Fortinet.NSE5_FSM-6.3.by.Linda.30q

Number: NSE5_FSM-6.3
Passing Score: 800
Time Limit: 120
File Version: 4.0

Exam Code: NSE5_FSM-6.3

Exam Name: Fortinet NSE 5 - FortiSIEM 6.3

Exam A

QUESTION 1

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

A. The collector drops incoming events like syslog. but stops performance collection.

B. The collector processes stop, and events ate dropped.

C. The collector continues performance collection of devices, but slops receiving syslog.

D. The collector buffers events

Correct Answer: C
Section:
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.
Reference: FortiSIEM 6.3 User Guide, Data Collection and Buffering section, explains the behavior of collectors during network disruptions.

QUESTION 2

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

Correct Answer: C
Section:
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.
Reference: FortiSIEM 6.3 User Guide, Event Correlation and Processing section, details how the Supervisor and Worker components collaborate for real-time event correlation.

QUESTION 3

FortiSIEM is deployed in disaster recovery mode.
When disaster strikes, which two tasks must you perform manually to achieve a successful disaster recovery operation? (Choose two.)

A. Promote the secondary workers to the primary rotes using the phSecworker2priworker command.

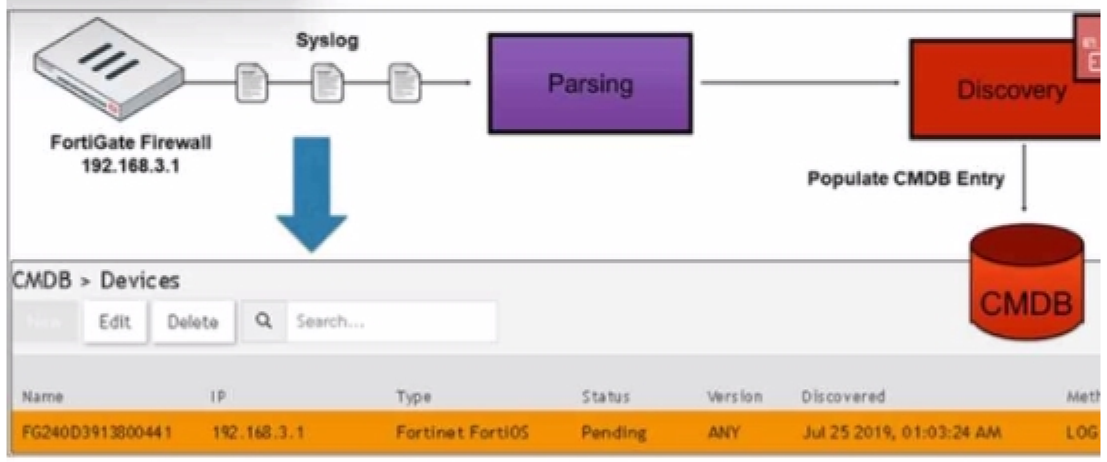
B. Promote the secondary supervisor to the primary role using the phSecondary2primary command.

C. Change the DNS configuration to ensure that users, devices, and collectors log in to the secondary FortiSIEM.

D. Change the configuration for shared storage NFS configured for EventDB to the secondary FortiSIEM.

Correct Answer: A, C
Section:
Explanation:
Disaster Recovery Mode: FortiSIEM's disaster recovery (DR) mode ensures that there is a backup system ready to take over in case the primary system fails.
Manual Tasks for DR Operation: In the event of a disaster, certain tasks must be performed manually to ensure a smooth transition to the secondary system.
Promoting the Secondary Supervisor:
Use the command phSecondary2primary to promote the secondary supervisor to the primary role. This command reconfigures the secondary supervisor to take over as the primary supervisor, ensuring continuity in management and coordination.
Changing DNS Configuration:
Update the DNS configuration to direct all users, devices, and collectors to the secondary FortiSIEM instance. This ensures that all components in the environment can communicate with the newly promoted primary supervisor without manual reconfiguration of individual devices.
Reference: FortiSIEM 6.3 Administration Guide, Disaster Recovery section, provides detailed steps on promoting the secondary supervisor and updating DNS configurations during a disaster recovery operation.

QUESTION 4
Refer to the exhibit.



CMDB > Devices

Name	IP	Type	Status	Version	Discovered	Meth
FG240D3913800441	192.168.3.1	Fortinet FortiOS	Pending	ANY	Jul 25 2019, 01:03:24 AM	LOG

How was the FortiGate device discovered by FortiSIEM?

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

Correct Answer: D
Section:
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.'
Reference: 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 5
What does the Frequency field determine on a rule?

A. How often the rule will 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.

Correct Answer: B
Section:
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.
Reference: FortiSIEM 6.3 User Guide, Rules and Incidents section, which explains the Frequency field and how it impacts the evaluation of subpatterns in rules.

QUESTION 6
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.

Correct Answer: B
Section:
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.
Reference: 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.

QUESTION 7
In me FortiSIEM CLI. which command must you use to determine whether or not syslog is being received from a network device?

A. tcpdump
B. OphSyslogRecorder
C. Onetcat
D. phDeviceTest

Correct Answer: A
Section:
Explanation:
Syslog Reception Verification: To verify whether syslog messages are being received from a network device, a network packet capture tool can be used.

tcpdump Command: tcpdump is a powerful command-line packet analyzer tool available in Unix-like operating systems. It allows administrators to capture and analyze network traffic.
Usage: By using tcpdump with the appropriate filters (e.g., port 514 for syslog), administrators can monitor the incoming syslog messages in real-time to verify if they are being received.
Example Command: tcpdump -i <interface> port 514 captures the syslog messages on the specified network interface.
Reference: FortiSIEM 6.3 User Guide, CLI Commands section, which details the usage of tcpdump for network traffic analysis and verification of syslog reception.

QUESTION 8

Which FortiSIEM components can do performance availability and performance monitoring?

A. Supervisor, worker, and collector
B. Supervisor and workers only
C. Supervisor only
D. Collectors only

Correct Answer: A
Section:
Explanation:
Performance and Availability Monitoring: Various components in FortiSIEM are responsible for monitoring the performance and availability of devices and services.
Components:
Supervisor: Oversees the entire FortiSIEM infrastructure and coordinates the activities of other components.
Worker: Processes and analyzes the collected data, including performance and availability metrics.
Collector: Gathers performance and availability data from devices in the network.
Collaborative Functioning: These components work together to ensure comprehensive monitoring of the network's performance and availability.
Reference: FortiSIEM 6.3 User Guide, Performance and Availability Monitoring section, which explains the roles of the supervisor, worker, and collector in monitoring tasks.

QUESTION 9

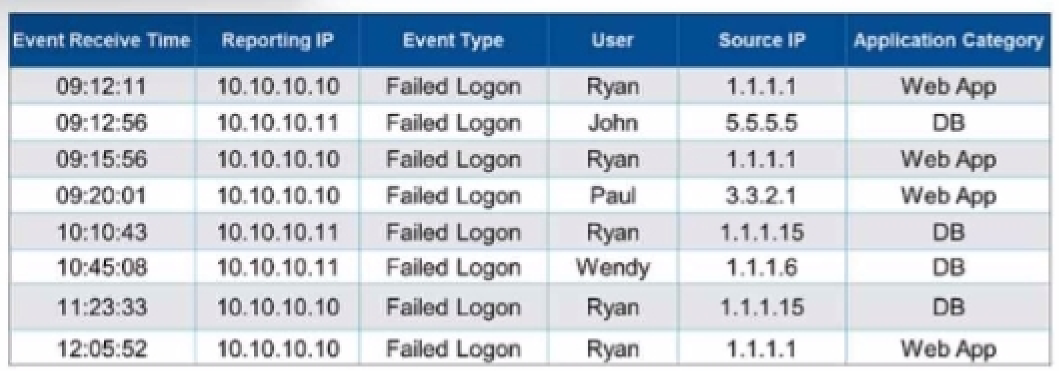
Which command displays the Linux agent status?

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

Correct Answer: C
Section:
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 is service fortisiem-linux-agent status.
Usage: Properly checking the agent status helps ensure that data collection from Linux devices is functioning as expected.
Reference: FortiSIEM 6.3 User Guide, Linux Agent Installation and Management section, which includes commands for managing the Linux agent.

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 User. Source IP. and Application Category attributes in FortiSiEM. how many results will be displayed?

A. Three results will be displayed.
B. Five results will be displayed.
C. No results will be displayed.
D. Seven results will be displayed.

Correct Answer: B
Section:
Explanation:
Grouping Events in FortiSIEM: Grouping events by specific attributes allows for the aggregation of similar events, providing clearer insights and reducing clutter.
Grouping Criteria: For this question, events are grouped by 'User,' 'Source IP,' and 'Application Category.'
Unique Combinations Analysis:
Ryan, 1.1.1.1, Web App (appears multiple times but is one unique combination)
John, 5.5.5.5, DB
Paul, 3.3.2.1, Web App
Ryan, 1.1.1.15, DB
Wendy, 1.1.1.6, DB
Result Calculation: There are five unique combinations in the provided data based on the specified grouping attributes.
Reference: FortiSIEM 6.3 User Guide, Event Management and Reporting sections, which explain how to group events by various attributes for analysis and reporting purposes.

QUESTION 11
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. A new incident is created based on the Rule Frequency value, and the First Seen and Last Seen times ate updated.
C. The Incident Count value increases, and the First Seen and Last Seen times update.
D. The incident status changes to Repeated, and the First Seen and Last Seen times are updated.

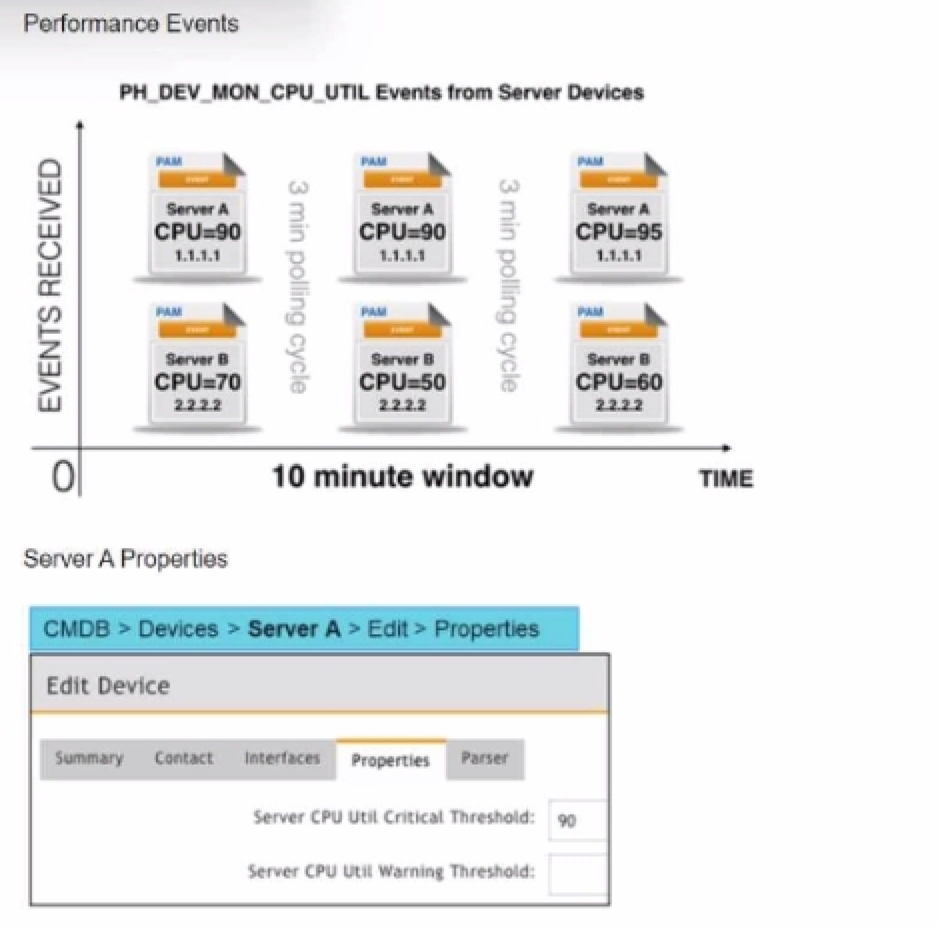
Correct Answer: C
Section:
Explanation:
Incident Management in FortiSIEM: FortiSIEM tracks incidents and their occurrences to help administrators manage and respond to recurring issues.
Performance Rule Triggering: When a performance rule, such as one for high CPU usage, is repeatedly triggered, FortiSIEM 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.
Reference: FortiSIEM 6.3 User Guide, Incident Management section, explains how FortiSIEM handles recurring incidents and updates the incident table accordingly.

QUESTION 12
Which process converts raw log data to structured data?

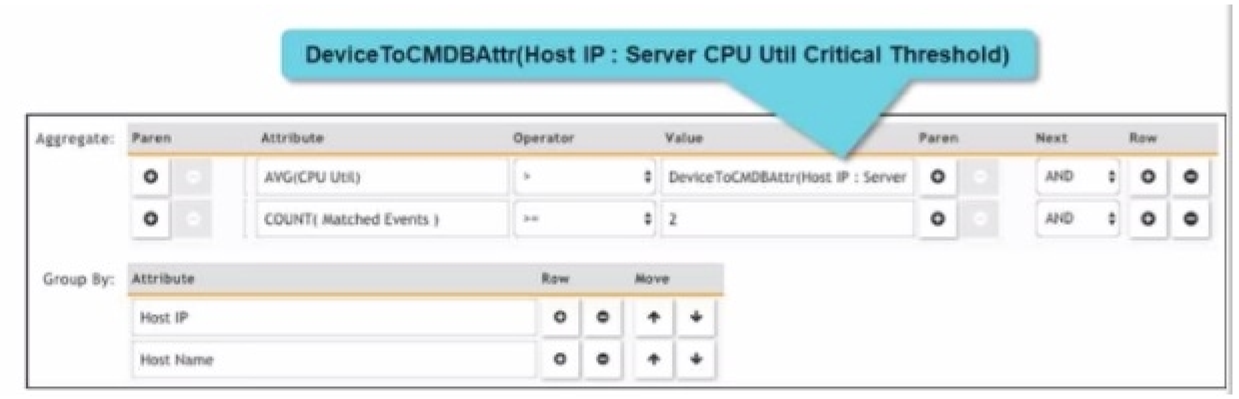
A. Data classification
B. Data validation
C. Data parsing
D. Data enrichment

Correct Answer: C
Section:
Explanation:
Raw Log Data: When devices send logs to FortiSIEM, the data arrives in a raw, unstructured format.
Data Parsing Process: The process that converts this raw log data into a structured format is known as data parsing.
Data Parsing: This involves extracting relevant fields from the raw log entries and organizing them into a structured format, making the data usable for analysis, reporting, and correlation.
Significance of Structured Data: Structured data is essential for effective event correlation, alerting, and generating meaningful reports.
Reference: FortiSIEM 6.3 User Guide, Data Parsing section, which details how raw log data is transformed into structured data through parsing.

QUESTION 13
Refer to the exhibits.



Server CPU Util Critical Threshold: 90
Server CPU Util Warning Threshold:



DeviceToCMDBAttr(Host IP : Server CPU Util Critical Threshold)

Aggregate:

Paren	Attribute	Operator	Value	Paren	Next
	AVG(CPU Util)	>	DeviceToCMDBAttr(Host IP : Server		AND
	COUNT(Matched Events)	>=	2		AND

Group By:

Attribute
Host IP
Host Name

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

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

Correct Answer: D
Section:
Explanation:
Event Collection Overview: The exhibits show three events collected over a 10-minute period from two servers, Server A and Server B.
Rule Subpattern Settings: The rule subpattern specifies two conditions:
AVG(CPU Util) > DeviceToCMDBAttr(Host IP : Server CPU Util Critical Threshold): This checks if the average CPU utilization exceeds the critical threshold defined for each server.
COUNT(Matched Events) >= 2: This requires at least two matching events within the specified period.
Server A Analysis:
Events: Three events (CPU=90, CPU=90, CPU=95).
Average CPU Utilization: (90+90+95)/3 = 91.67, which exceeds the critical threshold of 90.
Matched Events Count: 3, which meets the condition of being greater than or equal to 2.
Incident Generation: Server A meets both conditions, so it generates one incident.
Server B Analysis:
Events: Three events (CPU=70, CPU=50, CPU=60).
Average CPU Utilization: (70+50+60)/3 = 60, which does not exceed the critical threshold of 90.
Matched Events Count: 3, but since the average CPU utilization condition is not met, no incident is generated.
Conclusion: Based on the rule subpattern, Server A will generate one incident, and Server B will not generate any incidents.
Reference: FortiSIEM 6.3 User Guide, Event Correlation Rules and Incident Management sections, which explain how incidents are generated based on rule subpatterns and event conditions.

QUESTION 14
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

Correct Answer: B
Section:
Explanation:
FortiSIEM Architecture: In FortiSIEM, collectors gather data from various sources and send this data to supervisors and workers within the FortiSIEM architecture.

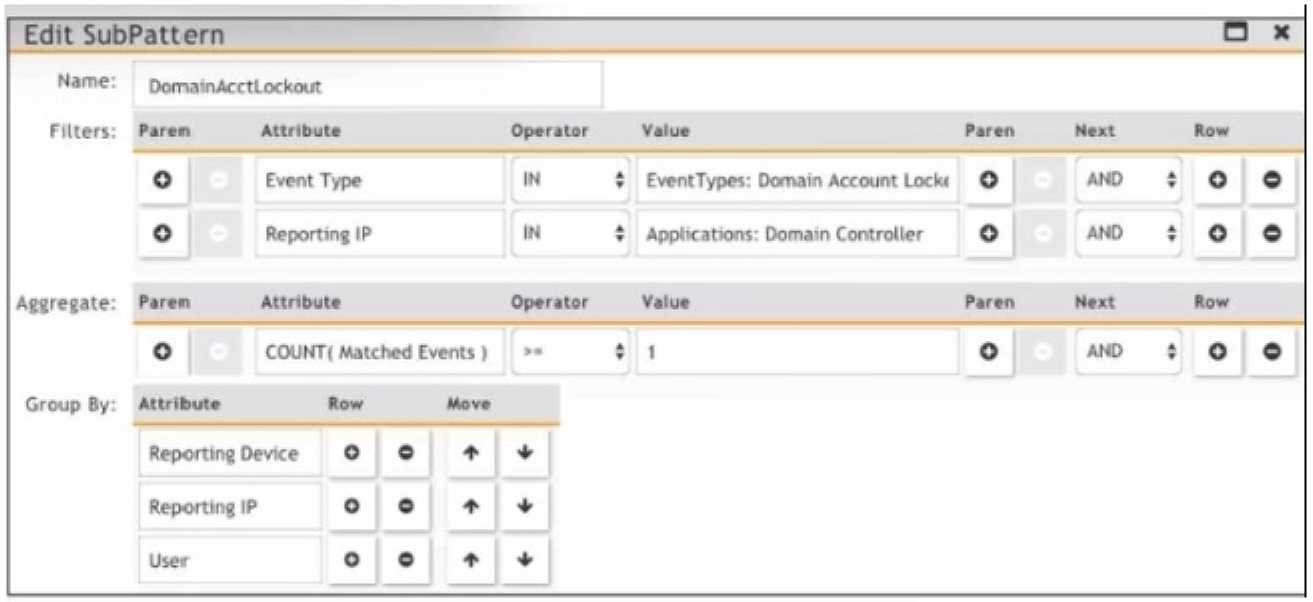
Communication Requirements: For collectors to effectively send data to the FortiSIEM system, specific communication channels must be open.
Port Usage: The primary port used for secure communication between the collectors and the FortiSIEM infrastructure is HTTPS (port 443).
Network Configuration: When 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.
Reference: FortiSIEM 6.3 Administration Guide, Network Ports section details the necessary ports for communication within the FortiSIEM architecture.

QUESTION 15
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

Correct Answer: A, C
Section:
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.
Reference: FortiSIEM 6.3 Administration Guide, Licensing section details the commands and procedures for obtaining system identification information necessary for license renewal.

QUESTION 16
Refer to the exhibit.



Edit SubPattern

Name: DomainAcctLockout

Filters:

Paren	Attribute	Operator	Value	Paren	Next	Row
	Event Type	IN	EventTypes: Domain Account Locke		AND	
	Reporting IP	IN	Applications: Domain Controller		AND	

Aggregate:

Paren	Attribute	Operator	Value	Paren	Next	Row
	COUNT(Matched Events)	>=	1		AND	

Group By:

Attribute	Row	Move
Reporting Device		
Reporting IP		
User		

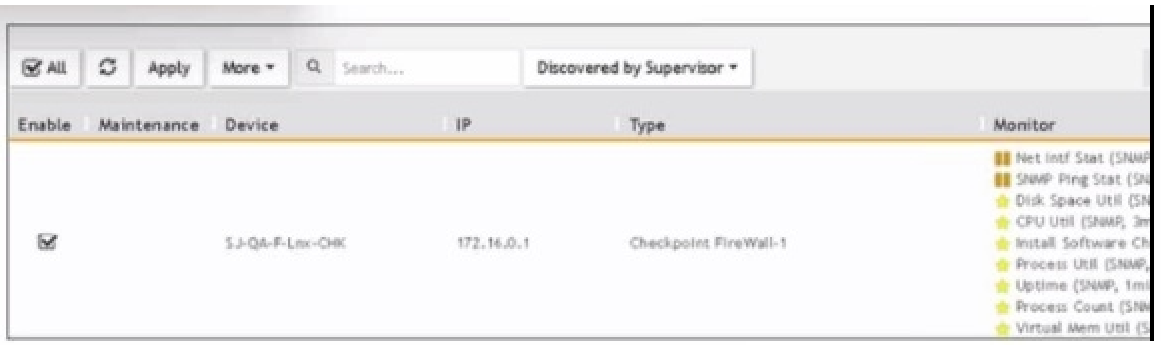
Which section contains the sortings that determine how many incidents are created?

A. Actions
B. Group By
C. Aggregate

D. Filters

Correct Answer: C
Section:
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.
Reference: FortiSIEM 6.3 User Guide, Rule and Pattern Creation section, which details how grouping impacts incident generation.

QUESTION 17
Refer to the exhibit.



Enable	Maintenance	Device	IP	Type	Monitor
☑		SJ-QA-F-Lnx-CHK	172.16.0.1	Checkpoint FireWall-1	⏸ Net Intf Stat (SNMP ⏸ SNMP Ping Stat (SN ★ Disk Space Util (SN ★ CPU Util (SNMP, 3m ★ Install Software Ch ★ Process Util (SNMP, ★ Uptime (SNMP, 1mi ★ Process Count (SNM ★ Virtual Mem Util (S

What does the pauso icon indicate?

A. Data collection is paused after the intervals shown for metrics.

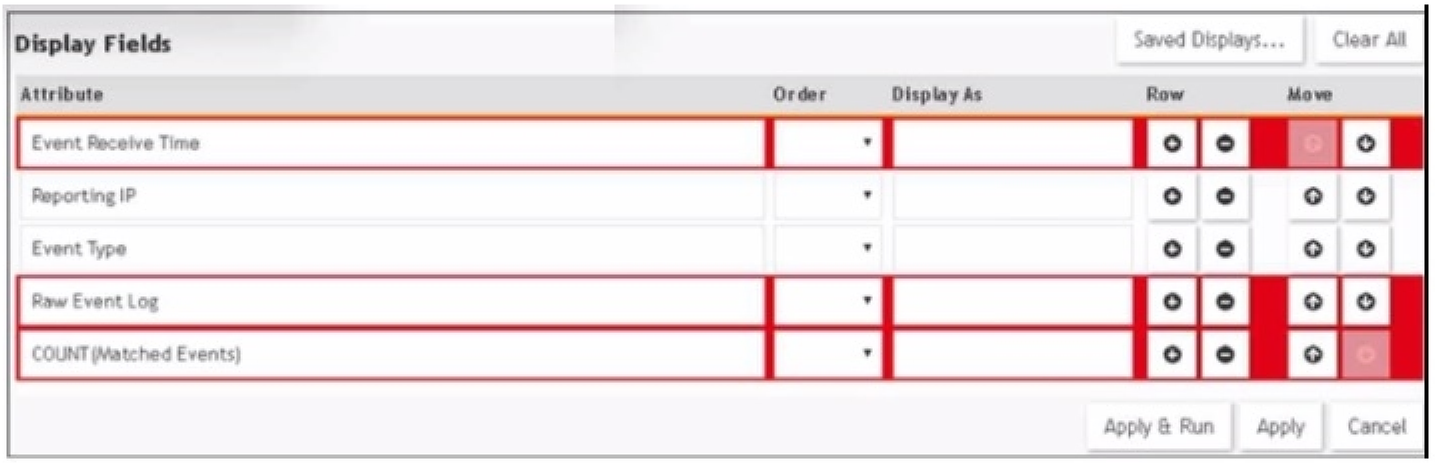
B. Data collection has not started.

C. Data collection execution failed because the device is not reachable.

D. Data collection is paused duo to an issue, such as a change of password.

Correct Answer: D
Section:
Explanation:
Data Collection Status: FortiSIEM displays various icons to indicate the status of data collection for different devices.
Pause Icon: The pause icon specifically indicates that data collection is paused, but this can happen due to several reasons.
Common Cause for Pausing: One common cause for pausing data collection is an issue such as a change of password, which prevents the system from authenticating and collecting data.
Exhibit Analysis: In the provided exhibit, the presence of the pause icon next to the device suggests that data collection has encountered an issue that has caused it to pause.
Reference: FortiSIEM 6.3 User Guide, Device Management and Data Collection Status Icons section, which explains the different icons and their meanings.

QUESTION 18
Refer to the exhibit.



Display Fields

Attribute	Order	Display As	Row	Move
Event Receive Time				
Reporting IP				
Event Type				
Raw Event Log				
COUNT (Matched Events)				

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.

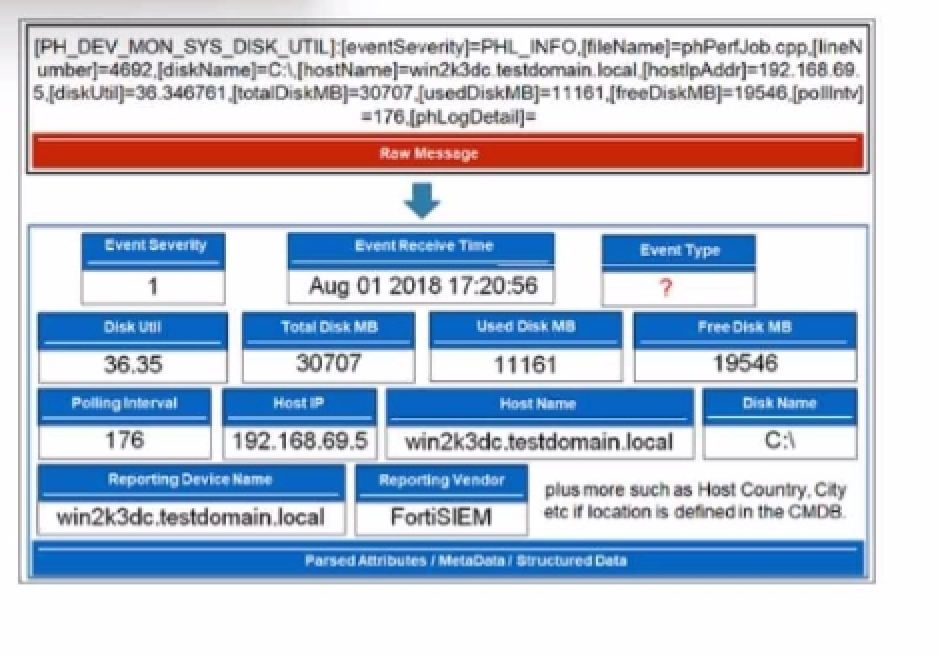
B. The Event Receive Time attribute is not available for logs.

C. The attribute COUNT(Matched events) is an invalid expression.

D. No RAW Event Log attribute is available for devices.

Correct Answer: A
Section:
Explanation:
Grouping Attributes in Reports: When creating reports in FortiSIEM, certain attributes can be grouped to summarize and organize the data.
Unique Attributes: Attributes that are unique for each event cannot be grouped because they do not provide a meaningful aggregation or summary.
Red Highlighting Explanation: The red highlighting in the exhibit indicates attributes that cannot be grouped together due to their unique nature. These unique attributes include Event Receive Time, Reporting IP, Event Type, Raw Event Log, and COUNT(Matched Events).
Attribute Characteristics:
Event Receive Time is unique for each event.
Reporting IP and Event Type can vary greatly, making grouping them impractical in this context.
Raw Event Log represents the unprocessed log data, which is also unique.
COUNT(Matched Events) is a calculated field, not suitable for grouping.
Reference: FortiSIEM 6.3 User Guide, Reporting section, explains the constraints on grouping attributes in reports.

QUESTION 19
Refer to the exhibit.



```
[PH_DEV_MON_SYS_DISK_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,[lineNumber]=4692,[diskName]=C:\,[hostName]=win2k3dc.testdomain.local,[hostIpAddr]=192.168.69.5,[diskUtil]=36.346761,[totalDiskMB]=30707,[usedDiskMB]=11161,[freeDiskMB]=19546,[pollIntv]=176,[phLogDetail]=
```

Raw Message

Event Severity: 1

Event Receive Time: Aug 01 2018 17:20:56

Event Type: ?

Disk Util: 36.35

Total Disk MB: 30707

Used Disk MB: 11161

Free Disk MB: 19546

Polling Interval: 176

Host IP: 192.168.69.5

Host Name: win2k3dc.testdomain.local

Disk Name: C:\

Reporting Device Name: win2k3dc.testdomain.local

Reporting Vendor: FortiSIEM

plus more such as Host Country, City etc if location is defined in the CMDB.

Parsed Attributes / MetaData / Structured Data

Which value will FortiSIEM use to populate the Event Type field?

A. PHL_INFO
B. phPerfJob
C. PH_DSV_MON_SYS_DISK_UTIL
D. diskUtil

Correct Answer: A
Section:
Explanation:
Event Type Population: In FortiSIEM, the Event Type field is populated based on specific identifiers within the raw message or event log.
Raw Message Analysis: The exhibit shows a raw message with various components, including PH_DEV_MON_SYS_DISK_UTIL, PHL_INFO, phPerfJob, and diskUtil.
Primary Event Identifier: The PH_DEV_MON_SYS_DISK_UTIL at the beginning of the raw message is the primary identifier for the event type. It categorizes the type of event, in this case, a system disk utilization monitoring event.
Event Type Field: FortiSIEM uses this primary identifier to populate the Event Type field, providing a clear categorization of the event.
Reference: FortiSIEM 6.3 User Guide, Event Processing and Event Types section, details how event types are identified and populated in the system.

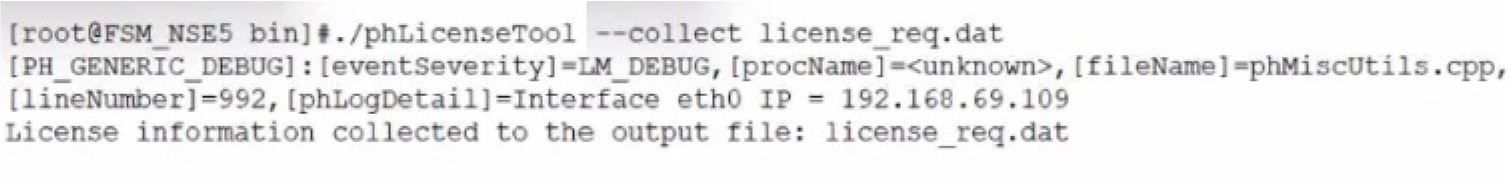
QUESTION 20
An administrator defines SMTP as a critical process on a Linux server.
It the SMTP process is stopped. FortiSIEM will generate a critical event with which event type?

A. Postfix-Mail-Stop
B. PH_DEV_MON_PROC_STOP
C. PH_DEV_MON_SMTP_STOP
D. Generic_SMTP_Procoss_Exit

Correct Answer: B
Section:
Explanation:
Process Monitoring in FortiSIEM: FortiSIEM can monitor critical processes on managed devices, such as an SMTP process on a Linux server.
Event Generation: When a critical process stops, FortiSIEM generates an event to alert administrators.
Event Types: Specific event types correspond to different monitored conditions. For a stopped process, the event type PH_DEV_MON_PROC_STOP is used.

Reasoning: The name PH_DEV_MON_PROC_STOP (Device Monitoring Process Stop) is a generic event type used by FortiSIEM to indicate that any monitored process, including SMTP, has stopped.
Reference: FortiSIEM 6.3 User Guide, Event Types section, explains the predefined event types and their usage in different monitoring scenarios.

QUESTION 21
Refer to the exhibit.



```
[root@FSM_NSE5 bin]#./phLicenseTool --collect license_req.dat
[PH_GENERIC_DEBUG]:[eventSeverity]=LM_DEBUG,[procName]=<unknown>,[fileName]=phMiscUtils.cpp,
[lineNumber]=992,[phLogDetail]=Interface eth0 IP = 192.168.69.109
License information collected to the output file: license_req.dat
```

An administrator is investigating a FortiSIEM license issue.
The procedure is for which offline licensing condition?

A. The procedure is for offline license debug.
B. The procedure is for offline license registration.
C. The procedure is for offline license validation.
D. The procedure is for offline license verification.

Correct Answer: B
Section:
Explanation:
Offline Licensing in FortiSIEM: FortiSIEM provides mechanisms for offline licensing to accommodate environments without direct internet access.
License Tool Command: The command ./phLicenseTool --collect license_req.dat is used to collect license information necessary for offline registration.
Procedure Analysis: The exhibit shows the output of this command, which indicates the collection of license information to a file named license_req.dat.
Offline License Registration: This collected data file is then typically uploaded to the FortiSIEM support portal or provided to the FortiSIEM support team for processing and generating a license file.
Reference: FortiSIEM 6.3 Administration Guide, Licensing section, details the procedures for both online and offline license registration, including the use of the phLicenseTool for offline scenarios.

QUESTION 22
Which FortiSIEM feature must you use to produce a report on which FortiGate devices in your environment are running which firmware version?

A. Run an analytic search.
B. Run a query using the Inventory tab.
C. Run a baseline report.
D. Run a CMDB report

Correct Answer: B
Section:
Explanation:
Feature Overview: FortiSIEM provides several tools for querying and reporting on device information within an environment.
Inventory Tab: The Inventory tab is specifically designed to display detailed information about devices, including their firmware versions.
Query Functionality: Within the Inventory tab, you can run queries to filter and display devices based on specific attributes, such as the firmware version for FortiGate devices.
Report Generation: By running a query in the Inventory tab, you can produce a report that lists the FortiGate devices and their corresponding firmware versions.
Reference: FortiSIEM 6.3 User Guide, Inventory Management section, explains how to use the Inventory tab to query and report on device attributes.

QUESTION 23
Which statement about global thresholds and per device thresholds is true?

A. FortiSIEM uses global and per device thresholds tor all performance metrics.
B. FortiSIEM uses global thresholds for all performance metrics.

C. FortiSIEM uses fixed hardcoded thresholds for all performance metrics.
D. FortiSIEM uses global thresholds for all security metrics.

Correct Answer: A
Section:
Explanation:
Threshold Management: FortiSIEM uses thresholds to generate alerts and incidents based on performance and security metrics.
Global Thresholds: These are default thresholds applied to all devices and metrics across the system, providing a baseline for alerts.
Per Device Thresholds: These thresholds can be customized for individual devices, allowing for more granular control and tailored monitoring based on specific device characteristics and requirements.
Usage in Performance Metrics: Both global and per device thresholds are used for performance metrics to ensure comprehensive and precise monitoring.
Reference: FortiSIEM 6.3 User Guide, Thresholds and Alerts section, details the application of global and per device thresholds for performance and security metrics.

QUESTION 24
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

Correct Answer: D
Section:
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.
Reference: FortiSIEM 6.3 User Guide, Event Search and Filters section, which describes the available attributes and their usage for filtering search results.

QUESTION 25
How is a subpattern for a rule defined?

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

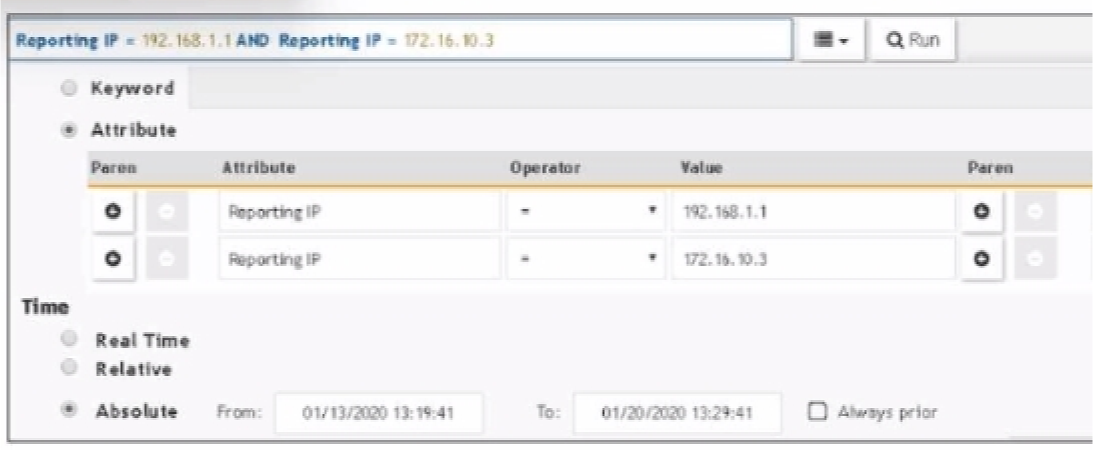
Correct Answer: C
Section:

QUESTION 26
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

Correct Answer: C
Section:
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.
Reference: FortiSIEM 6.3 User Guide, Incident Management section, which details the different categories of incidents and their significance.

QUESTION 27
Refer to the exhibit.



Reporting IP = 192.168.1.1 AND Reporting IP = 172.16.10.3

○ Keyword
● Attribute

Paren	Attribute	Operator	Value	Paren
	Reporting IP	=	192.168.1.1	
	Reporting IP	=	172.16.10.3	

Time
○ Real Time
○ Relative
● Absolute From: 01/13/2020 13:19:41 To: 01/20/2020 13:29:41 □ Always prior

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.

Correct Answer: B
Section:
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.
Reference: 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 28
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.

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

QUESTION 29
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. SVNDB
D. CMDB

Correct Answer: D
Section:
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.
Reference: 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.

QUESTION 30
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.

Correct Answer: D
Section:
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.

Reference: 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.