Free Questions for NSE5_FSM-6.3 by actualtestdumps

Shared by Ramsey on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which three ports can be used to send Syslogs to FortiSIEM? (Choose three.)

Options:

A- UDP9999

B- UDP 162

C- TCP 514

D- UDP 514

E- TCP 1470

Answer:

C, D, E

Explanation:

Syslog Ports: Syslog messages can be sent over different ports using TCP or UDP protocols.

Common Ports for Syslog:

UDP 514: This is the default port for sending syslog messages over UDP.

TCP 514: This is the default port for sending syslog messages over TCP, providing a more reliable transmission.

TCP 1470: This port is often used for secure or alternative syslog transmission.

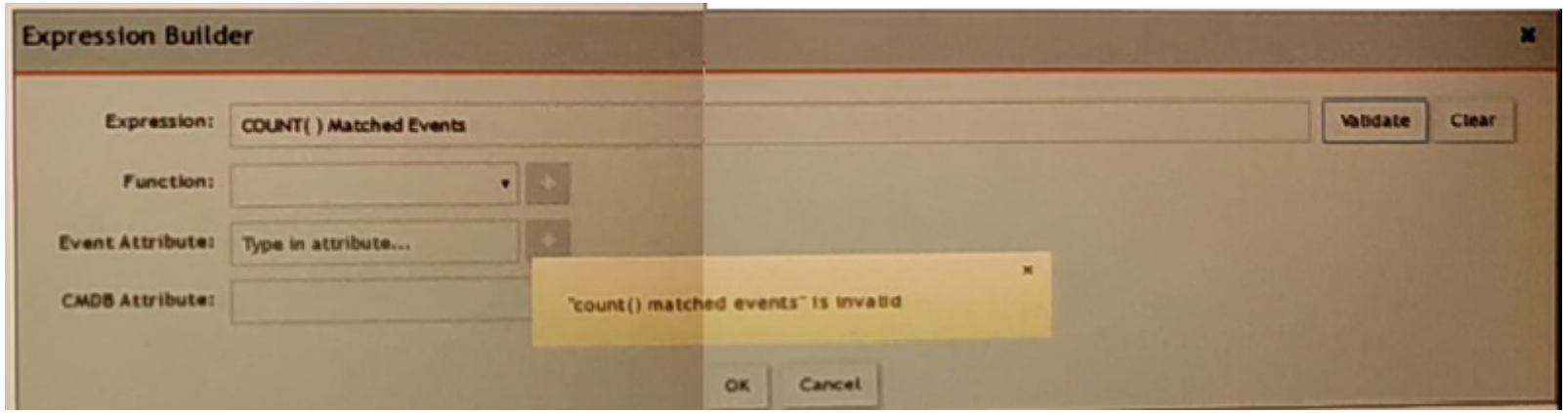
Usage in FortiSIEM: FortiSIEM can be configured to receive syslog messages on these ports to ensure the logs are collected from various network devices.

References: FortiSIEM 6.3 User Guide, Syslog Integration section, which details the supported ports for syslog transmission.

Question 2

Question Type: **MultipleChoice**

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?

Options:

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.

Question 3

Question Type: MultipleChoice

Which FortiSIEM components are capable of performing device discovery?

Options:

A- FortiSIEM Windows agent

B- Worker

C- FortiSIEM Linux agent

D- Collector

Answer:

D

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.

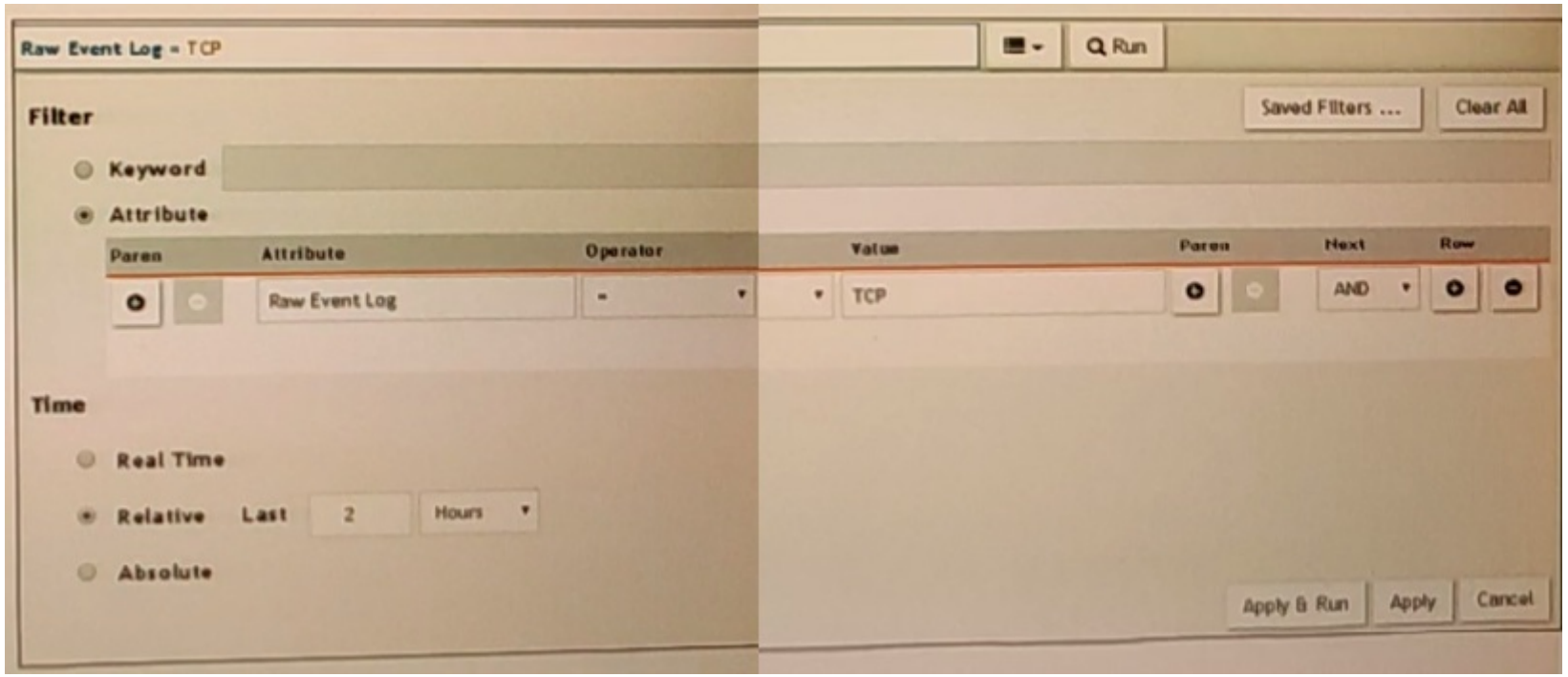
Capability: While agents (Windows and Linux) primarily gather data from their host systems, the collectors actively discover devices across the network.

References: FortiSIEM 6.3 User Guide, Device Discovery section, which details the role of collectors in discovering network devices.

Question 4

Question Type: MultipleChoice

Refer to the exhibit.



A FortiSIEM is continuously receiving syslog events from a FortiGate firewall The FortiSlfcM 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?

Options:

A- The keyword is case sensitive Instead of typing TCP in the Value field. the administrator should type tcp.

B- 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.

C- The administrator selected - in the Operator column That a the wrong operator.

D- The administrator selected AND in the Next drop-down list. 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.

References: FortiSIEM 6.3 User Guide, Search and Filtering section, which discusses the importance of case sensitivity in search queries.

Question 5

Question Type: MultipleChoice

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

Options:

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.'

Question 6

Question Type: MultipleChoice

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?

Options:

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.

Question 7

Question Type: MultipleChoice

In the rules engine, which condition instructs FortiSIEM to summarize and count the matching evaluated data?

Options:

A- Time Window

B- Aggregation

C- Group By

D- Filters

Answer:

B

Explanation:

Rules Engine in FortiSIEM: The rules engine evaluates incoming events based on defined conditions to detect incidents and anomalies.

Aggregation Condition: The aggregation condition instructs FortiSIEM to summarize and count the matching evaluated data.

Function: Aggregation is used to group events based on specified criteria and then perform operations such as counting the number of occurrences within a defined time window.

Purpose: This allows for the detection of patterns and anomalies, such as a high number of failed login attempts within a short period.

References: FortiSIEM 6.3 User Guide, Rules Engine section, which explains how aggregation is used to summarize and count matching data.

Question 8

Question Type: MultipleChoice

A customer is experiencing slow performance while executing long, adhoc analytic searches Which FortiSIEM component can make the searches run faster?

Options:

A- Correlation worker

B- Event worker

C- Storage worker

D- Query worker

Answer:

D

Explanation:

Component Roles in FortiSIEM: Different components in FortiSIEM have specific roles and responsibilities, which contribute to the overall performance and functionality of the system.

Query Worker: The query worker component is specifically designed to handle and optimize search queries within FortiSIEM.

Function: It processes search requests and executes analytic searches efficiently, handling large volumes of data to provide quick results.

Optimization: By improving the efficiency of query execution, the query worker can significantly speed up long, ad hoc analytic searches, addressing performance issues.

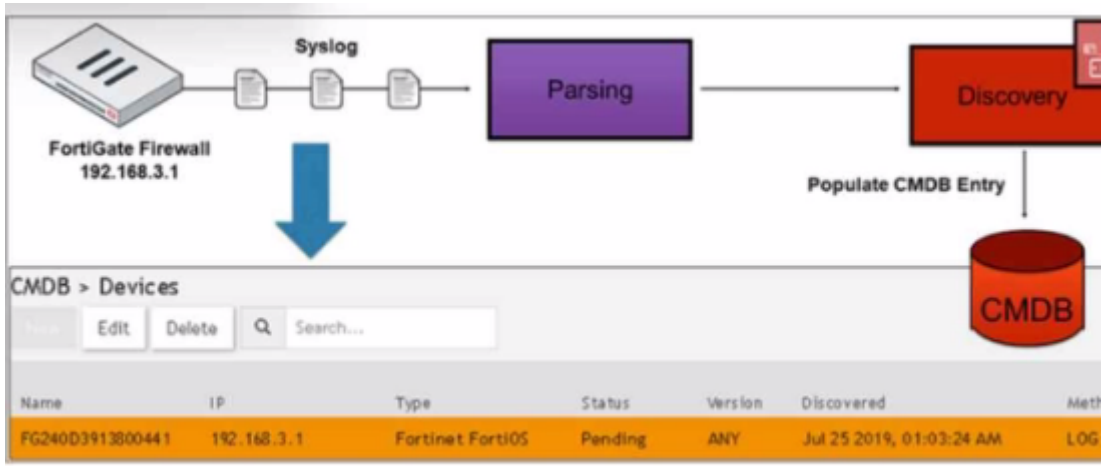
Performance Impact: Utilizing the query worker ensures that searches are handled by a component optimized for such tasks, reducing the load on other components and improving overall system performance.

References: FortiSIEM 6.3 User Guide, System Components section, which describes the roles of different workers, including the query worker, and their impact on system performance.

Question 9

Question Type: MultipleChoice

Refer to the exhibit.



How was the FortiGate device discovered by FortiSIEM?

Options:

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.

Question 10

Question Type: MultipleChoice

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

Options:

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:

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.

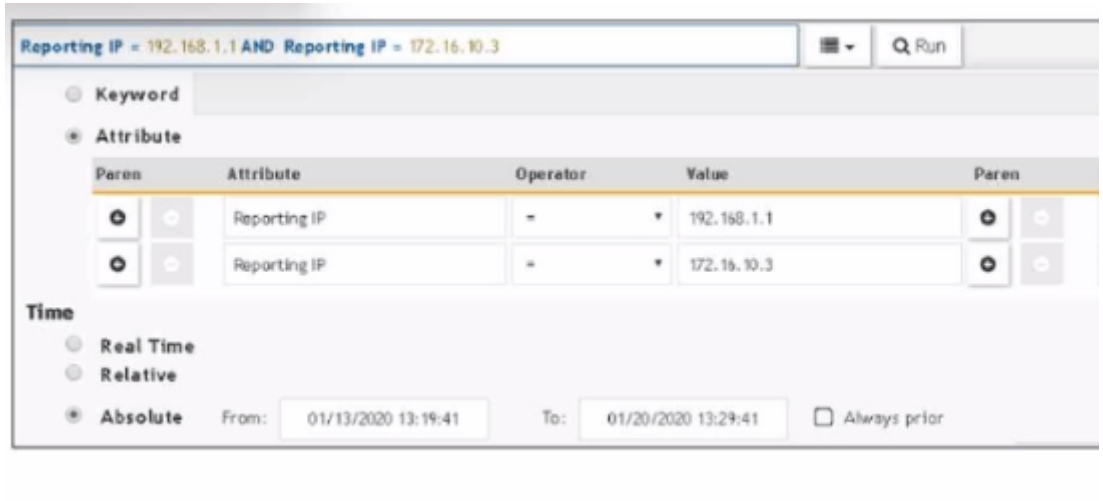
Comprehensive Data Collection: By using WMI, FortiSIEM can gather a wide range of event logs that are crucial for monitoring and analyzing the security and performance of Windows devices.

References: FortiSIEM 6.3 User Guide, Data Collection Methods section, which details the use of WMI for collecting event logs from Windows devices.

Question 11

Question Type: **MultipleChoice**

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 filters shown in the exhibit, why is the search returning no results?

Options:

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:

A

Explanation:

Search Filters in FortiSIEM: When searching for events, the correct use of filters and logical operators is crucial to obtain accurate results.

Issue Analysis:

Selected Filters: The exhibit shows filters for two different Reporting IP addresses.

Logical Operators: The use of 'AND' between the two Reporting IP addresses implies that an event must match both IP addresses simultaneously, which is not possible for a single event.

Correct Usage: To search for events from either of the two IP addresses, parentheses should be used to group conditions logically.

Corrected Filter: (Reporting IP = 192.168.1.1 OR Reporting IP = 172.16.10.3) would return events from either IP address.

References: FortiSIEM 6.3 User Guide, Search and Filters section, which explains the use of logical operators and the importance of parentheses in constructing effective search queries.

Question 12

Question Type: MultipleChoice

What are the four categories of incidents?

Options:

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:

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.