New NSE5_FSM-6.3 Exam Topics & NSE5_FSM-6.3 Actual Dumps

BTW, DOWNLOAD part of NewPassLeader NSE5_FSM-6.3 dumps from Cloud Storage: https://drive.google.com/open?id=1NtHmH0G9Quip3g8Gcp_0kpkDqcyDCXUP

The cost of registering a Fortinet NSE5_FSM-6.3 certification is quite expensive, ranging between $100 and $1000. After paying such an amount, the candidate is sure to be on a tight budget. NewPassLeader provides Fortinet NSE5_FSM-6.3 preparation material at very low prices compared to other platforms. We also assure you that the amount will not be wasted and you will not have to pay for the certification a second time. For added reassurance, we also provide up to 1 year of free updates. Free demo version of the actual product is also available so that you can verify its validity before purchasing. The key to passing the NSE5_FSM-6.3 Exam on the first try is vigorous practice. And that's exactly what you'll get when you prepare from our material. Each format excels in its own way and helps you get success on the first attempt.

Fortinet NSE5_FSM-6.3 Certification Exam is administered by Pearson VUE, a leading provider of computer-based testing services. NSE5_FSM-6.3 exam is available in multiple languages, including English, Chinese, French, German, Italian, Japanese, Korean, Portuguese, Russian, Spanish, and Turkish.

>> New NSE5_FSM-6.3 Exam Topics <<

100% Pass-Rate New NSE5_FSM-6.3 Exam Topics & Leading Offer in Qualification Exams & Fantastic NSE5_FSM-6.3: Fortinet NSE 5 -

FortiSIEM 6.3

Do you want to find a job that really fulfills your ambitions? That's because you haven't found an opportunity to improve your ability to lay a solid foundation for a good career. Our NSE5_FSM-6.3 quiz torrent can help you get out of trouble regain confidence and embrace a better life. Our NSE5_FSM-6.3 Exam Question can help you learn effectively and ultimately obtain the authority certification of Fortinet, which will fully prove your ability and let you stand out in the labor market. We have the confidence and ability to make you finally have rich rewards.

Fortinet NSE5_FSM-6.3 certification exam is an excellent way to validate your skills and knowledge in the field of network security. Fortinet NSE 5 - FortiSIEM 6.3 certification program is designed to test your practical skills and knowledge in deploying and managing Fortinet's network security solutions. Fortinet NSE 5 - FortiSIEM 6.3 certification program is highly recognized globally and is an excellent way to enhance your career prospects. If you are looking to enhance your skills and knowledge in network security, the Fortinet NSE5_FSM-6.3 Certification program is an excellent choice.

Fortinet NSE 5 - FortiSIEM 6.3 Sample Questions (Q54-Q59):

NEW QUESTION # 54
Three events are collected over a 10-minutc time period from two servers Server A and Server B.
Based on the settings being used for the rule subpattern. how many incidents will the servers generate?

- A. Server A will not generate any incidents and Server B will not generate any incidents
- B. Server A will generate one incident and Server 8 will generate one incident
- C. Server B will generate one incident and Server A will not generate any incidents
- D. Server A will generate one incident and Server 8 will not generate any incidents

Answer: D

NEW QUESTION # 55
Refer to the exhibit.
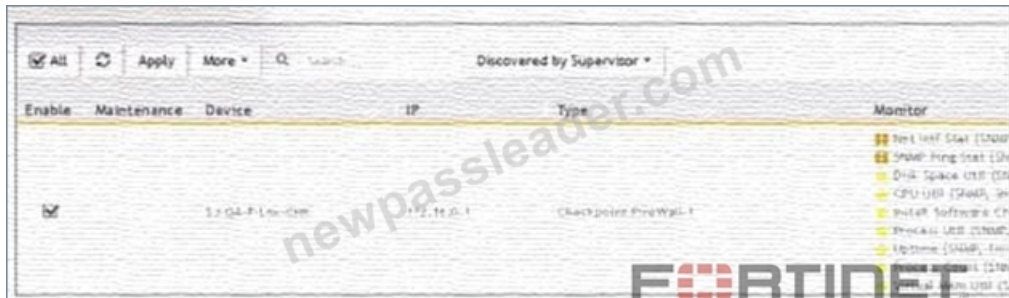
What does the pauso icon indicate?

- A. Data collection is paused duo to an issue, such as a change of password.
- B. Data collection has not started.
- C. Data collection execution failed because the device is not reachable.
- D. Data collection is paused after the intervals shown for metrics.

Answer: A

Explanation:
Data Collection Status: FortiSIEM displays various icons to indicate the status of data collection for different devices.
Pause Icon: The pause icon specifically indicates that data collection is paused, but this can happen due to several reasons.
Common Cause for Pausing: One common cause for pausing data collection is an issue such as a change of password, which prevents the system from authenticating and collecting data.
Exhibit Analysis: In the provided exhibit, the presence of the pause icon next to the device suggests that data collection has encountered an issue that has caused it to pause.
References: FortiSIEM 6.3 User Guide, Device Management and Data Collection Status Icons section, which explains the different icons and their meanings.

NEW QUESTION # 56

What are the four categories of incidents?

- A. Performance, devices, high risk, and low risk
- B. Devices, users, high risk, and low risk
- C. Security, change, high risk, and low risk
- D. Performance, availability, security, and change

Answer: D

Explanation:
* Incident Categories in FortiSIEM: Incidents in FortiSIEM are categorized to help administrators quickly identify and prioritize the type of issue.
* Four Main Categories:
Performance: Incidents related to the performance of devices and applications, such as high CPU usage or memory utilization.
Availability: Incidents affecting the availability of services or devices, such as downtime or connectivity issues.
Security: Incidents related to security events, such as failed login attempts, malware detection, or unauthorized access.
Change: Incidents triggered by changes in the configuration or state of devices, such as new software installations or configuration modifications.
* Importance of Categorization: These categories help in the efficient management and response to different types of incidents, allowing for better resource allocation and quicker resolution.
* Reference: FortiSIEM 6.3 User Guide, Incident Management section, which details the different categories of incidents and their significance.

NEW QUESTION # 57
Which process converts raw log data to structured data?

- A. Data classification
- B. Data validation
- C. Data enrichment
- D. Data parsing

Answer: D

Explanation:
Raw Log Data: When devices send logs to FortiSIEM, the data arrives in a raw, unstructured format.
Data Parsing Process: The process that converts this raw log data into a structured format is known as data parsing.
* Data Parsing: This involves extracting relevant fields from the raw log entries and organizing them into
* a structured format, making the data usable for analysis, reporting, and correlation.
Significance of Structured Data: Structured data is essential for effective event correlation, alerting, and generating meaningful reports.
References: FortiSIEM 6.3 User Guide, Data Parsing section, which details how raw log data is transformed into structured data through parsing.

NEW QUESTION # 58
An administrator defines SMTP as a critical process on a Linux server.
It the SMTP process is stopped. FortiSIEM will generate a critical event with which event type?

- A. PH_DEV_MON_PROC_STOP
- B. Postfix-Mail-Stop
- C. Generic_SMTP_Procoss_Exit
- D. PH_DEV_MON_SMTP_STOP

Answer: A

Explanation:
* Process Monitoring in FortiSIEM: FortiSIEM can monitor critical processes on managed devices, such as an SMTP process on a Linux server.
* Event Generation: When a critical process stops, FortiSIEM generates an event to alert administrators.
* Event Types: Specific event types correspond to different monitored conditions. For a stopped process, the event type

PH_DEV_MON_PROC_STOP is used.
* Reasoning: The name PH_DEV_MON_PROC_STOP (Device Monitoring Process Stop) is a generic event type used by FortiSIEM to indicate that any monitored process, including SMTP, has stopped.
* Reference: FortiSIEM 6.3 User Guide, Event Types section, explains the predefined event types and their usage in different monitoring scenarios.

NEW QUESTION # 59

......