Fortinet.NSE5_FSM-6.3.v2024-12-28.q41

Exam Code:	NSE5_FSM-6.3
Exam Name:	Fortinet NSE 5 - FortiSIEM 6.3
Certification Provider:	Fortinet
Free Question Number:	41
Version:	v2024-12-28
# of views:	1181
# of Questions views:	410
https://www.freepdfdumps.com/Fortinet.NSE5_FSM-6.3.v2024-12-28.q41.html	

NEW QUESTION: 1
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: C (LEAVE A REPLY)
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.

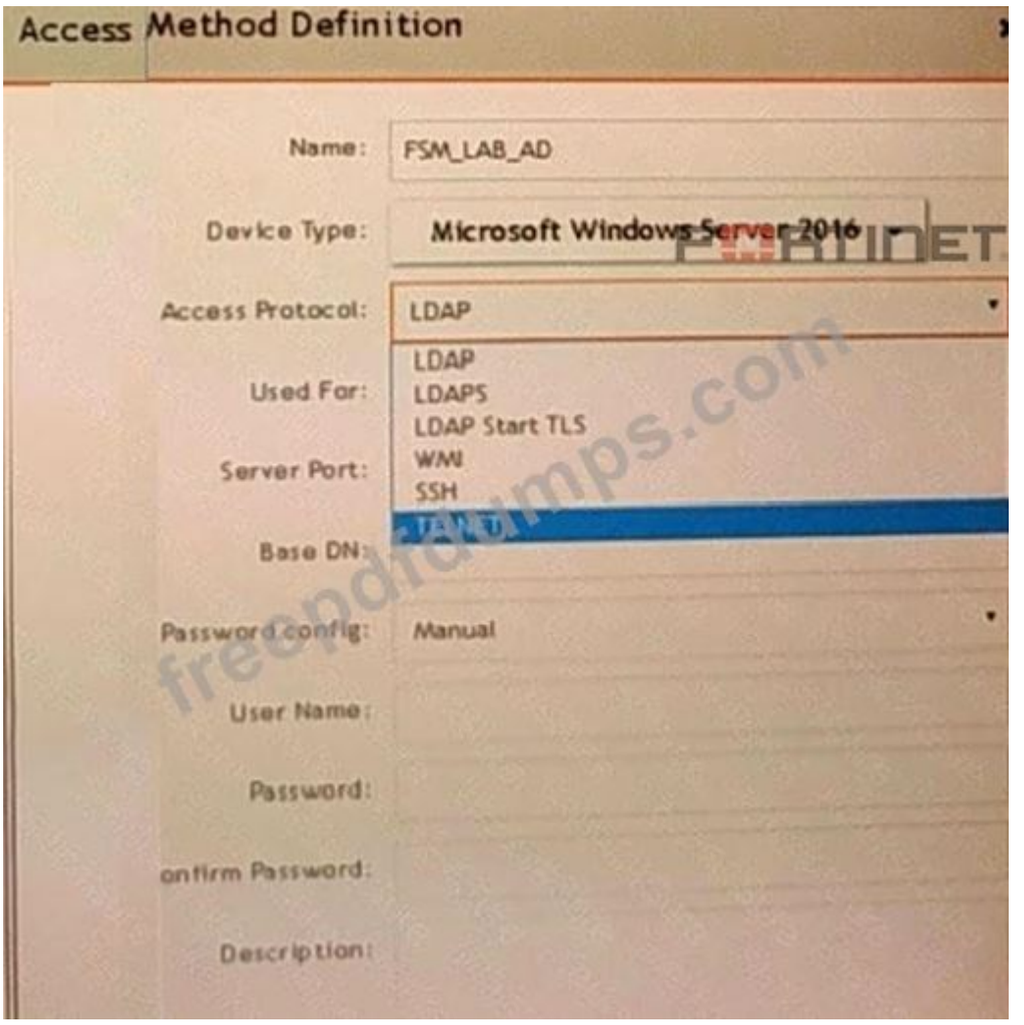
NEW QUESTION: 2
What is a prerequisite for FortiSIEM Linux agent installation?
A. The web server must be installed an the Linux server being monitored

B. Both the web server and the audit service must be installed on the Linux server being monitored
C. The Linux agent manager server must be installed
D. The auditd service must be installed an the Linux server being monitored
Answer: D (LEAVE A REPLY)

NEW QUESTION: 3
Which two FortiSIEM components work together to provide real-time event correlation?
A. Supervisor and collector
B. Worker and collector
C. Collector and Windows agent
D. Supervisor and worker
Answer: (SHOW ANSWER)

NEW QUESTION: 4
Which protocol is almost always required for the FortiSIEM GUI discovery process?
A. WMI
B. SNMP
C. Syslog
D. Telnet
Answer: (SHOW ANSWER)

NEW QUESTION: 5
Refer to the exhibit.



A FortiSIEM administrator wants to collect both SIEM event logs and performance and availability metrics (PAM) events from a Microsoft Windows server Which protocol should the administrator select in the Access Protocol drop-down list so that FortiSIEM will collect both SIEM and PAM events?

A. TELNET

B. WMI

C. LDAPS

D. LDAP start TLS

Answer: (SHOW ANSWER)

Collecting SIEM and PAM Events: To collect both SIEM event logs and Performance and Availability Monitoring (PAM) events from a Microsoft Windows server, a suitable protocol must be selected.

WMI Protocol: Windows Management Instrumentation (WMI) is the appropriate protocol for this task.

* SIEM Event Logs: WMI can collect security, application, and system logs from Windows devices.

* PAM Events: WMI can also gather performance metrics, such as CPU usage, memory utilization, and disk activity.

Comprehensive Data Collection: Using WMI ensures that both types of data are collected efficiently from the Windows server.
References: FortiSIEM 6.3 User Guide, Data Collection Methods section, which details the use of WMI for collecting various types of logs and performance metrics.

NEW QUESTION: 6
Consider thestorage 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
Answer: B (LEAVE A REPLY)
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: 7
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. (COUNT) Matched Events
B. COUNT(Matched Events)
C. Matched Events(COUNT)
D. Matched Events COUNT()
Answer: B (LEAVE A REPLY)

NEW QUESTION: 8
What does the Frequency field determine on a rule?
A. How often the rulewill evaluate the subpattern.
B. How often the rule will trigger for the same condition.
C. How often the rule will trigger.
D. How often the rule will take a clear action.

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

NEW QUESTION: 9
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 FortiSIEM is unable to collect data
C. A yellow star indicates that a metric was applied during discovery, but data collection has not started
D. A yellow star indicates that a metric was not applied during discovery and, therefore, FortiSIEM was unable to collect data.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 10
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. Data Conditions
B. CMDB Report Conditions
C. UI Access
Answer: A (LEAVE A REPLY)

NEW QUESTION: 11
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 (LEAVE A REPLY)

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 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: 12

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 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: (SHOW ANSWER)

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.

NEW QUESTION: 13

Which process converts raw log data to structured data?

A. Data classification

B. Data enrichment

C. Data parsing

D. Data validation

Answer: C (LEAVE A REPLY)

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.
References: FortiSIEM 6.3 User Guide, Data Parsing section, which details how raw log data is transformed into structured data through parsing.

NEW QUESTION: 14
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
Answer: D (LEAVE A REPLY)
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
Which database is used for storing anomaly data, that is calculated for different parameters, such as traffic and device resource usage running averages, and standard deviation values?
A. Event DB
B. Profile DB
C. CMDB
D. SVN DB
Answer: B (LEAVE A REPLY)

NEW QUESTION: 16

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

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

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

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

D. The collector buffers events

Answer: A (LEAVE A REPLY)

NEW QUESTION: 17

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_SMTP_STOP

B. Postfix-Mail-Slop

C. PH_DEV_MON_PROC_STOP

D. Generic SMTP Process Exit

Answer: C (LEAVE A REPLY)

NEW QUESTION: 18

Which FortiSIEM components can do performance availability and performance monitoring?

A. Supervisor only

B. Collectors only

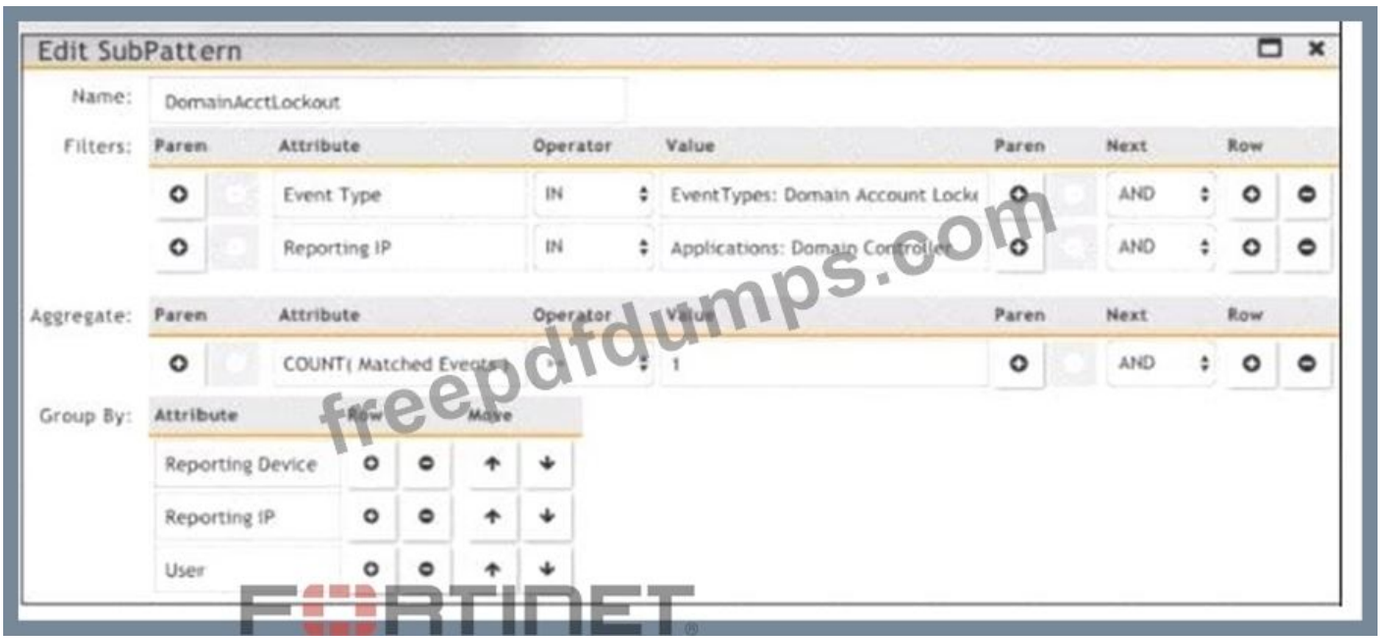
C. Supervisor, worker, and collector

D. Supervisor and workers only

Answer: C (LEAVE A REPLY)

NEW QUESTION: 19

Refer to the exhibit.



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

A. Actions

B. Group By

C. Aggregate

D. Filters

Answer: B (LEAVE A REPLY)

Incident Creation in FortiSIEM: Incidents in FortiSIEM are created based on specific patterns and conditions defined within the system.

Group By Function: The "Group By" section in the "Edit SubPattern" window specifies how the data should be grouped for analysis and incident creation.

Impact of Grouping: The way data is grouped affects the number of incidents generated. Each unique combination of the grouped attributes results in a separate incident.

Exhibit Analysis: In the provided exhibit, the "Group By" section lists "Reporting Device," "Reporting IP," and "User." This means incidents will be created for each unique combination of these attributes.

References: FortiSIEM 6.3 User Guide, Rule and Pattern Creation section, which details how grouping impacts incident generation.

NEW QUESTION: 20

How was the FortiGate device discovered by FortiSIEM?

A. using the pull events method

B. Through auto lag discovery

C. Through syslog discovery

D. Through GUI log discovery

Answer: (SHOW ANSWER)

NEW QUESTION: 21

Refer to the exhibit.

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.

Answer: D (LEAVE A REPLY)

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.

References: FortiSIEM 6.3 User Guide, Device Management and Data Collection Status Icons section, which explains the different icons and their meanings.

NEW QUESTION: 22

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: (SHOW ANSWER)

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: 23
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 (LEAVE A REPLY)
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: 24
If a performance rule is triggered repeatedly due to high CPU use. what occurs m the incident table?
A. The Incident Count value increases, and the First Seen and Last Seen tomes update
B. A new incident is created each time the rule is triggered, and the First Seen and Last Seen times are updated.
C. A new incident is created based an the Rule Frequency value, and the First Seen and Last Seen times are updated
D. The incident status changes to Repeated and the First Seen and Last Seen times are updated
Answer: (SHOW ANSWER)

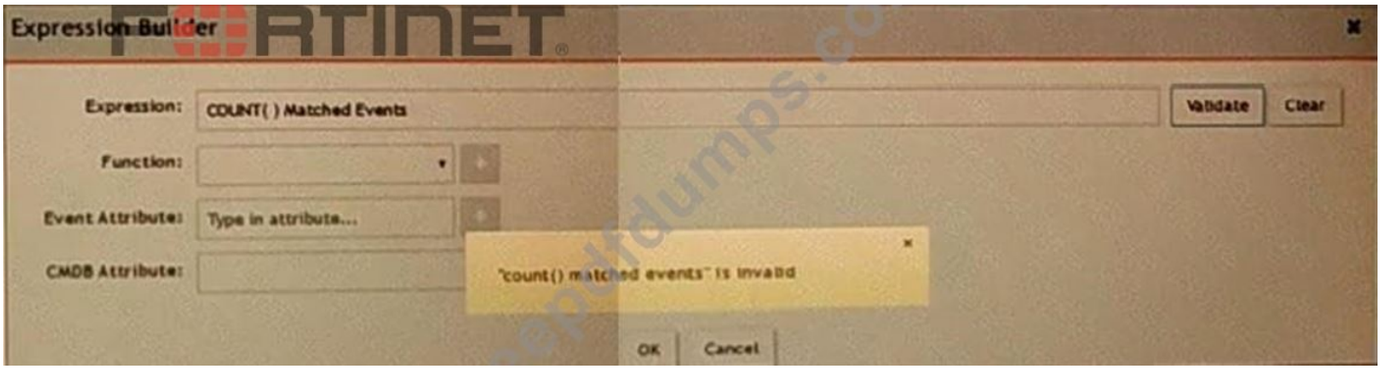
NEW QUESTION: 25
Which process converts raw log data to structured data?
A. Data classification
B. Data validation
C. Data parsing
D. Data enrichment

Answer: (SHOW ANSWER)
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.
References: FortiSIEM 6.3 User Guide, Data Parsing section, which details how raw log data is transformed into structured data through parsing.

NEW QUESTION: 26
What operating system is FortiSIEM based on?
A. Cent OS
B. Microsoft Windows
C. RedHat
D. Ubuntu
Answer: A (LEAVE A REPLY)

NEW QUESTION: 27
In FortiSIEM enterprise licensing mode, if the link between the collector and data center FortiSIEM cluster a down what happens?
A. The collector buffers events
B. The collector continues performance collection of devices, but stops receiving syslog
C. The collector drops incoming events like syslog, but slops performance collection
D. The collector processes stop, and events are dropped
Answer: A (LEAVE A REPLY)

NEW QUESTION: 28
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 (LEAVE A REPLY)
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 isCOUNT(Matched Events).
* Function:COUNTis 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: 29
Which process converts raw log data to structured data?
A. Data classification
B. Data validation
C. Data parsing
D. Data enrichment
Answer: (SHOW ANSWER)
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.
References: FortiSIEM 6.3 User Guide, Data Parsing section, which details how raw log data is transformed into structured data through parsing.

NEW QUESTION: 30
Device discovery information is stored in which database?
A. CMDB

B. Profile DB
C. Event DB
D. SVN DB
Answer: A (LEAVE A REPLY)
Device Discovery Information: Information about discovered devices, including their configurations and statuses, is stored in a specific database.
CMDB: The Configuration Management Database (CMDB) is used to store detailed information about the devices discovered by FortiSIEM.
* Function: It maintains comprehensive details about device configurations, relationships, and other metadata essential for managing the IT infrastructure.
Significance: Storing discovery information in the CMDB ensures that the FortiSIEM system has a centralized repository of device information, facilitating efficient management and monitoring.
References: FortiSIEM 6.3 User Guide, Configuration Management Database (CMDB) section, which details the storage and usage of device discovery information.

NEW QUESTION: 31
Which discovery scan type is prone to miss a device, if the device is quiet and the entry foe 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: (SHOW ANSWER)
Discovery Scan Types: FortiSIEM uses various scan types to discover devices on a network.
Layer 2 (L2) Scan: An L2 scan discovers devices based on ARP tables and MAC address information from adjacent devices.
* Limitation: If a device is quiet (not actively communicating) and its entry is not present in the ARP table of adjacent devices, the L2 scan may miss it.
Other Scan Types:
* CMDB Scan: Based on the existing Configuration Management Database (CMDB) entries.
* Range Scan: Scans a specified IP range for devices.
* Smart Scan: Uses a combination of methods to discover devices.
References: FortiSIEM 6.3 User Guide, Device Discovery section, which explains the different types of discovery scans and their characteristics.

NEW QUESTION: 32
Which three ports can be used to send Syslogs to FortiSIEM? (Choose three.)
A. UDP9999
B. UDP 162
C. TCP 514
D. UDP 514
E. TCP 1470
Answer: C,D,E (LEAVE A REPLY)
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.

NEW QUESTION: 33
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 (LEAVE A REPLY)
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: 34
A customer is experiencing slow performance while executing long, adhoc analytic searches
Which FortiSIEM component can make the searches run faster?
A. Correlation worker
B. Event worker
C. Storage worker
D. Query worker
Answer: D (LEAVE A REPLY)
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.

NEW QUESTION: 35
A FortiSIEM administrator wants to collect both SIEM event logs and performance and availability metrics (PAM) events from a Microsoft Windows server
Which protocol should the administrator select in the AccessProtocol drop-down list so that FortiSIEM will collect both SIEM and PAM events?
A. WMI
B. TELNET
C. LDAPS
D. LDAP start TLS
Answer: A (LEAVE A REPLY)

NEW QUESTION: 36
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: A (LEAVE A REPLY)

Incident Status Values: Incident statuses in FortiSIEM help administrators track and manage the lifecycle of incidents from detection to resolution.
Four Possible Status Values:
* Active: Indicates that the incident is currently ongoing and needs attention.
* Closed: Indicates that the incident has been resolved or addressed.
* Cleared: Indicates that the incident has been resolved automatically based on predefined conditions.
* Open: Indicates that the incident is acknowledged and under investigation but not yet resolved.
Usage: These statuses help in prioritizing and tracking incidents effectively, ensuring that all incidents are appropriately managed.
References: FortiSIEM 6.3 User Guide, Incident Management section, which details the different status values and their meanings.

NEW QUESTION: 37
Which two export methods are available for FortiSIEM analytics results? (Choose two.)
A. PNG
B. csv
C. HTML
D. PDF
Answer: (SHOW ANSWER)

NEW QUESTION: 38
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 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 (LEAVE A REPLY)
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.

NEW QUESTION: 39
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: (SHOW ANSWER)
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 discovery and data has been collected for that metric.

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: 40
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
Answer: D (LEAVE A REPLY)
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: 41
To determine SNMP discovery issues, which is the best command from the backend?
A. snmpwalk
B. phSNMPTest
C. snmptest
Answer: A (LEAVE A REPLY)