Mock Microsoft SC-200 Exam, SC-200 Visual Cert Test

SKILLCERTPRO
Microsoft (SC-200) Microsoft Security Operations Analyst
Prepare and pass your certification in first attempt

BONUS!!! Download part of Prep4sures SC-200 dumps for free: https://drive.google.com/open?id=1I9RSf-KoiSsEWkQgYsyjJ7z0VN3qN06Z

For Microsoft SC-200 certification test, are you ready? The exam comes in sight, but can you take the test with confidence? If you have not confidence to sail through your exam, here I will recommend the most excellent reference materials for you. The latest SC-200 Certification Training dumps that can pass your exam in a short period of studying have appeared. The dumps are provided by Prep4sures.

Get ready for the Microsoft SC-200 Exam

Microsoft Security Operations Analyst Certification is a professional-level certification that has been designed to recognize individuals with the knowledge and skills necessary to protect enterprise networks from any online threats. While taking the Microsoft SC-200 test, the candidate will be required to have a good understanding of various security threats, malware, and hacker attacks. They will also have to have a deep understanding of different types of firewalls and IDS/IPS systems, as well as how they work together. Candidates should also be aware of network infrastructure devices, such as routers, proxies, and servers involved in implementing an effective security strategy. Another important area that the candidate must cover is risk management techniques used by the enterprise department to identify potential risks and vulnerabilities. The candidate must also know how to effectively monitor internal and external networks for any signs of intrusions or other Cyber crime. The Microsoft **SC-200 exam dumps** have been designed to provide you with all the knowledge required to pass the Microsoft SC-200 Certification Exam.

The Microsoft SC-200 exam requires you to have expert knowledge on Windows Server Update Services (WSUS), Group Policy, and Active Directory. Candidates must also possess expert knowledge on System Center Configuration Manager (SCCM) 2007 R2 and Windows Intune.

>> Mock Microsoft SC-200 Exam <<

SC-200 Visual Cert Test | Latest SC-200 Test Online

Most candidates who register for Microsoft Security Operations Analyst (SC-200) certification lack the right resources to help them achieve it. As a result, they face failure, which causes them to waste time and money, and sometimes even lose motivation to repeat their Microsoft SC-200 exam. Prep4sures will solve such problems for you by providing you with SC-200 Questions. The Microsoft SC-200 certification exam is undoubtedly a challenging task, but it can be made much easier with the help of Prep4sures's reliable preparation material.

Microsoft Security Operations Analyst Sample Questions (Q10-Q15):

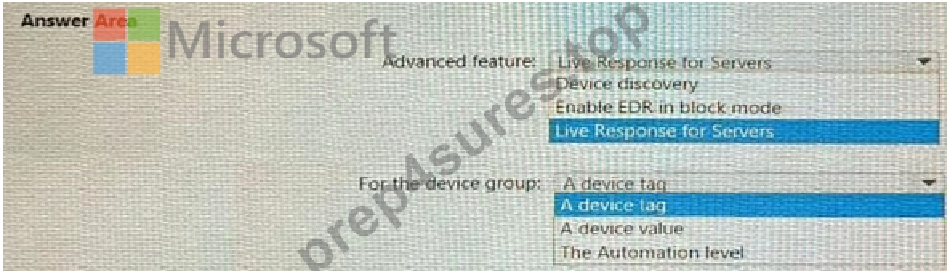
NEW QUESTION # 10

You have a Microsoft 365 E5 subscription that uses Microsoft 365 Defender for Endpoint.

You need to ensure that you can initiate remote shell connections to Windows servers by using the Microsoft 365 Defender portal.

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

NOTE: Each correct selection is worth one point.



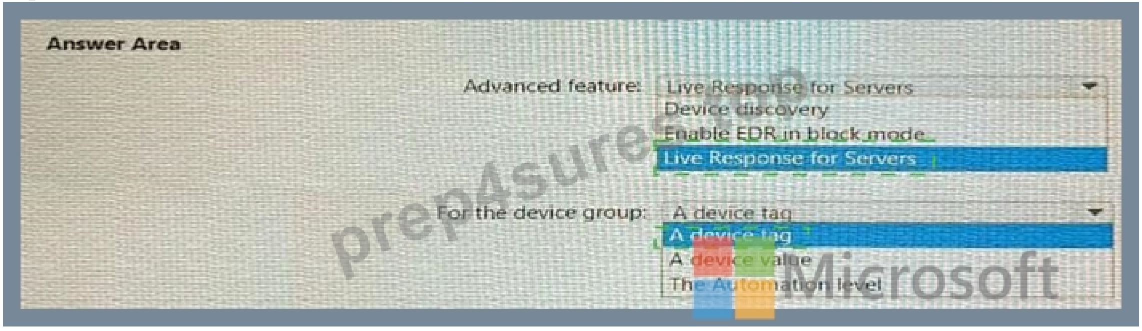
Answer Area

Advanced feature: Live Response for Servers
- Device discovery
- Enable EDR in block mode
- Live Response for Servers

For the device group: A device tag
- A device tag
- A device value
- The Automation level

Answer:

Explanation:

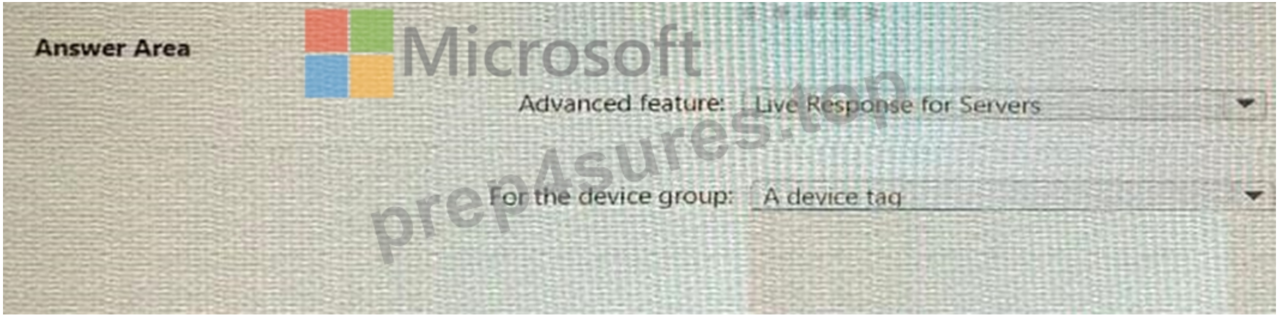


Answer Area

Advanced feature: Live Response for Servers
- Device discovery
- Enable EDR in block mode
- Live Response for Servers

For the device group: A device tag
- A device tag
- A device value
- The Automation level

Explanation:



Answer Area

Advanced feature: Live Response for Servers

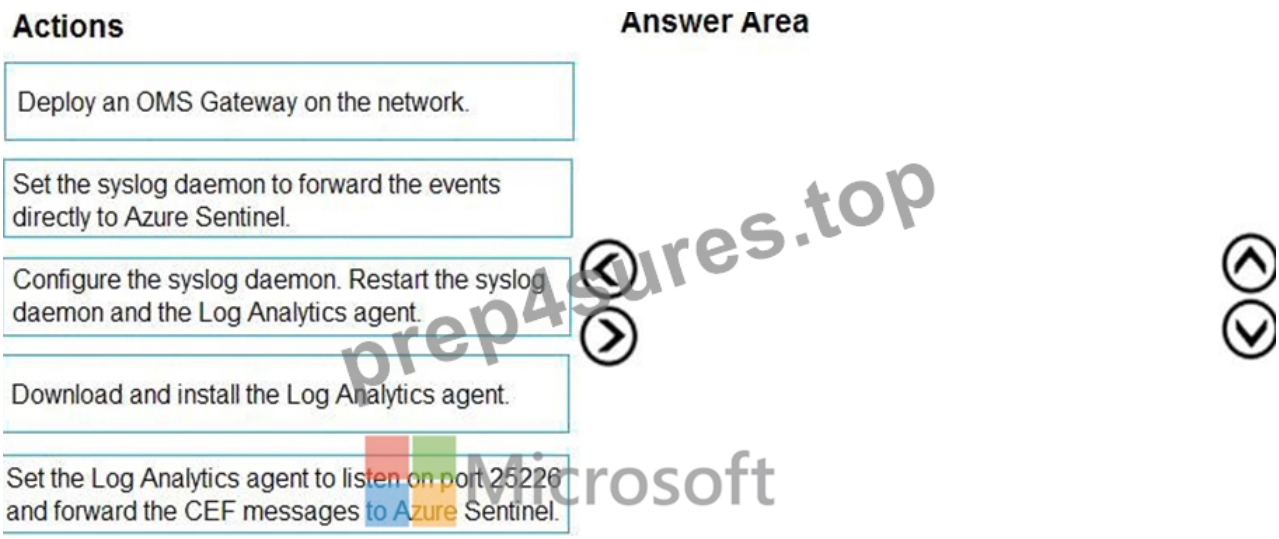
For the device group: A device tag

NEW QUESTION # 11

You plan to connect an external solution that will send Common Event Format (CEF) messages to Azure Sentinel.

You need to deploy the log forwarder.

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



Actions

Deploy an OMS Gateway on the network.

Set the syslog daemon to forward the events directly to Azure Sentinel.

Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.

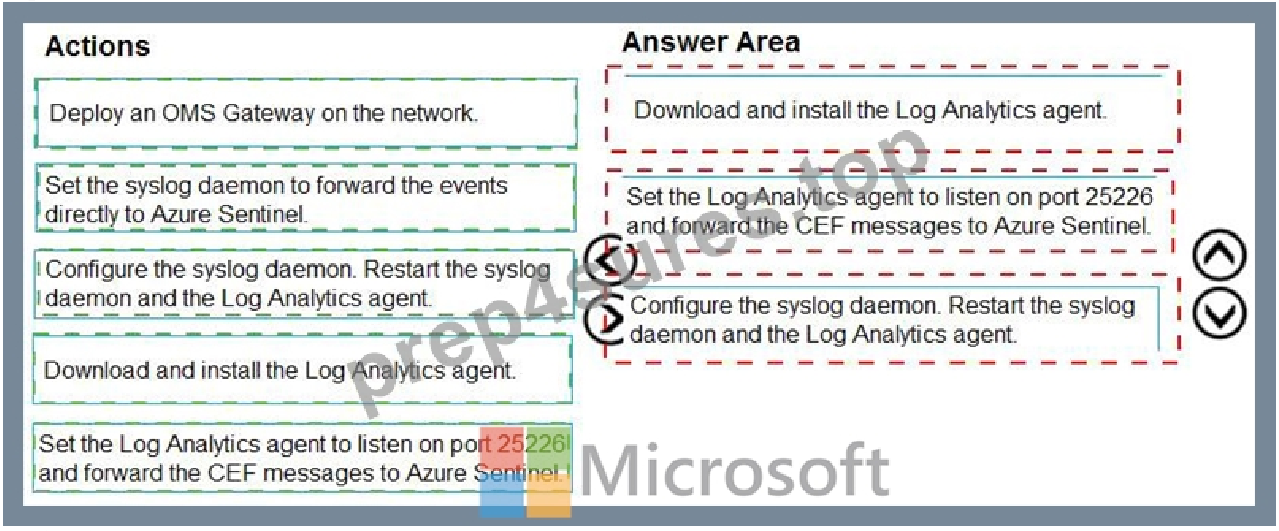
Download and install the Log Analytics agent.

Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.

Answer Area

Answer:

Explanation:



Actions

Deploy an OMS Gateway on the network.

Set the syslog daemon to forward the events directly to Azure Sentinel.

Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.

Download and install the Log Analytics agent.

Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.

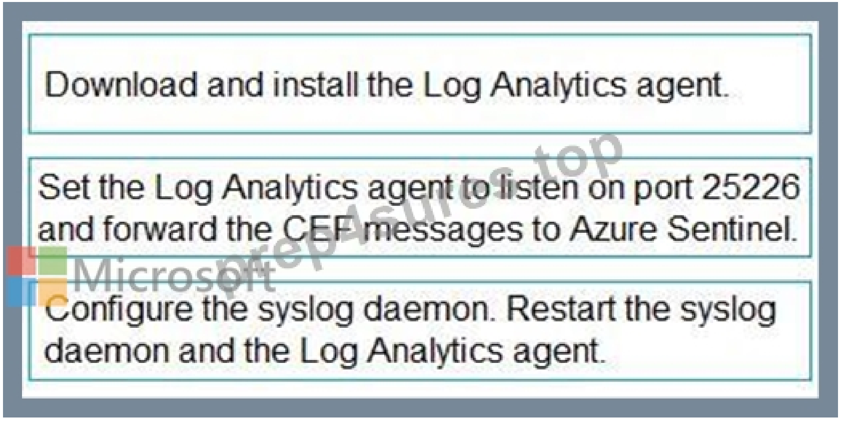
Answer Area

Download and install the Log Analytics agent.

Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.

Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.

Explanation



Download and install the Log Analytics agent.

Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.

Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.

Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-cef-agent?tabs=rsyslog

NEW QUESTION # 12

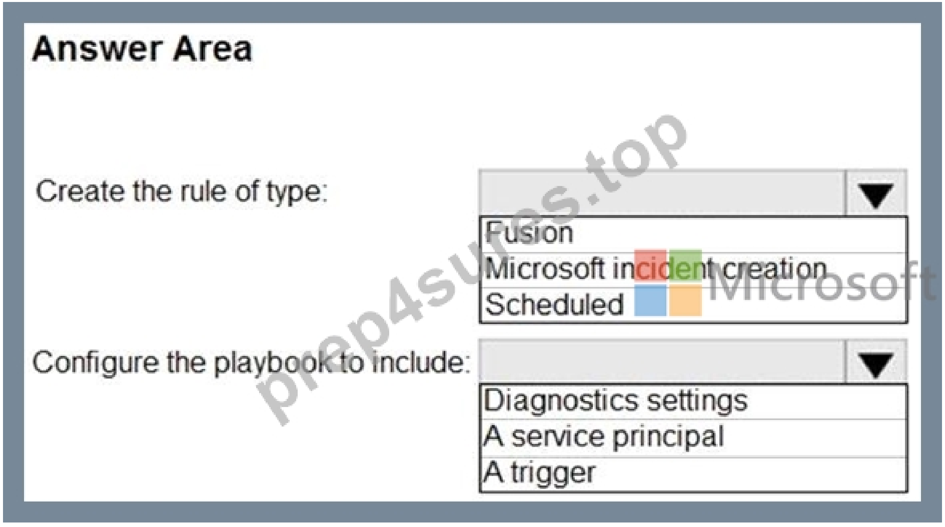
You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint.
You need to add threat indicators for all the IP addresses in a range of 171.23.3432-171.2334.63. The solution must minimize administrative effort.
What should you do in the Microsoft 365 Defender portal?

- A. Select Add indicator and set the IP address to 171.23.34.32/27
- B. Create an import file that contains the individual IP addresses in the range. Select Import and import the file.
- C. Create an import file that contains the IP address of 171.23.34.32/27. Select Import and import the file.
- D. Select Add indicator and set the IP address to 171.2334.32-171.23.34.63.

Answer: B

Explanation:
Explanation
This will add all the IP addresses in the range of 171.23.34.32/27 as threat indicators. This is the simplest and most efficient way to add all the IP addresses in the range.
Reference:
[1] https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/threat-intelligenc

NEW QUESTION # 13
You need to create the analytics rule to meet the Azure Sentinel requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



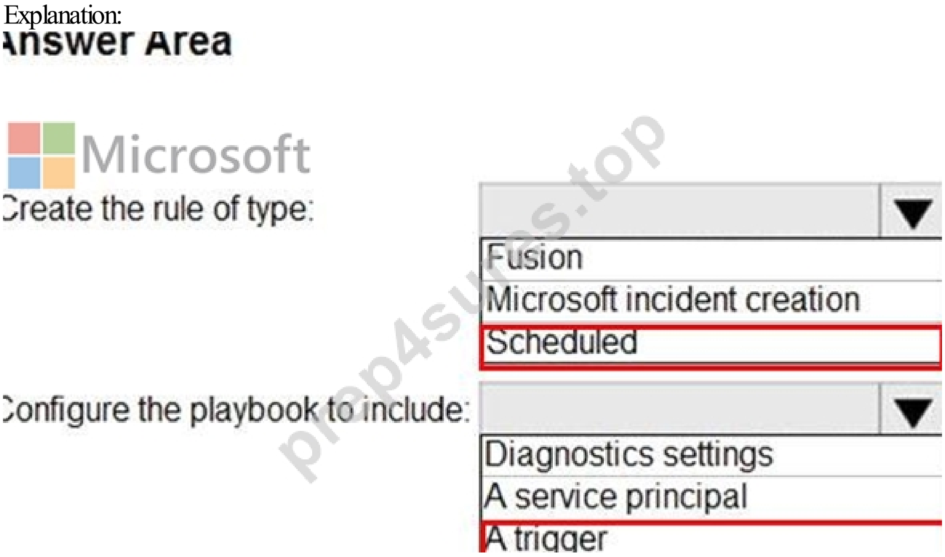
Answer Area

Create the rule of type:
- Fusion
- Microsoft incident creation
- Scheduled

Configure the playbook to include:
- Diagnostics settings
- A service principal
- A trigger

Answer:

Explanation:



nswer Area

reate the rule of type:
- Fusion
- Microsoft incident creation
- [✓ Scheduled]

onfigure the playbook to include:
- Diagnostics settings
- A service principal
- [✓ A trigger]

NEW QUESTION # 14
You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint Plan 2 and contains 500 Windows devices. You plan to create a Microsoft Defender XDR custom deception rule. You need to ensure that the rule will be applied to only 10 specific

devices. What should you do first?

- A. Add custom lures to the rule.
- B. Add the devices to a group.
- C. Add the IP address of each device to the list of decoy accounts and hosts of the rule.
- D. Assign a tag to the devices

Answer: D

Explanation:
Custom deception rules in Defender XDR/Defender for Endpoint can be targeted by scope (e.g., device tags /device groups). To apply a rule only to a specific subset (10 out of 500), first tag those devices, then target the rule to that tag (or a device group that uses that tag).

NEW QUESTION # 15
......

Our SC-200 simulating exam is made by our responsible company which means you can gain many other benefits as well. On condition that you fail the exam after using our SC-200 study prep unfortunately, we will switch other versions for you or give back full of your refund. If you are interested to our SC-200 simulating exam, just place your order now. And you will receive it only in a few minutes.

SC-200 Visual Cert Test: https://www.prep4sures.top/SC-200-exam-dumps-torrent.html

2025 Latest Prep4sures SC-200 PDF Dumps and SC-200 Exam Engine Free Share: https://drive.google.com/open?id=1I9RSf-KoiSsEWkQgYsyjJ7z0VN3qN06Z