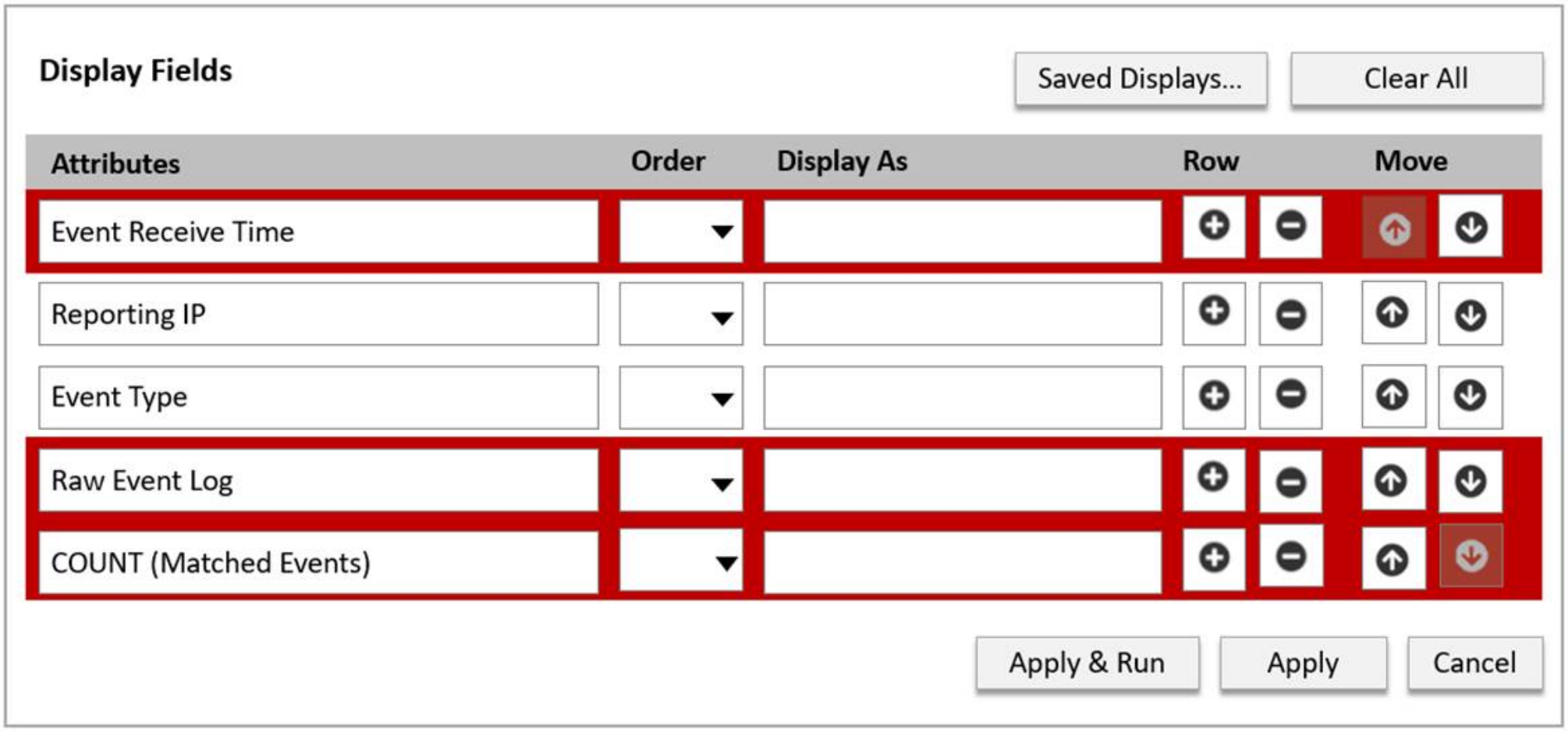
Fortinet

Exam Questions NSE5_FSM-6.3

Fortinet NSE 5 - FortiSIEM 6.3

NEW QUESTION 1
Refer to the exhibit.



A FortiSIEM administrator wants to group some attributes for a report, but is not able to do so successfully. As shown in the exhibit, why are some of the fields highlighted in red?

A. Unique attributes cannot be grouped.
B. The Event Receive Time attribute is not available for logs.
C. The attribute COUNT(Matched events) is an invalid expression.
D. No RAW Event Log attribute is available for devices.

Answer: A

Explanation:
The red highlighting in the exhibit indicates attributes that cannot be grouped together due to their unique nature. These unique attributes includeEvent Receive Time,Reporting IP,Event Type,Raw Event Log, andCOUNT(Matched Events).
Attribute Characteristics:

- Event Receive Timeis unique for each event.
- Reporting IPandEvent Typecan vary greatly, making grouping them impractical in this context.
- Raw Event Logrepresents the unprocessed log data, which is also unique.
- COUNT(Matched Events)is a calculated field, not suitable for grouping.

References: FortiSIEM 6.3 User Guide, Reporting section, explains the constraints on grouping attributes in reports.

NEW QUESTION 2
Which FortiSIEM components are capable of performing device discovery?

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

Answer: D

Explanation:
Explanation
Device Discovery in FortiSIEM: Device discovery is the process by which FortiSIEM identifies and adds devices to its management scope.
Role of Collectors: Collectors are responsible for gathering data from network devices, including discovering new devices in the network.

- Functionality: Collectors use protocols such as SNMP, WMI, and others to discover devices and gather their details.

Capability: While agents (Windows and Linux) primarily gather data from their host systems, the collectors actively discover devices across the network.
References: FortiSIEM 6.3 User Guide, Device Discovery section, which details the role of collectors in discovering network devices.

NEW QUESTION 3
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 triggere
B. and the First Seen and Last Seen times are updated.
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 Count value increases, and the First Seen and Last Seen times update.
E. The incident status changes to Repeated, and the First Seen and Last Seen times are updated.

Answer: C

Explanation:
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 4
Which command displays the Linux agent status?

A. Service fsm-linux-agent status
B. Service Ao-linux-agent status
C. Service fortisiem-linux-agent status
D. Service linux-agent status

Answer: C

Explanation:
Explanation
Linux Agent in FortiSIEM: The FortiSIEM Linux agent is responsible for collecting logs and metrics from Linux devices and forwarding them to the FortiSIEM system.
Command for Checking Status: The correct command to check the status of the FortiSIEM Linux agent isservice fortisiem-linux-agent status.
This command queries the status of the FortiSIEM Linux agent service, showing whether it is running, stopped, or encountering issues.
Usage: Properly checking the agent status helps ensure that data collection from Linux devices is functioning as expected.
References: FortiSIEM 6.3 User Guide, Linux Agent Installation and Management section, which includes commands for managing the Linux agent.

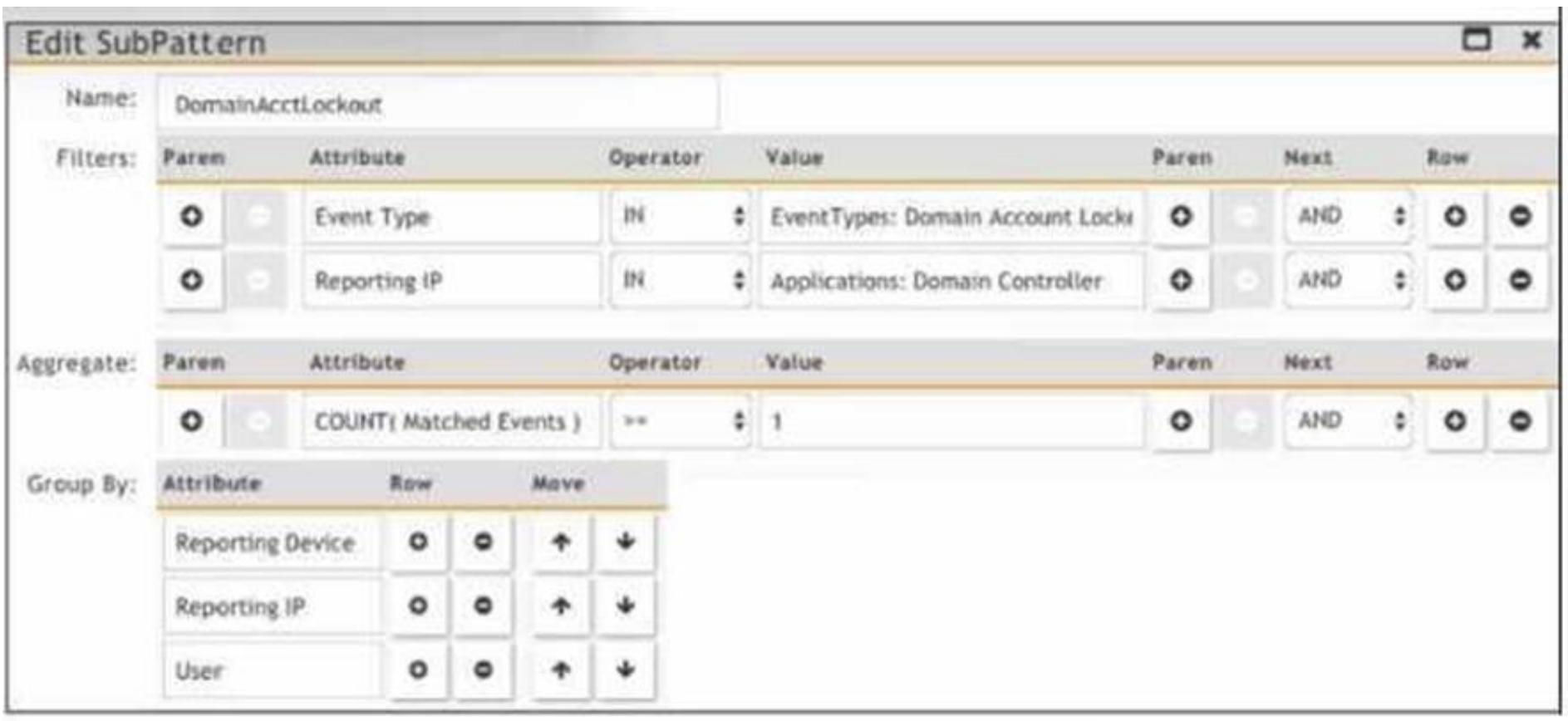
NEW QUESTION 5
When configuring collectors located in geographically separated sites, what ports must be open on a front end firewall?

A. HTTPS, from the collector to the worker upload settings address only
B. HTTPS, from the collector to the supervisor and worker upload settingsaddresses
C. HTTPS, from the Internet to the collector
D. HTTPS, from the Internet to the collector and from the collector to the FortiSIEM cluster

Answer: B

Explanation:
FortiSIEM Architecture: In FortiSIEM, collectors gather data from various sources and send this data to supervisors and workers within the FortiSIEM architecture.
Communication Requirements: For collectors to effectively send data to the FortiSIEM system, specific communication channels must be open.
Port Usage: The primary port used for secure communication between the collectors and the FortiSIEM infrastructure is HTTPS (port 443).
Network Configuration: When configuring collectors in geographically separated sites, the HTTPS port must be open for the collectors to communicate with both the supervisor and the worker upload settings addresses. This ensures that the collected data can be securely transmitted to the appropriate processing and analysis components.
References: FortiSIEM 6.3 Administration Guide, Network Ports section details the necessary ports for communication within the FortiSIEM architecture.

NEW QUESTION 6
Refer to the exhibit.



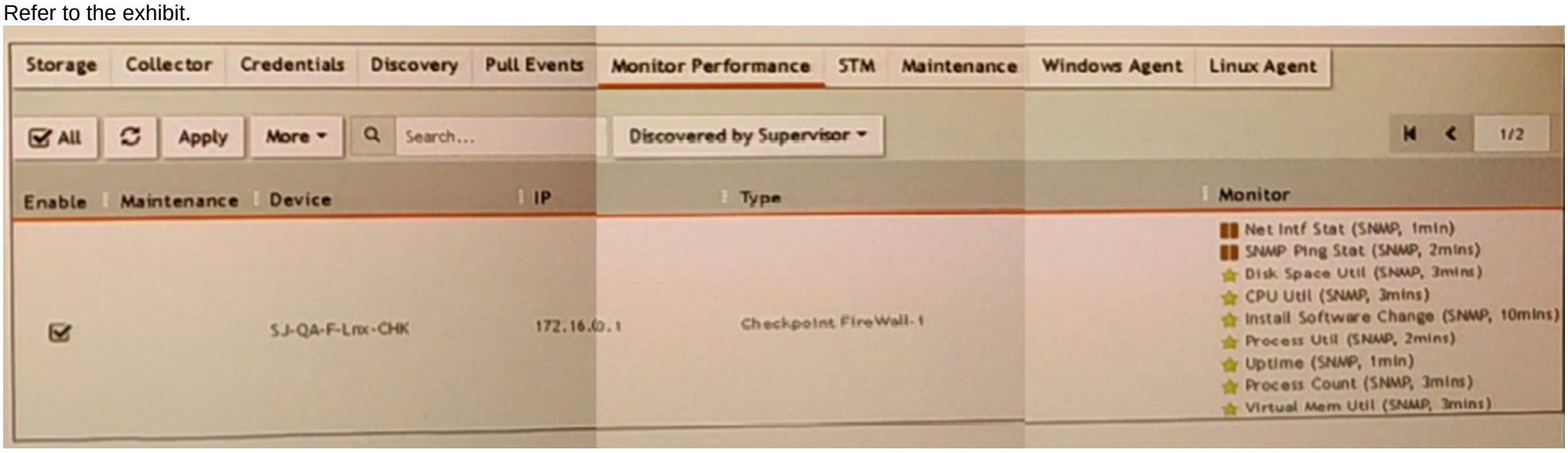
Which section contains the sortings that determine how many incidents are created?

A. Actions
B. Group By
C. Aggregate
D. Filters

Answer: B

Explanation:
Incident Creation in FortiSIEM: Incidents in FortiSIEM are created based on specific patterns and conditions defined within the system.
Group By Function: The "Group By" section in the "Edit SubPattern" window specifies how the data should be grouped for analysis and incident creation.
Impact of Grouping: The way data is grouped affects the number of incidents generated.
Each unique combination of the grouped attributes results in a separate incident.
Exhibit Analysis: In the provided exhibit, the "Group By" section lists "Reporting Device," "Reporting IP," and "User." This means incidents will be created for each unique combination of these attributes. References: FortiSIEM 6.3 User Guide, Rule and Pattern Creation section, which details how grouping impacts incident generation.

NEW QUESTION 7
Refer to the exhibit.



What do the yellow stars listed in the Monitor column indicate?

A. A yellow star indicates that a metric was applied during discovery, and data has been collected successfully
B. A yellow star indicates that a metric was applied during discovery, but data collection has not started
C. A yellow star indicates that a metric was applied during discovery, but FortiSIEM is unable to collect data.
D. A yellow star indicates that a metric was not applied during discovery and, therefore, FortiSEIM was unable to collect data.

Answer: A

Explanation:
Monitor Column Indicators: In FortiSIEM, the Monitor column displays the status of various metrics applied during the discovery process.
Yellow Star Meaning: A yellow star next to a metric indicates that the metric was successfully applied during
Successful Data Collection: This visual indicator helps administrators quickly identify which metrics are active and have data available for analysis.
References: FortiSIEM 6.3 User Guide, Device Monitoring section, which explains the significance of different icons and indicators in the Monitor column.

NEW QUESTION 8
An administrator wants to search for events received from Linux and Windows agents.
Which attribute should the administrator use in search filters, to view events received from agents only.

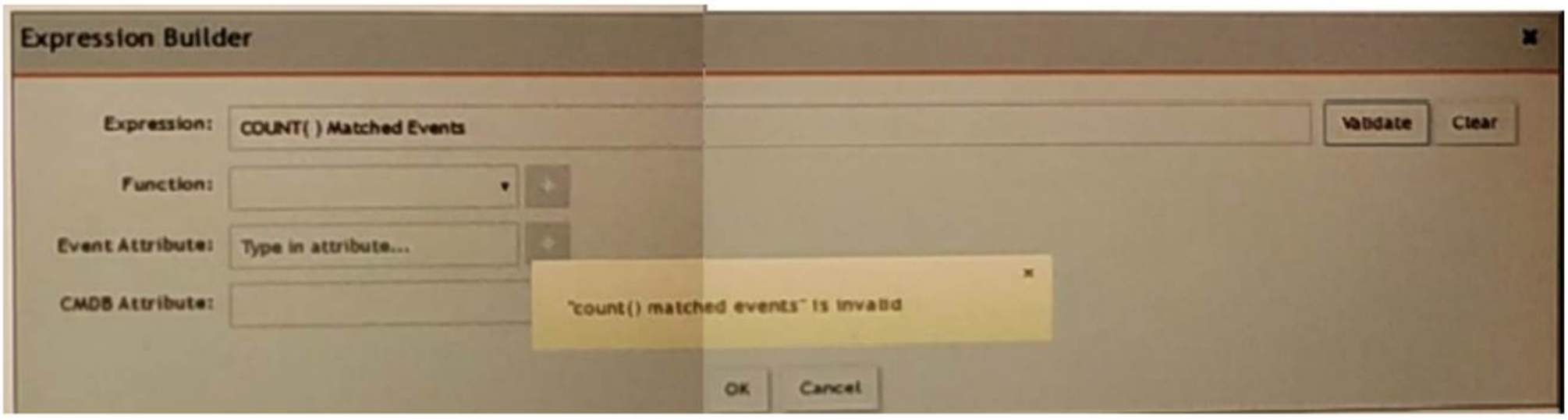
A. External Event Receive Protocol

B. Event Received Proto Agents
C. External Event Receive Raw Logs
D. External Event Receive Agents

Answer: D

Explanation:
Search Filters in FortiSIEM: When searching for specific events, administrators can use various attributes to filter the results.
Attribute for Agent Events: To view events received specifically from Linux and Windows agents, the attribute External Event Receive Agents should be used.
Function: This attribute filters events that are received from agents, distinguishing them from events received through other protocols or sources.
Search Efficiency: Using this attribute helps the administrator focus on events collected by FortiSIEM agents, making the search results more relevant and targeted.
References: FortiSIEM 6.3 User Guide, Event Search and Filters section, which describes the available attributes and their usage for filtering search results.

NEW QUESTION 9
Refer to the exhibit.



An administrator is trying to identify an issue using an expression bated on the Expression Builder settings shown in the exhibit however, the error message shown in the exhibit indicates that the expression is invalid.
Which is the correct expression?

A. Matched Events COUNT()
B. Matched Events(COUNT)
C. COUNT(Matched Events)
D. (COUNT) Matched Events

Answer: C

Explanation:
Expression Builder in FortiSIEM: The Expression Builder is used to create expressions for analyzing event data.
Correct Syntax: The correct syntax for counting matched events is COUNT(Matched Events).
Function: COUNT is a function that takes a parameter, in this case, 'Matched Events,' to count the number of occurrences.
Common Errors: Incorrect syntax, such as reversing the order or using parentheses improperly, can lead to invalid expressions.
References: FortiSIEM 6.3 User Guide, Expression Builder section, which explains the correct syntax and usage for creating valid expressions for event analysis.

NEW QUESTION 10
If an incident's status is Cleared, what does this mean?

A. Two hours have passed since the incident occurred and the incident has not reoccurred.
B. A clear condition set on a rule was satisfied.
C. A security rule issue has been resolved.
D. The incident was cleared by an operator.

Answer: B

Explanation:
Incident Status in FortiSIEM: The status of an incident indicates its current state and helps administrators track and manage incidents effectively.
Cleared Status: When an incident's status is 'Cleared,' it means that a specific condition set to clear the incident has been satisfied.
Clear Condition: This is typically a predefined condition that indicates the issue causing the incident has been resolved or no longer exists.
Automatic vs. Manual Clearance: While some incidents may be cleared automatically based on clear conditions, others might be manually cleared by an operator.
References: FortiSIEM 6.3 User Guide, Incident Management section, detailing the various incident statuses and the conditions that lead to an incident being marked as 'Cleared.'

NEW QUESTION 10
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. Seven results will be displayed.
B. There results will be displayed.
C. Unique attribute cannot be grouped.
D. Five results will be displayed.

Answer: A

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 14
Refer to the exhibit.

How was the FortiGate device discovered by FortiSIEM?

A. GUI log discovery
B. Syslog discovery
C. Pull events discovery
D. Auto log discovery

Answer: B

Explanation:
Discovery Methods in FortiSIEM: FortiSIEM can discover devices using various methods, including syslog, SNMP, and others. Syslog Discovery: The exhibit shows that the FortiGate device is discovered by FortiSIEM using syslog.
Syslog Parsing: The syslog messages sent by the FortiGate device are parsed by FortiSIEM to extract relevant information.
CMDB Entry: Based on the parsed information, an entry is populated in the Configuration Management Database (CMDB) for the device.
Evidence in Exhibit: The exhibit shows the syslog flow from the FortiGate Firewall to the parsing and discovery process, resulting in the device being listed in the CMDB with the status 'Pending.'

References: FortiSIEM 6.3 User Guide, Device Discovery section, which explains how syslog discovery works and how devices are added to the CMDB based on syslog data.

NEW QUESTION 17
Consider the storage of anomaly baseline date that is calculated for different parameters.
Which database is used for storing this data?

A. Event DB
B. Profile DB
C. SVN DB
D. CMDB

Answer: B

Explanation:
Anomaly Baseline Data: Anomaly baseline data refers to the statistical profiles and baselines calculated for various parameters to detect deviations indicative of potential security incidents.
Profile DB: The Profile DB is specifically designed to store such baseline data in FortiSIEM.
Purpose: It maintains statistical profiles for different monitored parameters to facilitate anomaly detection.
Usage: This data is used by FortiSIEM to compare real-time metrics against the established baselines to identify anomalies.
References: FortiSIEM 6.3 User Guide, Database Architecture section, which describes the different databases used in FortiSIEM and their purposes, including the Profile DB for storing anomaly baseline data.

NEW QUESTION 22
What does the Frequency field determine on a rule?

A. How often the rulewill evaluate the subpattern.
B. How often the rule will trigger for the same condition.
C. How often the rule will trigger.
D. How often the rule will take a clear action.

Answer: A

Explanation:
Rule Evaluation in FortiSIEM: Rules in FortiSIEM are evaluated periodically to check if the defined conditions or subpatterns are met.
Frequency Field: The Frequency field in a rule determines the interval at which the rule's subpattern will be evaluated.
Evaluation Interval: This defines how often the system will check the incoming events against the rule's subpattern to determine if an incident should be triggered.
Impact on Performance: Setting an appropriate frequency is crucial to balance between timely detection of incidents and system performance.
Examples:
If the Frequency is set to 5 minutes, the rule will evaluate the subpattern every 5 minutes.
This means that every 5 minutes, the system will check if the conditions defined in the subpattern are met by the incoming events.
References: FortiSIEM 6.3 User Guide, Rules and Incidents section, which explains the Frequency field and how it impacts the evaluation of subpatterns in rules.

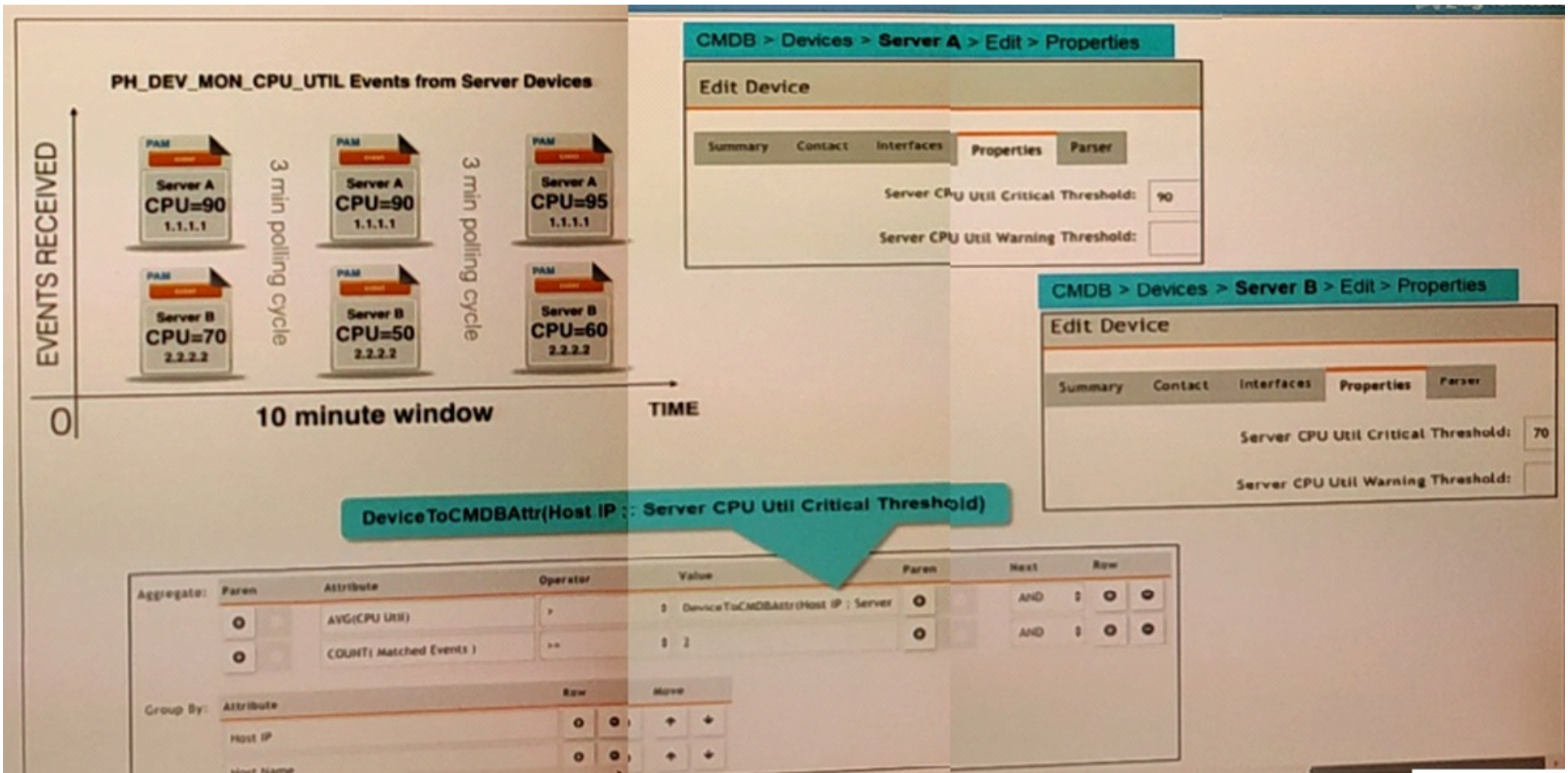
NEW QUESTION 24
IF the reported packet loss is between 50% and 98%. which status is assigned to the device in the Availability column of summary dashboard?

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

Answer: C

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 25
Refer to the exhibit.

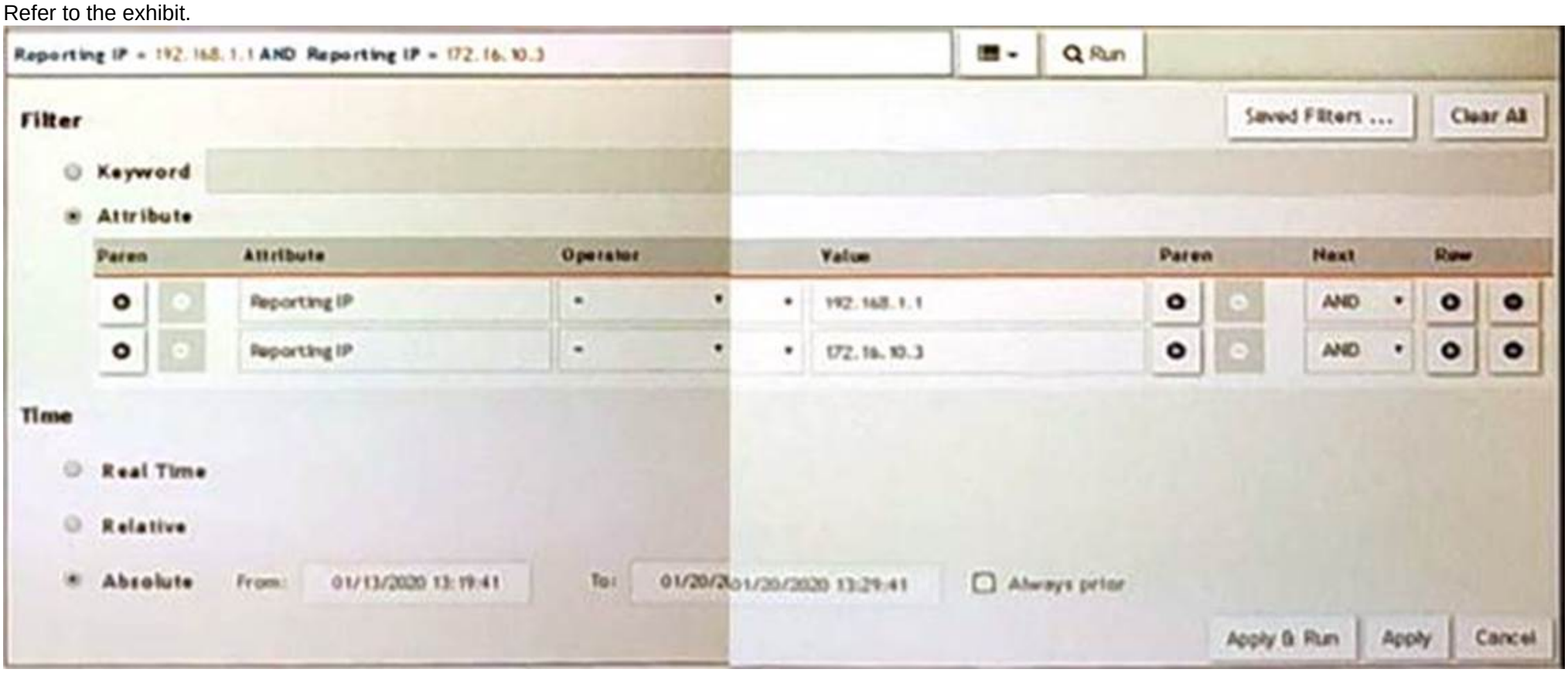


Three events are collected over a 10-minutc time period from two servers Server A and Server B. Based on the settings being used for the rule subpattern. how many incidents will the servers generate?

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

Answer: A

NEW QUESTION 28
Refer to the exhibit.



The FortiSIEM administrator is examining events for two devices to investigate an issue However, the administrator is not getting any results from their search. Based on the selected fillers shown in the exhibit, why is the search returning no results?

A. Parenthesis are missing
B. The wrong boolean operator is selected in the Next column
C. The wrong option is selected in the Operator column
D. An invalid IP subnet is typed in the Value column

Answer: B

NEW QUESTION 32
Which item is required to register a FortiSIEM appliance license?

A. Static storage
B. Static MAC address

C. Static IP address
D. Static Hardware ID

Answer: D

NEW QUESTION 34
To determine whether or not syslog is being received from a network device, which is the best command from the backend?

A. tcpdump
B. phDeviceTest
C. netcat
D. phSyslogRecorder

Answer: A

NEW QUESTION 36
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

NSE5_FSM-6.3 Practice Exam Features:

* NSE5_FSM-6.3 Questions and Answers Updated Frequently

* NSE5_FSM-6.3 Practice Questions Verified by Expert Senior Certified Staff

* NSE5_FSM-6.3 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE5_FSM-6.3 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year