

Real Fortinet NSE5_FSM-6.3 Questions Formats - Prepare Better For Exam

Fortinet NSE5_FSM-6.3 Practice Questions

Fortinet NSE 5 - FortISIM 6.3

Order our NSE5_FSM-6.3 Practice Questions Today and Get Ready to Pass with Flying Colors!



NSE5_FSM-6.3 Practice Exam Features | QuestionsTube

- Latest & Updated Exam Questions
- Subscribe to FREE Updates
- Both PDF & Exam Engine
- Download Directly Without Waiting

https://www.questiontube.com/exam/nse5_fsm-6-3/

At QuestionsTube, you can read NSE5_FSM-6.3 free demo questions in pdf file, so you can check the questions and answers before deciding to download the Fortinet NSE5_FSM-6.3 practice questions. These free demo questions are parts of the NSE5_FSM-6.3 exam questions. Download and read them carefully, you will find that the NSE5_FSM-6.3 test questions of QuestionsTube will be your great learning materials online. Share some NSE5_FSM-6.3 exam online questions below.

BTW, DOWNLOAD part of TroytecDumps NSE5_FSM-6.3 dumps from Cloud Storage: <https://drive.google.com/open?id=1OALi8RtpptlQ9l3cDhN4v-rD0nO1yjfe>

If you choose to buy our NSE5_FSM-6.3 study pdf torrent, it is no need to purchase anything else or attend extra training. We promise you can pass your NSE5_FSM-6.3 actual test at first time with our Fortinet free download pdf. NSE5_FSM-6.3 questions and answers are created by our certified senior experts, which can ensure the high quality and high pass rate. In addition, you will have access to the updates of NSE5_FSM-6.3 Study Material for one year after the purchase date.

Through many people complain that it is hard for searching a job. But If you get an excellent certification (with NSE5_FSM-6.3 new test collection materials), you may be took as a skilled engineer. There is increasing demand for all kinds of senior R & D engineer in each link of internet, website, soft, App. Fortinet NSE5_FSM-6.3 new test collection materials will be a stepping-stone to success; you will have a good job with good prospects for development.

>> New NSE5_FSM-6.3 Exam Price <<

Fortinet NSE5_FSM-6.3 Cost Effective Dumps | NSE5_FSM-6.3 Exam Practice

With the simulation function, our NSE5_FSM-6.3 training guide is easier to understand and have more vivid explanations to help

you learn more knowledge. You can set time to test your study efficiency, so that you can accomplish your test within the given time when you are in the Real NSE5_FSM-6.3 Exam. Besides, you can get the real feeling of taking part in the real exam for our NSE5_FSM-6.3 exam questions have the function of simulating the real exam. So that you can have a better performance when you attend the real exam.

Fortinet NSE5_FSM-6.3 (Fortinet NSE 5 - FortiSIEM 6.3) Exam is a certification test designed to validate the knowledge and skills of security professionals in implementing and managing FortiSIEM 6.3. NSE5_FSM-6.3 Exam aims to equip candidates with the technical expertise needed to monitor and analyze security events, detect threats, and respond to security incidents in real-time.

Fortinet NSE 5 - FortiSIEM 6.3 Sample Questions (Q34-Q39):

NEW QUESTION # 34

Refer to the exhibit.

Event Receive Time	Reporting IP	Event Type	User	Source IP	Application Category
09:12:11	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App
09:12:56	10.10.10.11	Failed Logon	John	5.5.5.5	DB
09:15:56	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App
09:20:01	10.10.10.10	Failed Logon	Paul	3.3.2.1	Web App
10:10:43	10.10.10.11	Failed Logon	Ryan	1.1.1.15	DB
10:45:08	10.10.10.11	Failed Logon	Wendy	1.1.1.6	DB
11:23:33	10.10.10.10	Failed Logon	Ryan	1.1.1.15	DB
12:05:52	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App

If events are grouped by Reporting IP, Event Type, and user attributes in FortiSIEM, how many results will be displayed?

- A. There results will be displayed.
- **B. Seven results will be displayed.**
- C. Unique attribute cannot be grouped.
- D. Five results will be displayed.

Answer: B

Explanation:

Grouping Events: Grouping events by specific attributes allows for the aggregation of similar events.

Grouping Criteria: For this question, events are grouped by "Reporting IP," "Event Type," and "User." Unique Combinations Analysis:

- * 10.10.10.10, Failed Logon, Ryan, 1.1.1.1, Web App
- * 10.10.10.11, Failed Logon, John, 5.5.5.5, DB
- * 10.10.10.10, Failed Logon, Ryan, 1.1.1.1, Web App(duplicate, counted as one unique result)
- * 10.10.10.10, Failed Logon, Paul, 3.3.2.1, Web App
- * 10.10.10.11, Failed Logon, Ryan, 1.1.1.15, DB
- * 10.10.10.11, Failed Logon, Wendy, 1.1.1.6, DB
- * 10.10.10.10, Failed Logon, Ryan, 1.1.1.15, DB

Result Calculation: There are seven unique combinations based on the specified grouping attributes.

References: FortiSIEM 6.3 User Guide, Event Management and Reporting sections, explaining how events are grouped and reported based on selected attributes.

NEW QUESTION # 35

How is a subpattern for a rule defined?

- A. Filters, Aggregation, Group by definitions
- B. Filters, Group By definitions, Threshold
- **C. Filters, Threshold, Time Window definitions**
- D. Filters, Aggregation, Time Window definitions

Answer: C

NEW QUESTION # 36

Which statement about global thresholds and per device thresholds is true?

- A. FortiSIEM uses fixed hardcoded thresholds for all performance metrics.
- B. FortiSIEM uses global thresholds for all security metrics.
- **C. FortiSIEM uses global and per device thresholds for all performance metrics.**
- D. FortiSIEM uses global thresholds for all performance metrics.

Answer: C

Explanation:

* Threshold Management: FortiSIEM uses thresholds to generate alerts and incidents based on performance and security metrics.

* Global Thresholds: These are default thresholds applied to all devices and metrics across the system, providing a baseline for alerts.

* Per Device Thresholds: These thresholds can be customized for individual devices, allowing for more granular control and tailored monitoring based on specific device characteristics and requirements.

* Usage in Performance Metrics: Both global and per device thresholds are used for performance metrics to ensure comprehensive and precise monitoring.

* Reference: FortiSIEM 6.3 User Guide, Thresholds and Alerts section, details the application of global and per device thresholds for performance and security metrics.

NEW QUESTION # 37

In FortiSIEM enterprise licensing mode, if the link between the collector and data center FortiSIEM cluster is down what happens?

- **A. The collector buffers events**
- B. The collector processes stop, and events are dropped
- C. The collector drops incoming events like syslog, but stops performance collection
- D. The collector continues performance collection of devices, but stops receiving syslog

Answer: A

NEW QUESTION # 38

Which FortiSIEM components are capable of performing device discovery?

- A. Worker
- B. FortiSIEM Windows agent
- **C. Collector**
- D. FortiSIEM Linux agent

Answer: C

NEW QUESTION # 39

.....

The Fortinet NSE5_FSM-6.3 desktop practice exam software simulates a real test environment and familiarizes you with the actual test format. This Fortinet NSE5_FSM-6.3 practice exam software tracks your progress and performance, allowing you to see how much you've improved over time. We frequently update the Fortinet NSE5_FSM-6.3 Practice Exam software with the latest Fortinet NSE5_FSM-6.3 DUMPS PDF.

NSE5_FSM-6.3 Cost Effective Dumps: https://www.troytecdumps.com/NSE5_FSM-6.3-troytec-exam-dumps.html

- NSE5_FSM-6.3 Pass Leader Dumps NSE5_FSM-6.3 Dumps Discount NSE5_FSM-6.3 Pass Guide Immediately open www.prepawaypdf.com and search for NSE5_FSM-6.3 to obtain a free download NSE5_FSM-6.3 Actual Test Pdf
- Free PDF New NSE5_FSM-6.3 Exam Price | Perfect NSE5_FSM-6.3 Cost Effective Dumps: Fortinet NSE 5 - FortiSIEM 6.3 Open [www.pdfvce.com] enter NSE5_FSM-6.3 and obtain a free download NSE5_FSM-6.3 Valid Exam Tutorial
- Free PDF New NSE5_FSM-6.3 Exam Price | Perfect NSE5_FSM-6.3 Cost Effective Dumps: Fortinet NSE 5 - FortiSIEM

