# Fortinet

## Exam Questions NSE5_FSM-6.3

Fortinet NSE 5 - FortiSIEM 6.3

**NEW QUESTION 1**
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. Four results will be displayed.
B. Eight results will be displayed.
C. Two results will be displayed.
D. No results will be displayed.

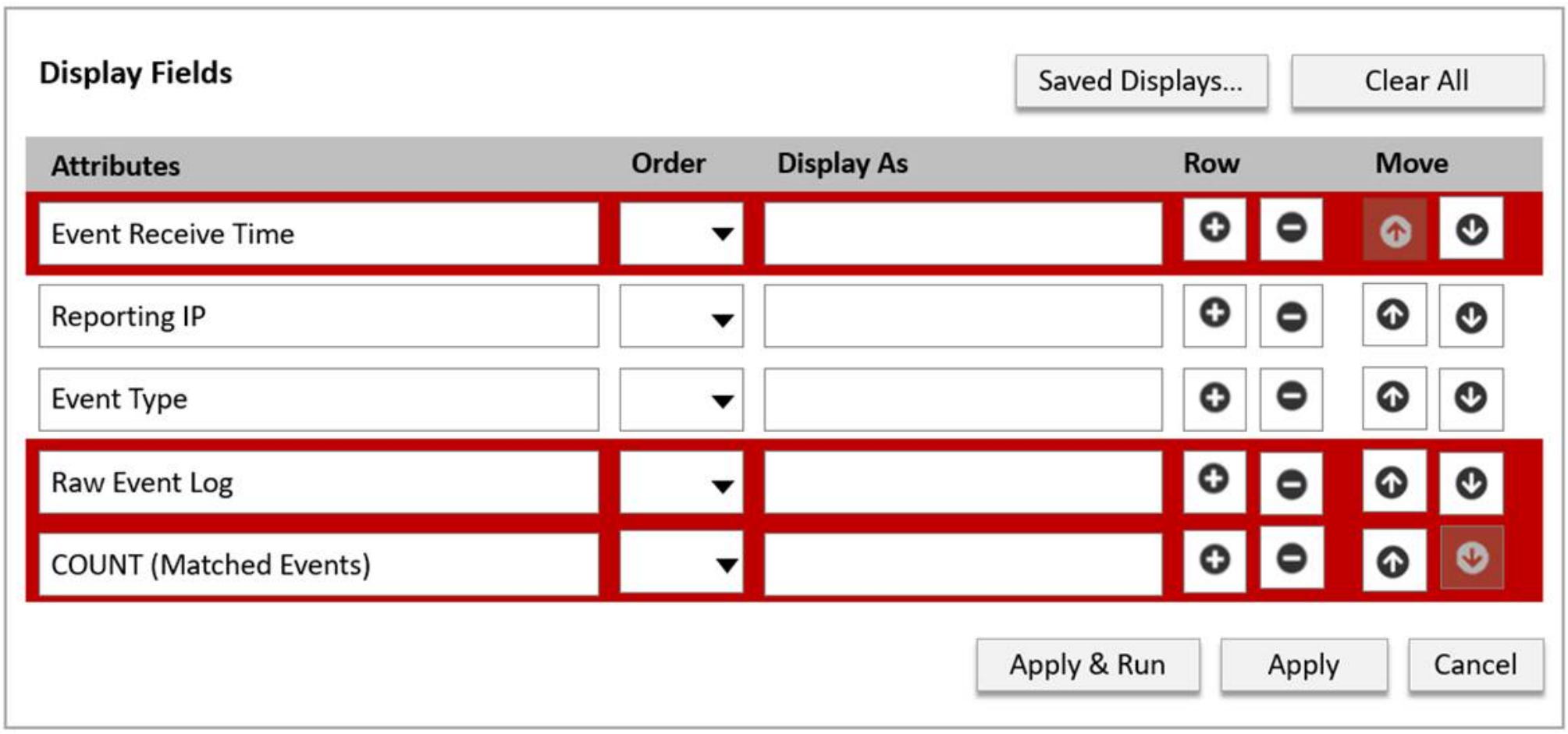
**Answer:** A

**Explanation:**
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 2**
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 3**
Which two FortiSIEM components work together to provide real-time event correlation?

A. Supervisor and worker
B. Collector and Windows agent
C. Worker and collector
D. Supervisor and collector

**Answer:** A

**Explanation:**
Explanation
FortiSIEM Architecture: The FortiSIEM architecture includes several components such as Supervisors, Workers, Collectors, and Agents, each playing a distinct role in the SIEM ecosystem.
Real-Time Event Correlation: Real-time event correlation is a critical function that involves analyzing and correlating incoming events to detect patterns indicative of security incidents or operational issues.
Role of Supervisor and Worker:

- Supervisor: The Supervisor oversees the entire FortiSIEM system, coordinating the processing and analysis of events.
- Worker: Workers are responsible for processing and correlating the events received from Collectors and Agents.

Collaboration for Correlation: Together, the Supervisor and Worker components perform real-time event correlation by distributing the load and ensuring efficient processing of events to identify incidents in
real-time.
References: FortiSIEM 6.3 User Guide, Event Correlation and Processing section, details how the Supervisor and Worker components collaborate for real-time event correlation.

**NEW QUESTION 4**
An administrator is using SNMP and WMI credentials to discover a Windows device. How will the WMI method handle this?

A. WMI method will collect only traffic and IIS logs.
B. WMI method will collect only DNS logs.
C. WMI method will collect only DHCP logs.
D. WMI method will collect security, application, and system events logs.

**Answer:** D

**Explanation:**
Explanation
WMI Method: Windows Management Instrumentation (WMI) is a set of specifications from Microsoft for consolidating the management of devices and applications in a network.
Log Collection: WMI is used to collect various types of logs from Windows devices.

- Security Logs: Contains records of security-related events such as login attempts and resource access.
- Application Logs: Contains logs generated by applications running on the system.
- System Logs: Contains logs related to the operating system and its components.

Comprehensive Data Collection: By using WMI, FortiSIEM can gather a wide range of event logs that are crucial for monitoring and analyzing the security and performance of Windows devices.
References: FortiSIEM 6.3 User Guide, Data Collection Methods section, which details the use of WMI for collecting event logs from Windows devices.

**NEW QUESTION 5**
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 6**
An administrator is in the process of renewing a FortiSIEM license. Which two commands will provide the system ID? (Choose two.)

A. phgetHWID
B. ./phLicenseTool - support
C. phgetUUID
D. ./phLicenseTool-show

**Answer:** AC

**Explanation:**
License Renewal Process: When renewing a FortiSIEM license, it is essential to provide the system ID, which uniquely identifies the FortiSIEM instance.
Commands to Retrieve System ID:
phgetHWID: This command retrieves the hardware ID of the FortiSIEM appliance.
Usage: Run the command phgetHWID in the CLI to obtain the hardware ID.
phgetUUID: This command retrieves the universally unique identifier (UUID) for the FortiSIEM system.
Usage: Run the command phgetUUID in the CLI to obtain the UUID.
Verification: Both phgetHWID and phgetUUID are valid commands for retrieving the necessary system IDs required for license renewal.
References: FortiSIEM 6.3 Administration Guide, Licensing section details the commands and procedures for obtaining system identification information necessary for license renewal.

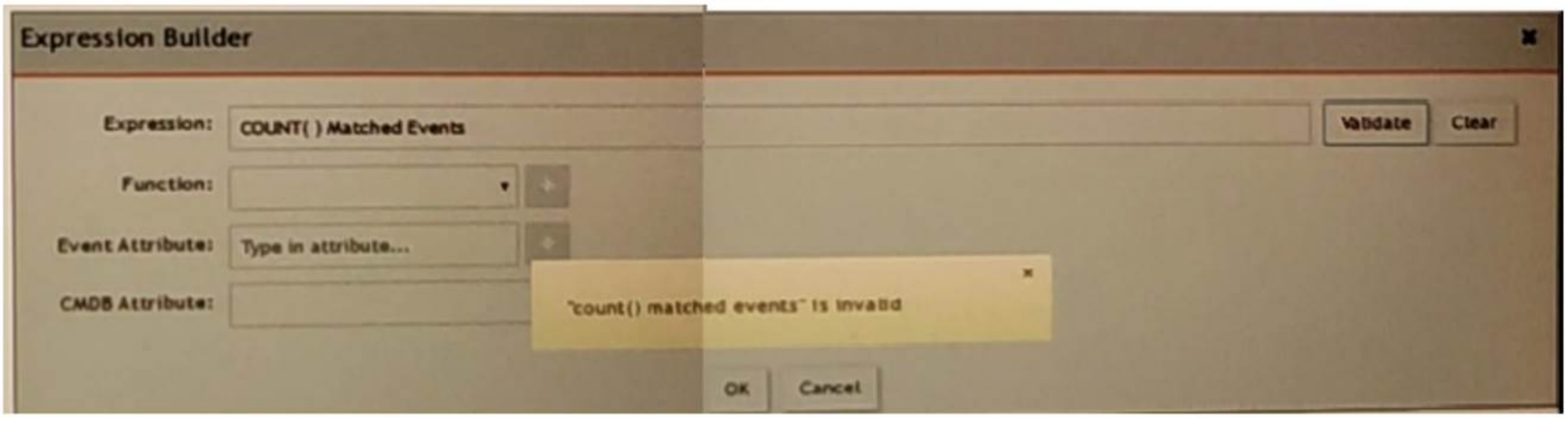
**NEW QUESTION 7**
An administrator wants to search for events received from Linux and Windows agents.
Which attribute should the administrator use in search filters, to view events received from agents only.

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 8**
Refer to the exhibit.



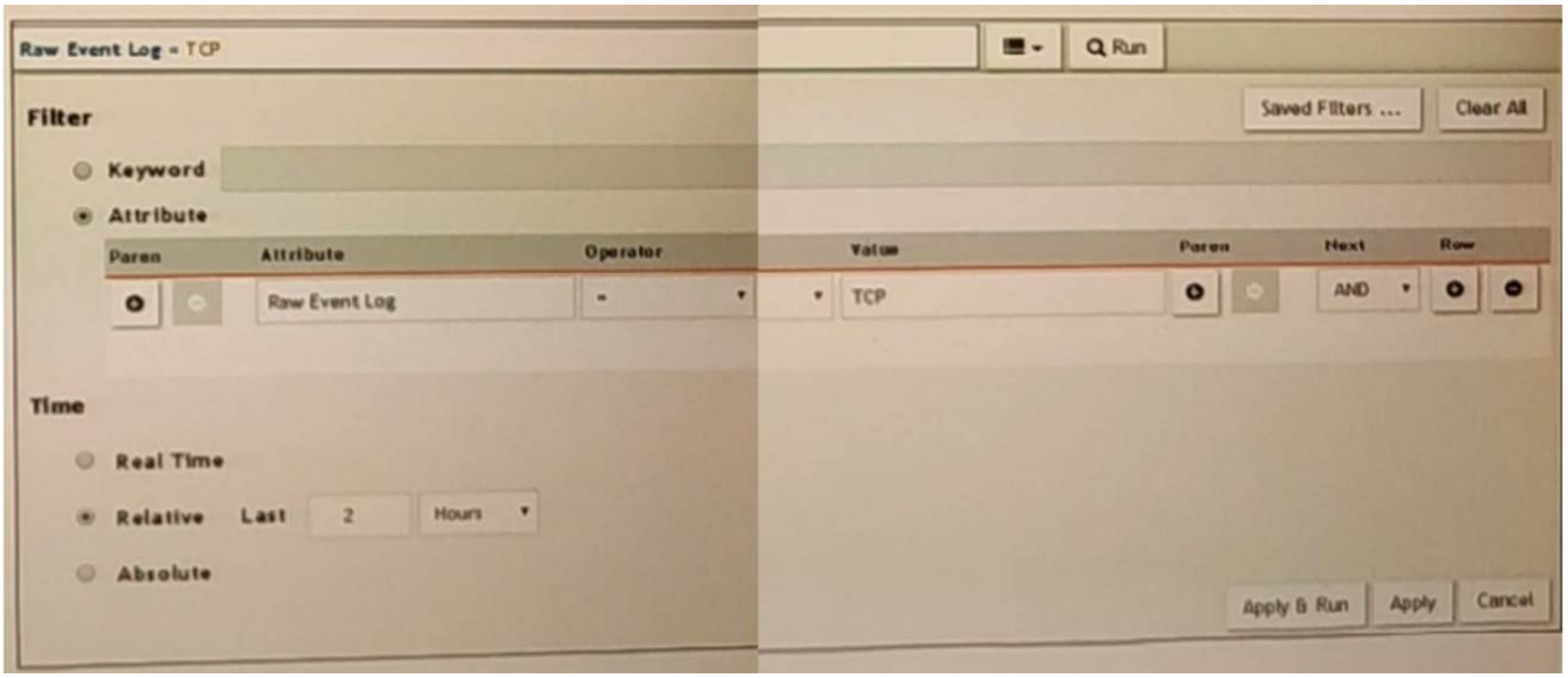

An administrator is trying to identify an issue using an expression bated on the Expression Builder settings shown in the exhibit however, the error message shown in the exhibit indicates that the expression is invalid.
Which is the correct expression?

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 9**
Refer to the exhibit.



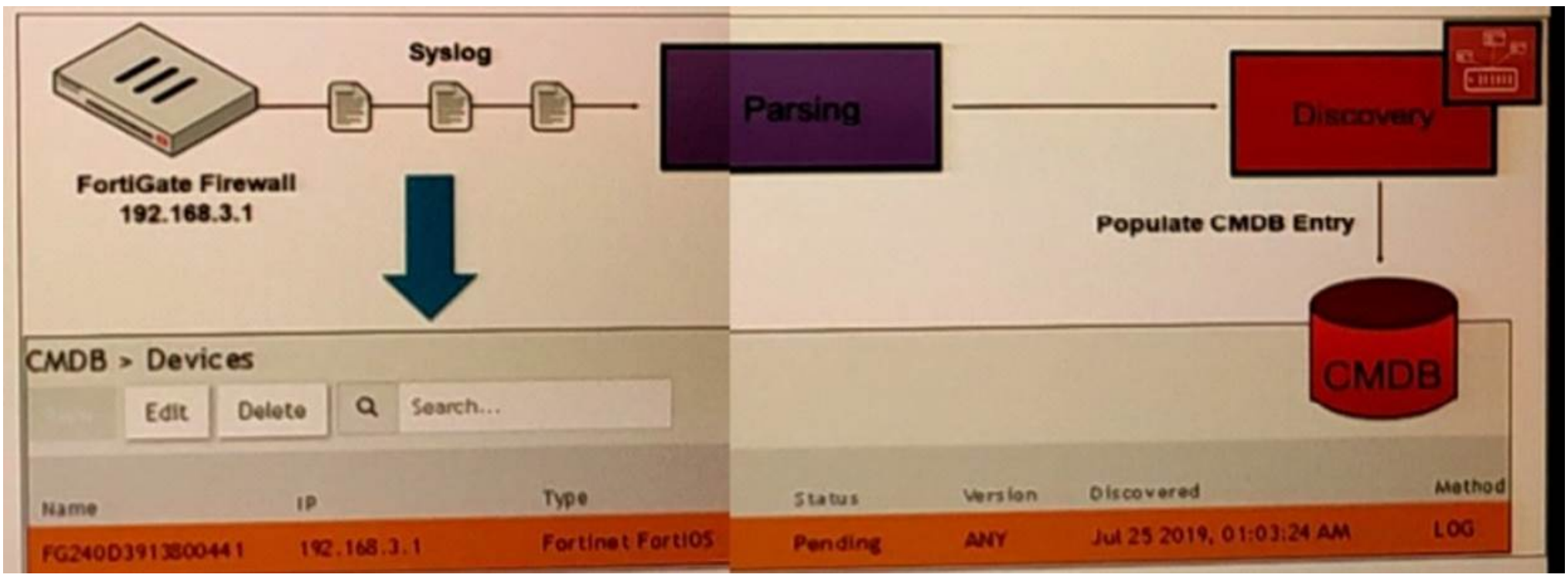

\A FortiSIEM is continuously receiving syslog events from a FortiGate firewall The FortiSIfcM administrator is trying to search the raw event logs for the last two hours that contain the keyword tcp . However, the administrator is getting no results from the search.
Based on the selected filters shown in the exhibit, why are there no search results?

A. The keyword is case sensitive Instead of typing TCP in the Value fiel
B. the administrator should type tcp.
C. In the Time section, the administrator selected the Relative Last option, and in the drop-down lists, selected 2 and Hours as the lime period The time period should be 24 hours.
D. The administrator selected - in the Operator column That a the wrong operator.
E. The administrator selected AND in the Next drop-down lis
F. This is the wrong boolean operator.

**Answer:** A

**Explanation:**
Case Sensitivity in Searches: In FortiSIEM, search queries, including those for raw event logs, are case sensitive. This means that keywords must be entered exactly as they appear in the logs.
Keyword Mismatch: The exhibit shows the keyword 'TCP' in the Value field. If the actual events use 'tcp' (lowercase), the search will return no results because of the case mismatch.
Correct Keyword: To match the keyword correctly, the administrator should enter 'tcp' in the Value field.

**NEW QUESTION 10**
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 10**
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 15**
In the advanced analytical rules engine in FortiSIEM, multiple subpatterns can be referenced using which three operation?(Choose three.)

A. ELSE
B. NOT
C. FOLLOWED_BY
D. OR
E. AND

**Answer:** CDE

**Explanation:**
Advanced Analytical Rules Engine: FortiSIEM's rules engine allows for complex event correlation using multiple subpatterns.
Operations for Referencing Subpatterns:
FOLLOWED_BY: This operation is used to indicate that one event follows another within a specified time window.
OR: This logical operation allows for the inclusion of multiple subpatterns, where the rule triggers if any of the subpatterns match.
AND: This logical operation requires all referenced subpatterns to match for the rule to trigger.
Usage: These operations allow for detailed and precise event correlation, helping to detect complex patterns and incidents.
References: FortiSIEM 6.3 User Guide, Advanced Analytics Rules Engine section, which explains the use of different operations to reference subpatterns in rules.

**NEW QUESTION 18**
In FortiSIEM enterprise licensing mode, it the link between the collector and data center FortiSlEM cluster is down, what happens?

A. The collector drops incoming events like syslo
B. but stops performance collection.
C. The collector processes stop, and events ate dropped.
D. The collector continues performance collection of devices, but slops receiving syslog.
E. The collector buffers events

**Answer:** D

**Explanation:**
Enterprise Licensing Mode: In FortiSIEM enterprise licensing mode, collectors are deployed in remote sites to gather and forward data to the central FortiSIEM cluster located in the data center.
Collector Functionality: Collectors are responsible for receiving logs, events (e.g., syslog), and performance metrics from devices.
Link Down Scenario: When the link between the collector and the FortiSIEM cluster is down, the collector needs a mechanism to ensure no data is lost during the disconnection.
Event Buffering: The collector buffers the events locally until the connection is restored, ensuring that no incoming events are lost. This buffered data is then forwarded to the FortiSIEM cluster once the link is re-established.
References: FortiSIEM 6.3 User Guide, Data Collection and Buffering section, explains the behavior of collectors during network disruptions.

**NEW QUESTION 20**
What protocol can be used to collect Windows event logs in an agentless method?

A. SSH
B. SNMP
C. WMI
D. SMTP

**Answer:** C

**NEW QUESTION 22**
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**
What operating system is FortiSIEM based on?

A. Cent OS
B. Microsoft Windows
C. RedHat
D. Ubuntu

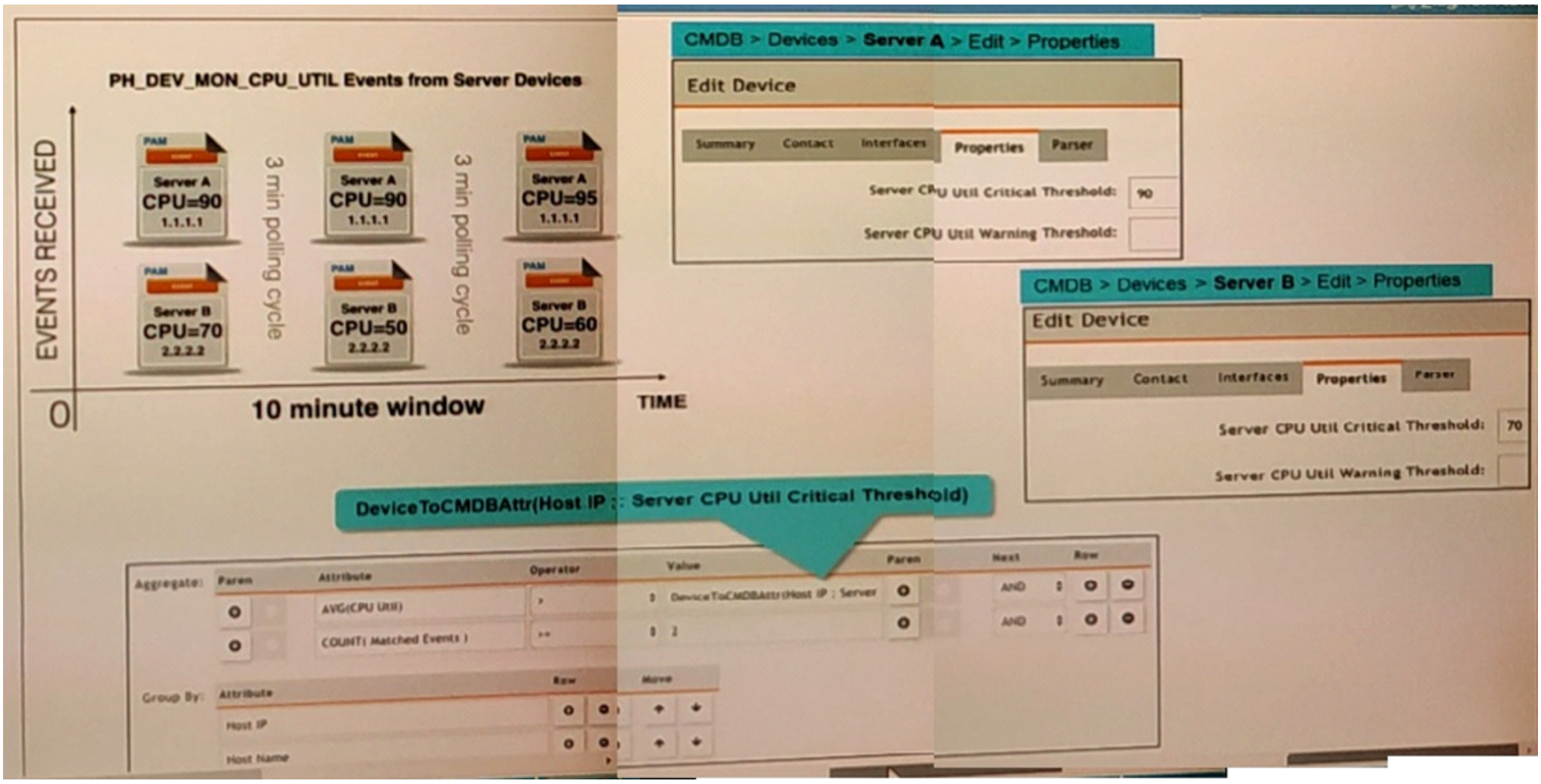
**Answer:** A

**NEW QUESTION 28**
A FortiSIEM administrator wants to restrict a network administrator to running searches for only firewall devices. Under role management, which option does the FortiSIEM administrator need to configure to achieve this scenario?

A. CMDB Report Conditions
B. Data Conditions
C. UI Access

**Answer:** B

**NEW QUESTION 29**
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 32**
Which two export methods are available for FortiSIEM analytics results? (Choose two.)

A. CSV
B. PNG
C. HTML
D. PDF

**Answer:** AD

**NEW QUESTION 36**
What is the best discovery scan option for a network environment where ping is disabled on all network devices?

A. Smart scan
B. Range scan
C. CMDB scan
D. L2 scan

**Answer:** A

**NEW QUESTION 39**
What are the minimum memory requirements for the FortiSIEM supervisor virtual appliance, when the proprietary flat file database is used?

A. 16GB RAM
B. 32GB RAM
C. 64GB RAM
D. 24GB RAM

**Answer:** D

**NEW QUESTION 44**
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 49**

.....

# 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