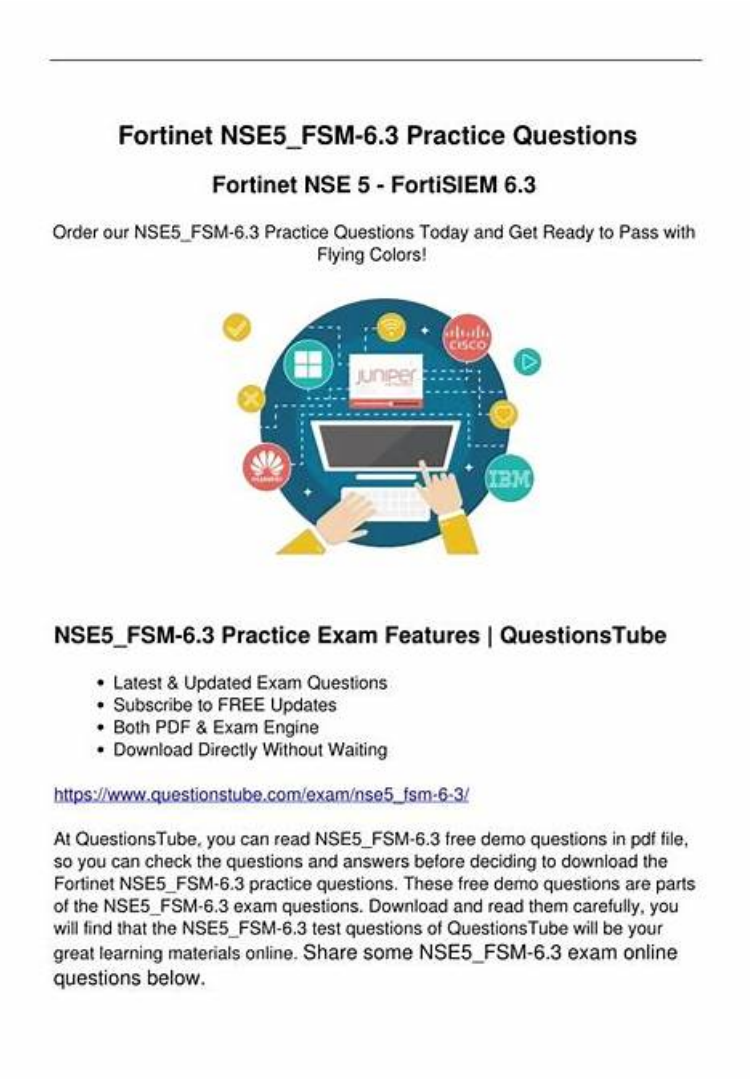
Latest NSE5_FSM-6.3 Exam Topic for Real Exam



BONUS!!! Download part of Dumpcollection NSE5_FSM-6.3 dumps for free: https://drive.google.com/open?id=1jJFl0_UOHH5juaRFxnWP7GrQHFDc6Tsz

In fact, in real life, we often use performance of high and low to measure a person's level of high or low, when we choose to find a good job, there is important to get the NSE5_FSM-6.3 certification as you can. Our product is elaborately composed with major questions and answers. We are choosing the key from past materials to finish our NSE5_FSM-6.3 Guide question. It only takes you 20 hours to 30 hours to do the practice. After your effective practice, you can master the examination point from the NSE5_FSM-6.3 test question. Then, you will have enough confidence to pass it.

Fortinet NSE5_FSM-6.3 exam is designed to test the knowledge and skills of IT professionals in deploying and managing Fortinet FortiSIEM 6.3 solutions. Fortinet FortiSIEM is a comprehensive security information and event management (SIEM) solution that provides real-time visibility into security events and threats across an organization's entire infrastructure. The NSE5_FSM-6.3 Exam covers topics such as configuring and deploying FortiSIEM, managing security events, creating custom dashboards, and using FortiSIEM for compliance reporting.

>> NSE5_FSM-6.3 Exam Topic <<

Free PDF Quiz Newest Fortinet - NSE5_FSM-6.3 - Fortinet NSE 5 - FortiSIEM 6.3 Exam Topic

Likewise, Web-Based Fortinet NSE5_FSM-6.3 exam questions are supported by all the major browsers like Chrome, Opera, Safari, Firefox, and IE. In the same way, the Web-based Fortinet NSE 5 - FortiSIEM 6.3 pdf exam requires no special plugin. Lastly, the web-based Fortinet NSE 5 - FortiSIEM 6.3 (NSE5_FSM-6.3) practice exam is customizable and requires an active Internet connection.

Fortinet NSE5_FSM-6.3 certification exam is designed for IT professionals who wish to validate their knowledge and skills in FortiSIEM, a cybersecurity solution offered by Fortinet. FortiSIEM is a comprehensive platform that provides real-time monitoring, analysis, and reporting of security and performance data across an organization's IT infrastructure. NSE5_FSM-6.3 Exam Tests candidates on their ability to deploy, configure, and administer FortiSIEM, as well as their understanding of the product's features and capabilities.

Fortinet NSE 5 - FortiSIEM 6.3 Sample Questions (Q52-Q57):

NEW QUESTION # 52
Which is a requirement for implementing FortiSIEM disaster recovery?

- A. All worker nodes must access both supervisor nodes using IP.
- B. DNS names must be used for the worker upload addresses.
- C. SNMP, and WMI ports must be open between the two supervisor nodes.
- D. The two supervisor nodes must have layer 2 connectivity.

Answer: D

Explanation:
Disaster Recovery (DR) Implementation: For FortiSIEM to effectively support disaster recovery, specific requirements must be met to ensure seamless failover and data integrity.
Layer 2 Connectivity: One of the critical requirements for implementing FortiSIEM DR is that the two supervisor nodes must have layer 2 connectivity.
* Layer 2 Connectivity: This ensures that the supervisors can communicate directly at the data link layer, which is necessary for synchronous data replication and other DR processes.
Importance of Connectivity: Layer 2 connectivity between the supervisor nodes ensures that they can maintain consistent and up-to-date state information, which is essential for a smooth failover in the event of a disaster.
References: FortiSIEM 6.3 Administration Guide, Disaster Recovery section, which details the requirements and configurations needed for setting up disaster recovery, including the necessity for layer 2 connectivity between supervisor nodes.

NEW QUESTION # 53
How is a subpattern for a rule defined?

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

Answer: B

NEW QUESTION # 54
If a performance rule is triggered repeatedly due to high CPU use, what occurs in the incident table?

- A. A now incident is created each time the rule is triggered. and the First Seen and Last Seen times are updated.
- B. The Incident Count value increases, and the First Seen and Last Seen times update.
- C. A new incident is created based on the Rule Frequency value, and the First Seen and Last Seen times ate updated.
- D. The incident status changes to Repeated, and the First Seen and Last Seen times are updated.

Answer: B

Explanation:
Incident Management in FortiSIEM: FortiSIEM tracks incidents and their occurrences to help administrators manage and respond to recurring issues.
Performance Rule Triggering: When a performance rule, such as one for high CPU usage, is repeatedly triggered, FortiSIEM

updates the corresponding incident rather than creating a new one each time.
Incident Table Updates:
* Incident Count: The Incident Count value increases each time the rule is triggered, indicating how many times the incident has occurred.
* First Seen and Last Seen Times: These timestamps are updated to reflect the first occurrence and the most recent occurrence of the incident.
References: FortiSIEM 6.3 User Guide, Incident Management section, explains how FortiSIEM handles recurring incidents and updates the incident table accordingly.

NEW QUESTION # 55
IF the reported packet loss is between 50% and 98%. which status is assigned to the device in the Availability column of summary dashboard?

- A. Up status is assigned because of received packets.
- B. Degraded status is assigned because of packet loss
- C. Critical status is assigned because of reduction in number of packets received.
- D. Down status is assigned because of packet loss.

Answer: B

Explanation:
Device Status in FortiSIEM: FortiSIEM assigns different statuses to devices based on their operational state and performance metrics.
Packet Loss Impact: The reported packet loss percentage directly influences the status assigned to a device.
Packet loss between 50% and 98% indicates significant network issues that affect the device's performance.
Degraded Status: When packet loss is between 50% and 98%, FortiSIEM assigns a "Degraded" status to the device. This status indicates that the device is experiencing substantial packet loss, which impairs its performance but does not render it completely non-functional.
Reasoning: The "Degraded" status helps administrators identify devices with serious performance issues that need attention but are not entirely down.
References: FortiSIEM 6.3 User Guide, Device Availability and Status section, explains the criteria for assigning different statuses based on performance metrics such as packet loss.

NEW QUESTION # 56
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

It events are grouped by Event Type and User attributes in FortiSIEM. how many results will be displayed?

- A. No results will be displayed.
- B. Four results will be displayed.
- C. Eight results will be displayed.
- D. Two results will be displayed.

Answer: C

Explanation:

Grouping Events in FortiSIEM: Grouping events by specific attributes allows administrators to aggregate and analyze data more efficiently.
Grouping Criteria: In this case, the events are grouped by "Event Type" and "User" attributes.
Unique Combinations: To determine the number of results displayed, identify the unique combinations of the "Event Type" and "User" attributes in the provided data.
* Failed Logon by Ryan(appears multiple times but is one unique combination)
* Failed Logon by John
* Failed Logon by Paul
* Failed Logon by Wendy
Unique Groupings: There are four unique groupings based on the given data: "Failed Logon" by "Ryan", "John", "Paul", and "Wendy".
References: FortiSIEM 6.3 User Guide, Event Management and Reporting sections, which explain how events are grouped and reported based on selected attributes.

NEW QUESTION # 57
.....