NSE6_FSM_AN-7.4 Valid Exam Syllabus, NSE6_FSM_AN-7.4 Latest Demo

GetValidTest provides you with Fortinet NSE6_FSM_AN-7.4 exam questions in 3 different formats to open up your study options and suit your preparation tempo. The Fortinet NSE6_FSM_AN-7.4 PDF is the most convenient format to go through all exam questions easily. It is a compilation of actual Fortinet NSE6_FSM_AN-7.4 exam questions and answers.

Fortinet NSE6_FSM_AN-7.4 Exam Syllabus Topics:

Section	Objectives
Machine Learning, UEBA, and ZTNA	- Advanced analytics integration • 1. Configure ML configuration tasks • 2. Integrate UEBA data into rules and dashboards • 3. Describe ZTNA integration in FortiSIEM operations
Rules and Subpatterns	- Analytics rules configuration • 1. Configure FortiSIEM analytics rules • 2. Use rule subpatterns, aggregation, and group by • 3. Identify rule components
Incidents, Notifications, and Remediation	- Incident management • 1. Manage and tune incidents • 2. Configure remediation options • 3. Configure notification policies
Analytics	- Query and event analysis • 1. Perform CMDB and lookup table queries • 2. Perform nested query lookups • 3. Build queries from search results and events • 4. Apply group by and data aggregation on search results
FortiEDR Security Settings and Policies	- Security configuration • 1. Explain Fortinet Cloud Service (FCS) • 2. Configure playbooks • 3. Configure communication control policy • 4. Configure security policies

NSE6_FSM_AN-7.4 Latest Demo, Exam NSE6_FSM_AN-7.4 Questions Answers

Candidates may have different ways to practice the NSE6_FSM_AN-7.4 study materials, some may like to practice in paper, and some may like to practice it in the computer. We have three versions for you to meet your different needs. If you like to practice in the paper, NSE6_FSM_AN-7.4 PDF version will be your choice, which can be printed into the hard one. If you like to practice on your computer, NSE6_FSM_AN-7.4 Soft test engine will be your best, choice, besides it also stimulates the exam environment, you can experience the exam environment through this.

Fortinet NSE 6 - FortiSIEM 7.4 Analyst Sample Questions (Q55-Q60):

NEW QUESTION # 55
A critical server is sending traffic that is triggering a high severity outbound intrusion prevention system (IPS) permitted IPS exploit rule. This traffic must be allowed. Which two items must you configure to prevent this sever from triggering the incident? (Choose two.)

- A. Change the time window on the rule conditions.
- B. Modify the aggregate count in the subpattern.
- C. Create a rule exception for the IP address.
- D. Modify the subpattern filter to exclude the IP address.
- E. Modify the group by parameters to exclude the IP address.

Answer: C,D

Explanation:
To stop a known allowed server from generating this incident, you can tune the rule logic by excluding the server IP address in the subpattern filter. You can also create a rule exception for that IP address, which suppresses incident generation for matching traffic from the approved server while leaving the rule active for other sources.

NEW QUESTION # 56
Refer to the exhibit. Which event type attribute value will the FortiSIEM parser save for this event?

- A. phLogDetail
- B. PH_DEV_MON_SYS_UPTIME
- C. PHL_INFO
- D. sysUpTime

Answer: B

Explanation:
FortiSIEM parsers map raw event attributes to normalized event type attributes. In this event, the parser identifies the sysUpTime value and stores it under the normalized FortiSIEM attribute name PH_DEV_MON_SYS_UPTIME.

NEW QUESTION # 57
Refer to the exhibit.

Source IP	Reporting Device	Reporting IP	Event Type	User	Count
15.2.3.4	FW01	10.1.1.1	Logon	Mike	4
21.3.4.5	FW01	10.1.1.1	Logon	Bob	3
14.12.3.1	FW01	10.1.1.1	Logon	Alice	2
192.168.1.5	FW01	10.1.1.1	Logon	Alice	2
10.1.1.1	FW01	10.1.1.1	Logon	Bob	6
123.123.1.1	FW01	10.1.1.1	Logon	Mike	5

If you group the events by User and Count attributes, how many results will FortiSIEM display?

- A. Two
- B. Three
- C. Five
- D. Six
- E. One

Answer: C

Explanation:
The verified answer is D. Five . FortiSIEM grouping is based on unique combinations of the selected Group By fields. The Study Guide explains this behavior clearly: if multiple events have the same selected Group By values, "they are grouped together in one row," and the count column tracks the number of events for each row. In this question, the selected fields are User and Count . The six raw rows contain these combinations:
Mike/4, Bob/3, Alice/2, Alice/2, Bob/6, and Mike/5. Because Alice/2 appears twice, those two rows are grouped into a single result. The remaining combinations are unique. So FortiSIEM displays five grouped results, not six. Six would be correct only if every row had a unique User-and-Count combination, or if grouping included another differentiating attribute such as Source IP. Since the question specifically groups only by User and Count, duplicate User/Count pairs collapse into one row. Therefore, the correct result count is five .

NEW QUESTION # 58
What can you use to send data to FortiSIEM for user and entity behavior analytics (UEBA)?

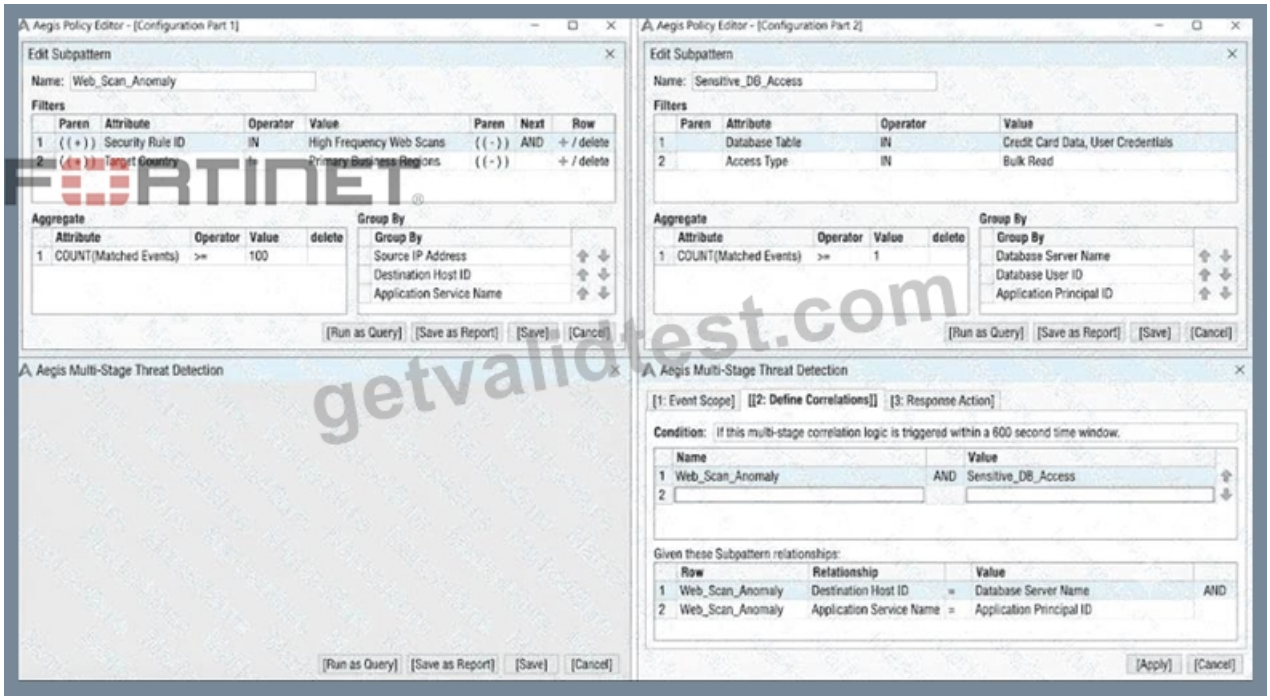
- A. SSH
- B. SNMP
- C. FortiSIEM worker
- D. FortiSIEM agent

Answer: D

Explanation:
The correct answer is A. FortiSIEM agent. The FortiSIEM Study Guide identifies FortiSIEM agents as the component responsible for "file, log monitoring, and UEBA." It also explains that FortiSIEM agents can be installed on endpoints or servers to provide data collection functions that native syslog may not provide. For Windows systems specifically, the guide states that Windows servers do not natively send syslog messages and that a FortiSIEM Windows agent can be installed to perform that function. The FortiSIEM 7.4 User Guide also confirms that FortiInsight UEBA functionality runs as an integrated module within the FortiSIEM Windows Agent in newer releases. SSH and SNMP are access or monitoring protocols; they can support discovery or performance monitoring, but they are not the UEBA data-sending component. A FortiSIEM worker performs analysis and search functions inside the FortiSIEM architecture; it is not installed on endpoints to collect UEBA telemetry. Therefore, the FortiSIEM agent is the correct mechanism for sending UEBA-relevant endpoint data to FortiSIEM.

NEW QUESTION # 59

Refer to the exhibits.



You are troubleshooting why the rule shown in the exhibit is generating incidents for successful Remote Desktop Protocol (RDP) connections with correct logins. It should only be triggering when a person fails to log in three or more times to the target device when connecting with RDP.
What is causing the rule to be triggered by correct login events? (Choose one answer)

- A. The RDP login is different from the login used to access the target device.
- B. The Boolean between the subpatterns is incorrect.
- C. The attribute types in the subpatterns do not match.
- D. The subpattern relationship RDP_Connection:User = Failed_Logon:User never matches.

Answer: B

Explanation:
The rule is triggering on successful RDP connection events because the Next operator between the two subpatterns is set to OR . The FortiSIEM Study Guide explains that multiple subpattern rules are used when patterns must occur within a specific time period or when one of several patterns proves that an incident condition exists. It lists the OR operator as: "Subpattern X OR Subpattern Y occurred within the Time Window." The same Study Guide further explains that if multiple patterns are used, FortiSIEM requires a next operator, and in the OR example, "an event that matches either" subpattern will trigger. It also states that because the next operator is OR, the constraint between the two subpatterns is not enforced.
In the exhibit, Subpattern 1 matches RDP traffic on TCP/UDP port 3389 from FortiGate traffic- forward events, while Subpattern 2 matches logon failure events with COUNT(Matched Events) > = 3.
Because the rule uses OR, FortiSIEM can trigger when only the RDP connection subpattern matches, even if the failed-logon subpattern does not match. The correct logic should require both subpatterns to match with the intended relationship constraints, not either subpattern independently.

NEW QUESTION # 60
.....

NSE6_FSM_AN-7.4 Format

- 2026 NSE6_FSM_AN-7.4 – 100% Free Valid Exam Syllabus | Professional Fortinet NSE 6 - FortiSIEM 7.4 Analyst Latest Demo □ Open website □ www.pdfvce.com □ and search for □ NSE6_FSM_AN-7.4 □ for free download □ □NSE6_FSM_AN-7.4 Lab Questions
- Free PDF Quiz 2026 NSE6_FSM_AN-7.4: Fortinet NSE 6 - FortiSIEM 7.4 Analyst Newest Valid Exam Syllabus □ Easily obtain ➤ NSE6_FSM_AN-7.4 □ for free download through ➤ www.testkingpass.com □ □New NSE6_FSM_AN-7.4 Braindumps Pdf
- Real NSE6_FSM_AN-7.4 Questions With Free Updates – Start Exam Preparation Today □ Search for " NSE6_FSM_AN-7.4 " and download exam materials for free through ⇛ www.pdfvce.com ⇚ □Test NSE6_FSM_AN-7.4 Guide
- Quiz 2026 Fortinet NSE6_FSM_AN-7.4 Perfect Valid Exam Syllabus □ Search for □ NSE6_FSM_AN-7.4 □ and download exam materials for free through ➡ www.prepawaypdf.com □□□ 🈸NSE6_FSM_AN-7.4 Lab Questions
- 2026 NSE6_FSM_AN-7.4 – 100% Free Valid Exam Syllabus | Professional Fortinet NSE 6 - FortiSIEM 7.4 Analyst Latest Demo □ Search for ➥ NSE6_FSM_AN-7.4 □ and download it for free on □ www.pdfvce.com □ website □ □Test NSE6_FSM_AN-7.4 Guide
- 2026 NSE6_FSM_AN-7.4 – 100% Free Valid Exam Syllabus | Professional Fortinet NSE 6 - FortiSIEM 7.4 Analyst Latest Demo □ Search for ▹ NSE6_FSM_AN-7.4 ◃ and obtain a free download on □ www.troytecdumps.com □ □ □Valid NSE6_FSM_AN-7.4 Test Preparation
- Reliable NSE6_FSM_AN-7.4 Test Question □ Exam NSE6_FSM_AN-7.4 Cram □ Exam NSE6_FSM_AN-7.4 Objectives Pdf □ Easily obtain ▹ NSE6_FSM_AN-7.4 ◃ for free download through " www.pdfvce.com " □Reliable NSE6_FSM_AN-7.4 Real Test
- Test NSE6_FSM_AN-7.4 Guide □ Reliable NSE6_FSM_AN-7.4 Real Test □ Free NSE6_FSM_AN-7.4 Download Pdf □ Search for ⇛ NSE6_FSM_AN-7.4 ⇚ on " www.examcollectionpass.com " immediately to obtain a free download □Free NSE6_FSM_AN-7.4 Download Pdf
- Reliable NSE6_FSM_AN-7.4 Test Question □ Exam NSE6_FSM_AN-7.4 Objectives Pdf □ Exam NSE6_FSM_AN-7.4 Cram □ Go to website ✔ www.pdfvce.com □✔□ open and search for ➥ NSE6_FSM_AN-7.4 □ to download for free □Exam NSE6_FSM_AN-7.4 Cram
- Real NSE6_FSM_AN-7.4 Questions With Free Updates – Start Exam Preparation Today □ Easily obtain ➽ NSE6_FSM_AN-7.4 □ for free download through 【 www.prep4sures.top 】 □NSE6_FSM_AN-7.4 New Cram Materials
- blogfreely.net, jobs.electronicsweekly.com, pastebin.com, scalar.usc.edu, fortunetelleroracle.com, dorahacks.io, p.me-page.com, wefunder.com, fortunetelleroracle.com, fortunetelleroracle.com, Disposable vapes