

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

If 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

What is a prerequisite for FortiSIEM Linux agent installation?

- A. The web server must be installed on the Linux server being monitored
- B. The auditd service must be installed on the Linux server being monitored
- C. The Linux agent manager server must be installed.
- D. Both the web server and the audit service must be installed on the Linux server being monitored

Answer: B

Explanation:

Explanation

FortiSIEM Linux Agent: The FortiSIEM Linux agent is used to collect logs and performance metrics from Linux servers and send them to the FortiSIEM system.

Prerequisite for Installation: Theauditdservice, which is the Linux Audit Daemon, must be installed and running on the Linux server to capture and log security-related events.

- auditd Service: This service collects and logs security events on Linux systems, which are essential for monitoring and analysis by FortiSIEM.
- Importance of auditd: Without the auditd service, the FortiSIEM Linux agent will not be able to collect the necessary event data from the Linux server.
- References: FortiSIEM 6.3 User Guide, Linux Agent Installation section, which lists the prerequisites and steps for installing the FortiSIEM Linux agent.

NEW QUESTION 3

What are the four categories of incidents?

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

Answer: C

Explanation:

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.

References: FortiSIEM 6.3 User Guide, Incident Management section, which details the different categories of incidents and their significance.

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

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 settings addresses
- 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

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.

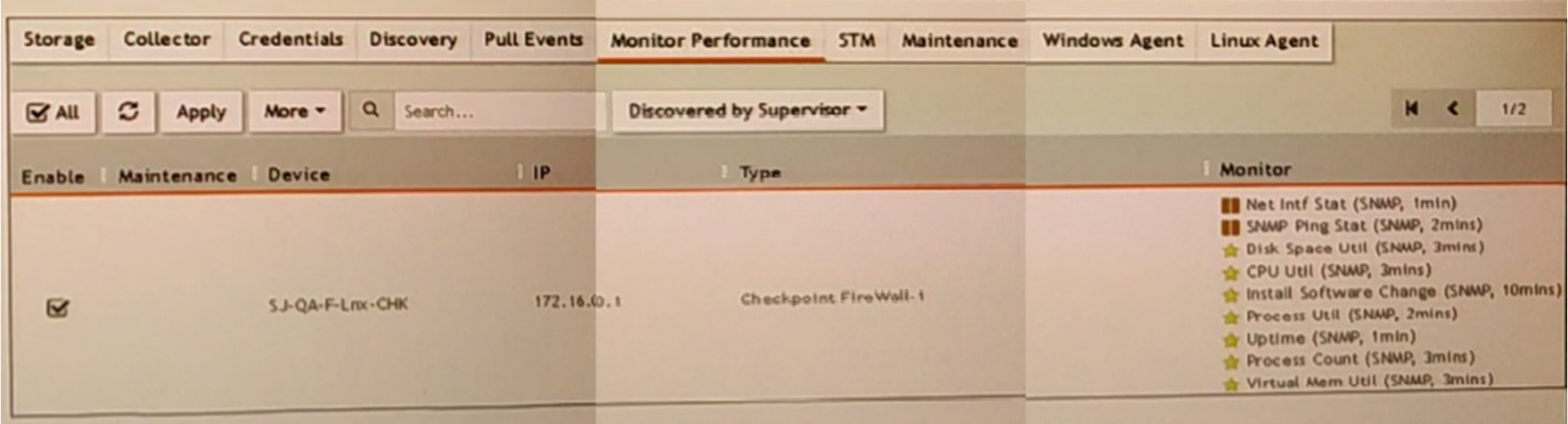
Usage: Run the command phgetHWID in the CLI to obtain the hardware ID.

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
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.

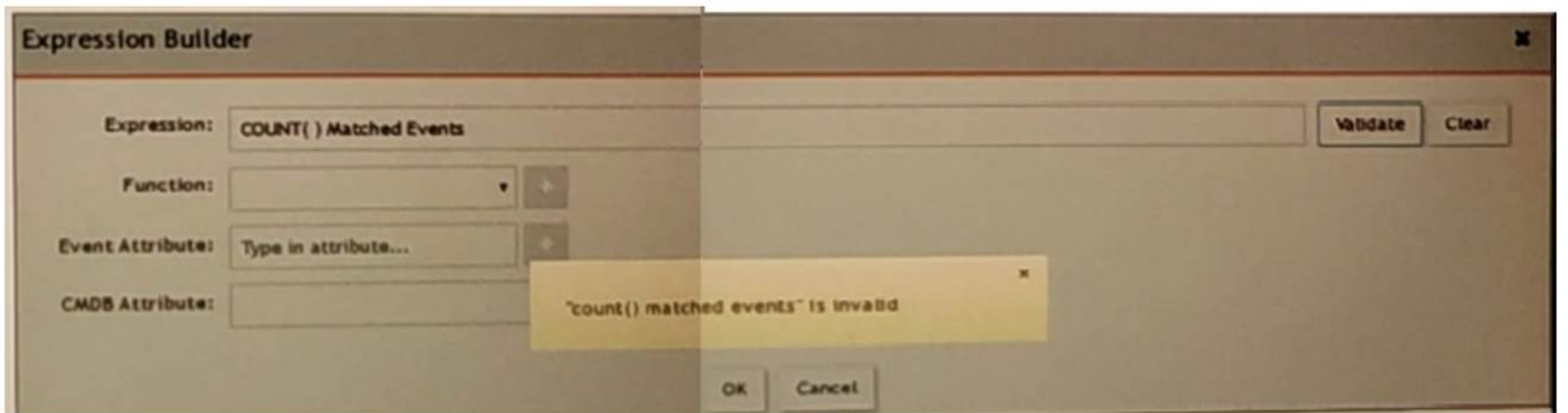
- A. External Event Receive Protocol
- B. Event Received Proto Agents
- C. External Event Receive Raw Logs
- D. External Event Receive Agents

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

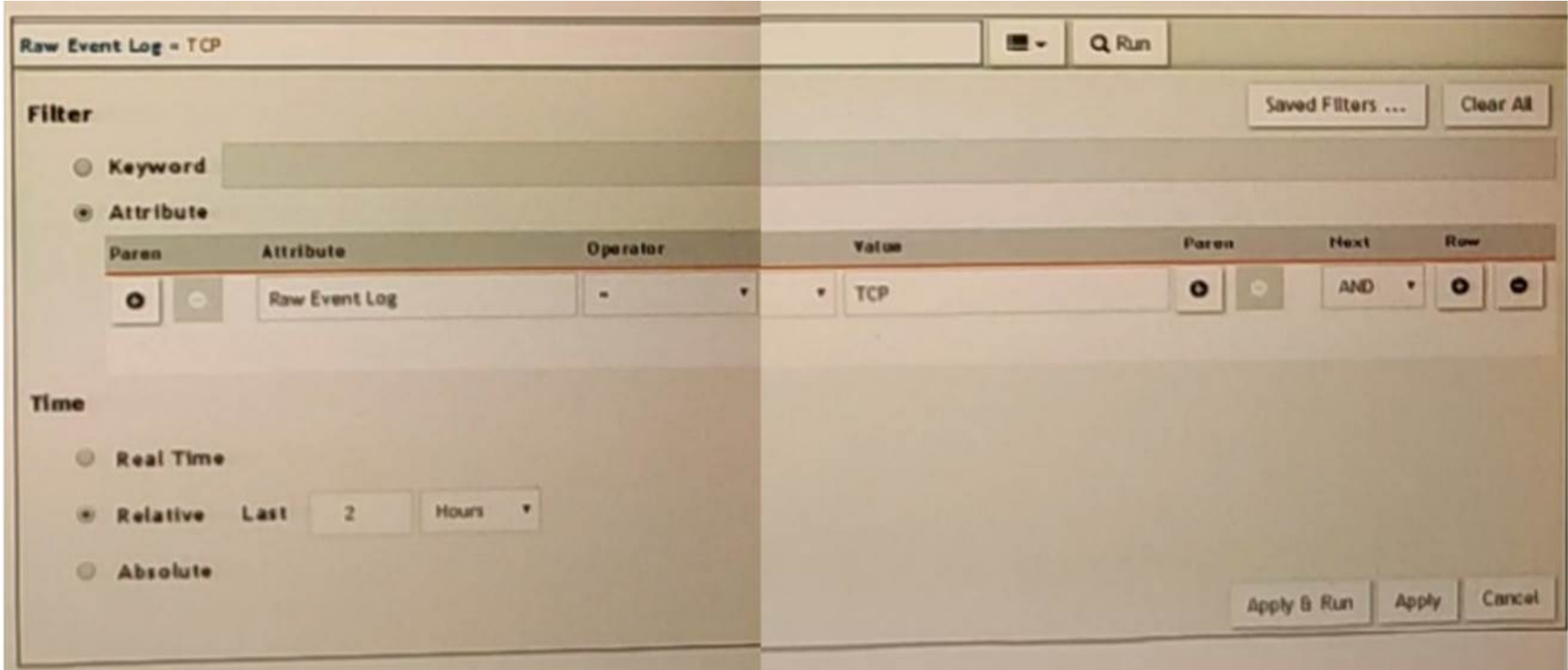
Answer: C

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

Refer to the exhibit.



VA FortiSIEM is continuously receiving syslog events from a FortiGate firewall The FortiSIEM 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

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.

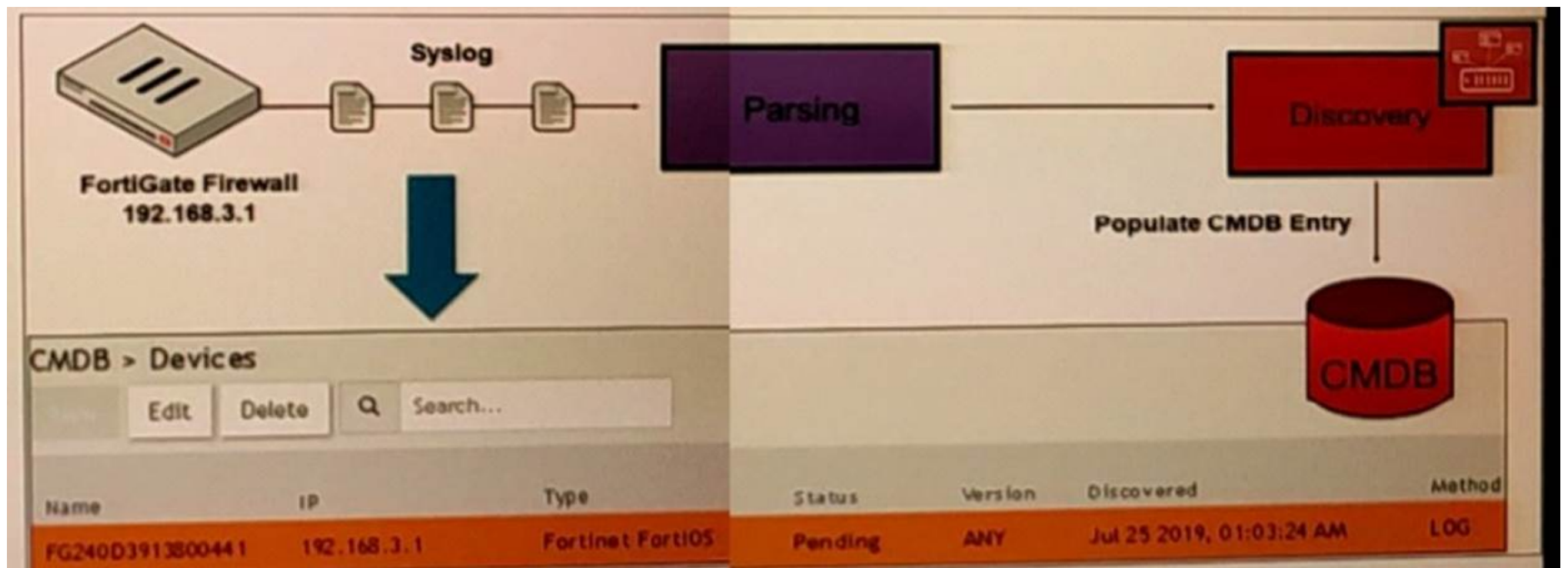
Answer: B

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 15

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 20

Consider the storage of anomaly baseline data 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 23

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 24

Which is a requirement for implementing FortiSIEM disaster recovery?

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

Answer: C

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 25

An administrator defines SMTP as a critical process on a Linux server. If the SMTP process is stopped, FortiSIEM would generate a critical event with which event type?

- A. PH_DEV_MON_PROC_STOP
- B. Postfix-Mail-Slop
- C. Generic_SMTP_Process_Exit
- D. PH_DEV_MON_SMTP_STOP

Answer: A

NEW QUESTION 26

What operating system is FortiSIEM based on?

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

Answer: A

NEW QUESTION 29

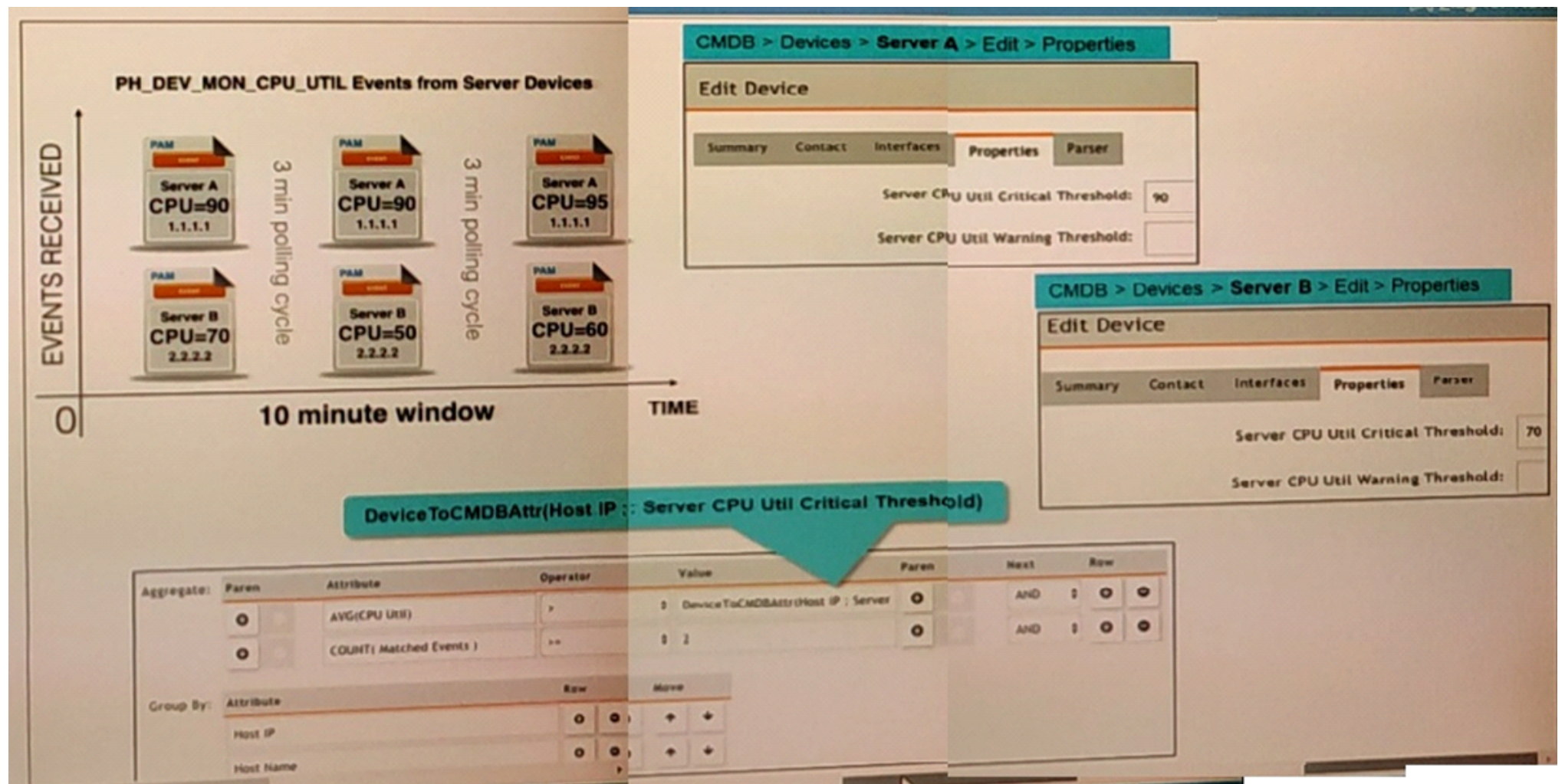
A FortiSIEM administrator wants to restrict a network administrator to running searches for only firewall devices. Under role management, which option does the FortiSIEM administrator need to configure to achieve this scenario?

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

Answer: B

NEW QUESTION 33

Refer to the exhibit.



Three events are collected over a 10-minute 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 will 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 38

Refer to the exhibit.

The screenshot shows the 'Filter' configuration window in FortiSIEM. The 'Filter' section is expanded, showing the 'Attribute' filter type. The filter is configured as follows:

Filter Type	Attribute	Operator	Value	Next	Row
Attribute	Reporting IP	=	192.168.1.1	AND	1
	Reporting IP	=	172.16.10.3	AND	2

The 'Time' section is also visible, with 'Absolute' selected. The 'From' date is 01/13/2020 13:19:41 and the 'To' date is 01/20/2020 13:29:41. The 'Always prior' checkbox is unchecked.

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 filters 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 39

What are the four possible incident status values?

- A. Active, dosed, cleared, open
- B. Active, cleared, cleared manually, system cleared

- C. Active, closed, manual, resolved
- D. Active, auto cleared, manual, false positive

Answer: C

NEW QUESTION 40

Which discovery scan type is prone to miss a device, if the device is quiet and the entry for that device is not present in the ARP table of adjacent devices?

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

Answer: D

NEW QUESTION 44

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

NEW QUESTION 47

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 51

A FortiSIEM supervisor at headquarters is struggling to keep up with an increase of EPS (Events Per Second) being reported across the enterprise. What components should an administrator consider deploying to assist the supervisor with processing data?

- A. Supervisor
- B. Worker
- C. Collector
- D. Agent

Answer: B

NEW QUESTION 52

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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

100% Actual & Verified — Instant Download, Please Click
[Order The NSE5_FSM-6.3 Practice Test Here](#)