 Defender, and third-party security products. Since the Security Operations Analyst consumes the operational output of these tools, they are also a critical stakeholder in the configuration and deployment of these technologies.

Part of the requirements for: Microsoft Certified: Security Operations Analyst Associate

Download exam skills outline

>> Valid SC-200 Test Materials <<

Best Microsoft SC-200 Preparation Materials, SC-200 Visual Cert Exam

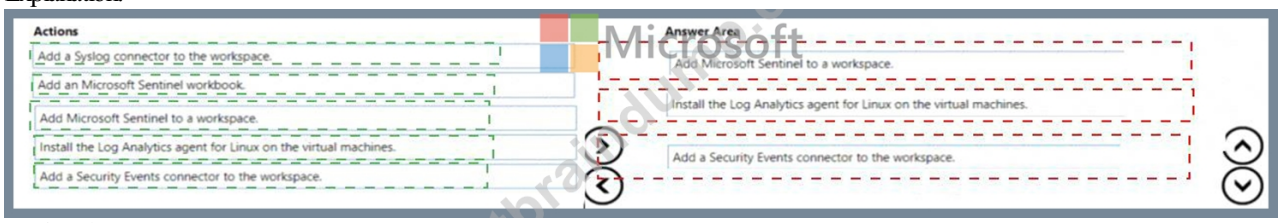
Time is life, time is speed, and time is power. You have to spend less time reaching your goals before you can walk ahead and seize more opportunities. Now, if you use our SC-200 preparation materials, you only need to learn twenty to thirty hours to go to the exam. And this data is provided and tested by our worthy customers. For they have passed the exam with the help of our SC-200 Exam Questions in such a short time and as 98% to 100% of them passed. The pass rate is also unmatched in the market!

Microsoft Security Operations Analyst Sample Questions (Q63-Q68):

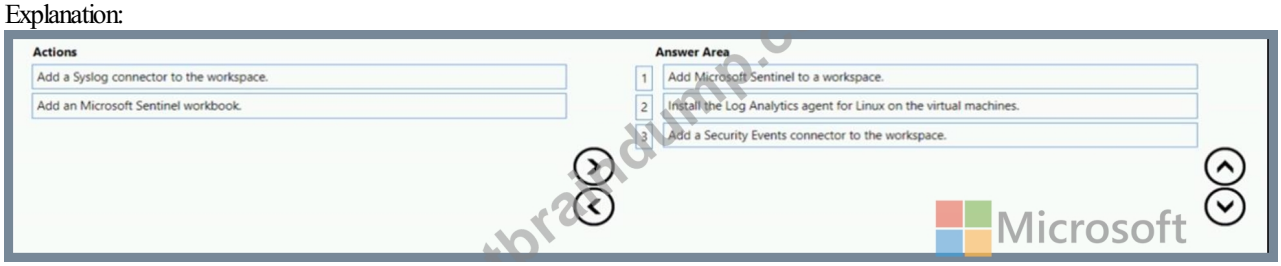
NEW QUESTION # 63
You have an Azure subscription that contains 100 Linux virtual machines.
You need to configure Microsoft Sentinel to collect event logs from the virtual machines.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Answer:

Explanation:



Explanation:



NEW QUESTION # 64

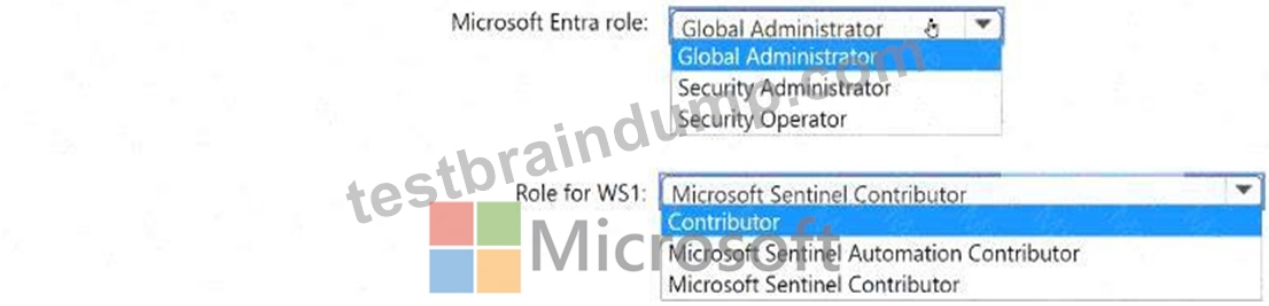
You have an Azure subscription that contains a user named User1 and a Microsoft Sentinel workspace named WS1.

You need to ensure that User1 can enable User and Entity Behavior Analytics (UEBA) for WS1. The solution must follow the principle of least privilege.

Which roles should you assign to User1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

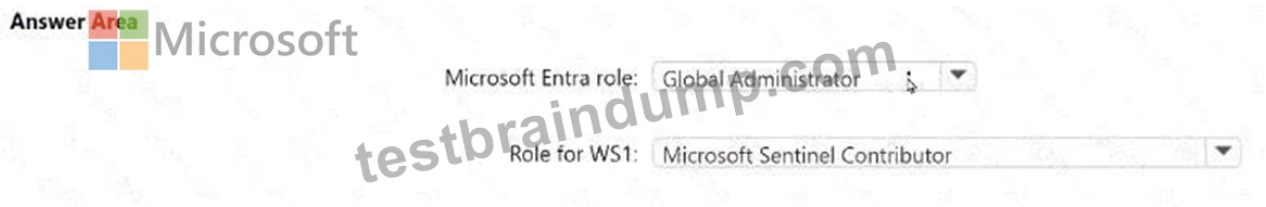


Answer:

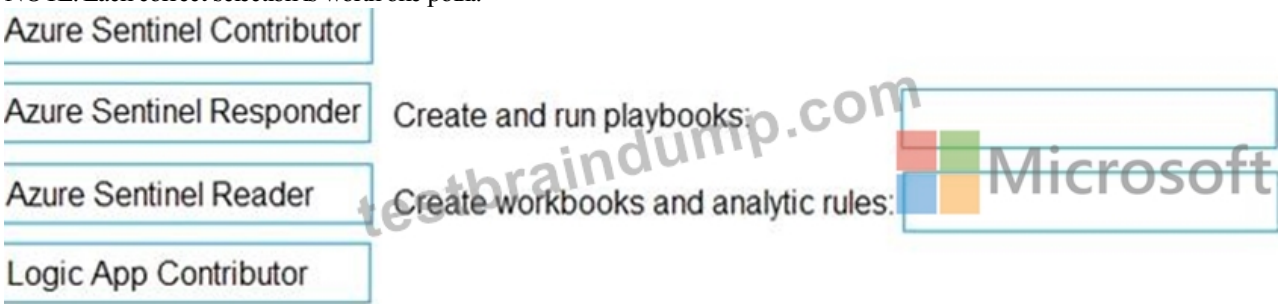
Explanation:

Answer Area

Explanation:

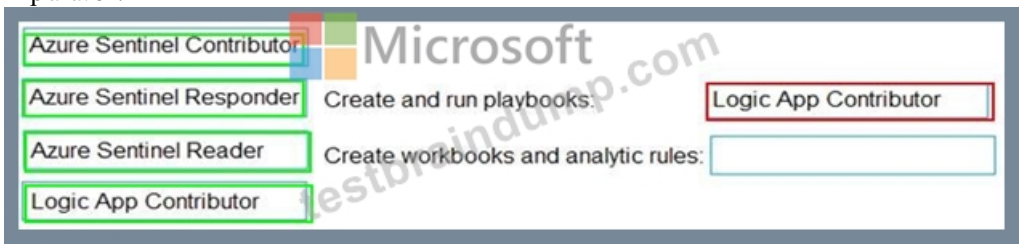


NEW QUESTION # 65
Your company deploys Azure Sentinel.
You plan to delegate the administration of Azure Sentinel to various groups.
You need to delegate the following tasks:
Create and run playbooks
Create workbooks and analytic rules.
The solution must use the principle of least privilege.
Which role should you assign for each task? To answer, drag the appropriate roles to the correct tasks. 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.



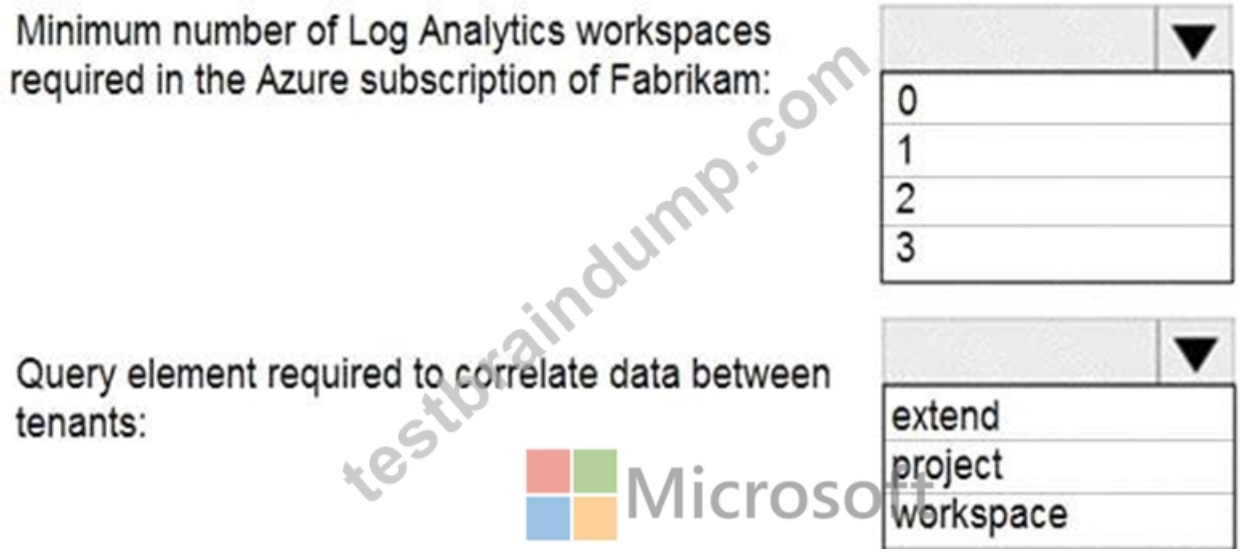
Answer:

Explanation:



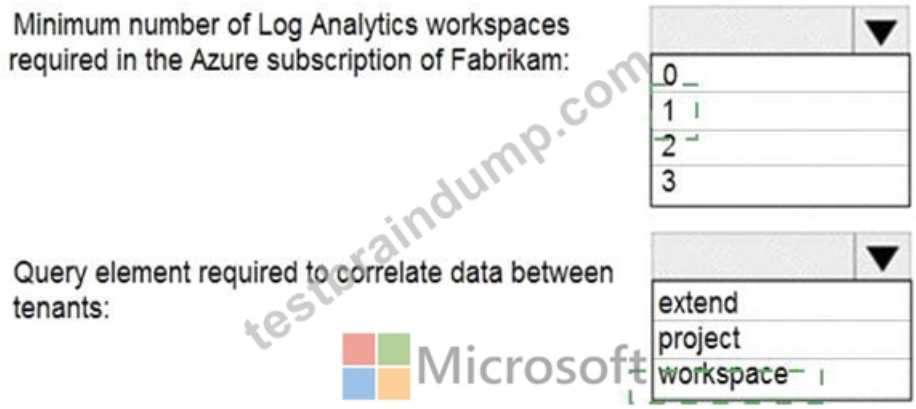
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/roles

NEW QUESTION # 66
You need to implement Azure Sentinel queries for Contoso and Fabrikam to meet the technical requirements.
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.

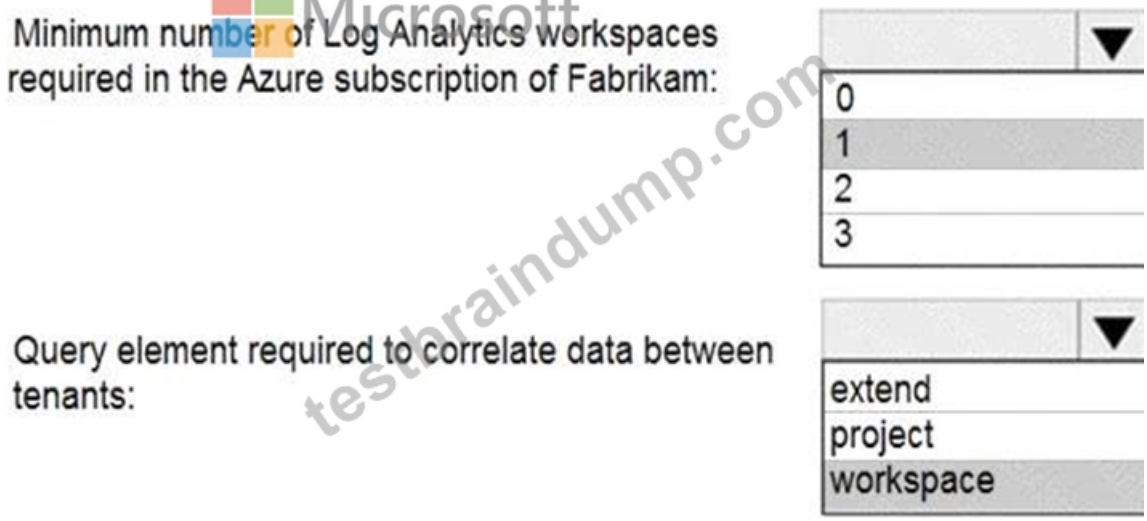


Answer:

Explanation:



Explanation:



Reference:
https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants

NEW QUESTION # 67
You receive a security bulletin about a potential attack that uses an image file.
You need to create an indicator of compromise (IoC) in Microsoft Defender for Endpoint to prevent the attack.
Which indicator type should you use?

- A. a URL/domain indicator that has Action set to Alert and block
- B. a file hash indicator that has Action set to Alert and block
- C. a URL/domain indicator that has Action set to Alert only
- D. a certificate indicator that has Action set to Alert and block

Answer: B

Explanation:
Section: [none]
Explanation/Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-file?view=o365-worldwide

NEW QUESTION # 68
.....

The SC-200 latest question we provide all candidates that that is compiled by experts who have good knowledge of exam, and they are very experience in compile study materials. Not only that, our team checks the update every day, in order to keep the latest information of SC-200 Exam Question. So why not try our SC-200 original questions, which will help you maximize your pass rate? Even if you unfortunately fail to pass the exam, we will give you a full refund.