Free Questions for NSE5_FSM-6.3

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 command displays the Linux agent status?

Options:

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

Answer:

C

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 2

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.

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

Question 3

Question Type: MultipleChoice

What are the four possible incident status values?

Options:

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

Explanation:

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.

Reference: FortiSIEM 6.3 User Guide, Incident Management section, which details the different status values and their meanings.

Question 4

Question Type: MultipleChoice

In the advanced analytical rules engine in FortiSIEM, multiple subpatterms can be referenced using which three operation?(Choose three.)

Options:

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

Answer:

C, D, E

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.

Reference: FortiSIEM 6.3 User Guide, Advanced Analytics Rules Engine section, which explains the use of different operations to reference subpatterns in rules.

Question 5

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:

A

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 6

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.

Reference: 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 7

Question Type: MultipleChoice

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?

Options:

A- Profile DB
B- Event DB
C- CMDB
D- SVN DB

Answer:

A

Explanation:

Anomaly Data Storage: Anomaly data, including running averages and standard deviation values for different parameters such as traffic and device resource usage, is stored in a specific database.

Profile DB: The Profile DB is used to store this type of anomaly data.

Function: It maintains statistical profiles and baselines for monitored parameters, which are used to detect anomalies and deviations from normal behavior.

Significance: Storing anomaly data in the Profile DB allows FortiSIEM to perform advanced analytics and alerting based on deviations from established baselines.

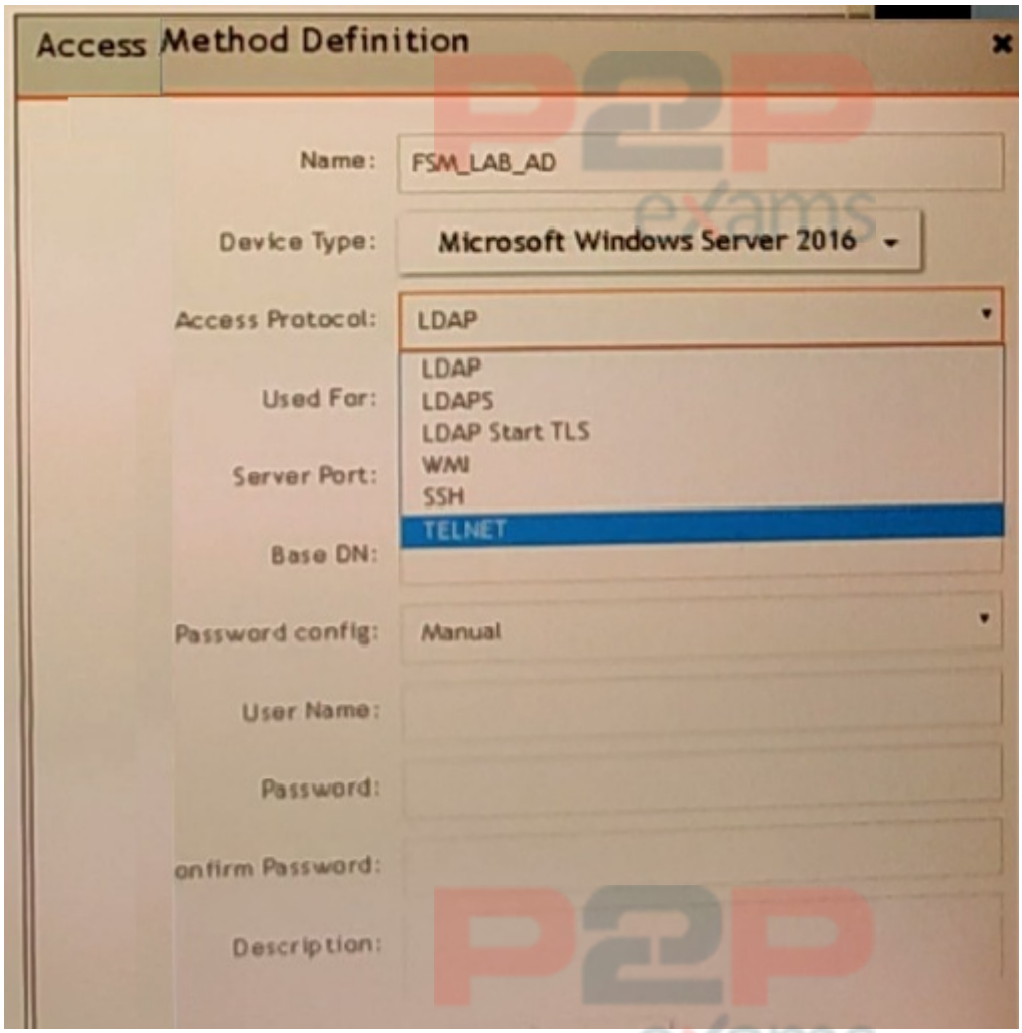
Reference: FortiSIEM 6.3 User Guide, Database Architecture section, which describes the purpose

and contents of the Profile DB in storing anomaly and baseline data.

Question 8

Question Type: MultipleChoice

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?

Options:

A- TELNET

B- WMI

C- LDAPS
D- LDAP start TLS

Answer:

B

Explanation:

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.

Reference: FortiSIEM 6.3 User Guide, Data Collection Methods section, which details the use of WMI for collecting various types of logs and performance metrics.

Question 9

Question Type: MultipleChoice

What is a prerequisite for FortiSIEM Linux agent installation?

Options:

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:

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: The auditd service, 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.

Reference: FortiSIEM 6.3 User Guide, Linux Agent Installation section, which lists the prerequisites and steps for installing the FortiSIEM Linux agent.

Question 10

Question Type: MultipleChoice

Consider the storage of anomaly baseline date that is calculated for different parameters. Which database is used for storing this data?

Options:

A- Event DB
B- Profile DB
C- SVNDB
D- CMDB

Answer:

D

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.

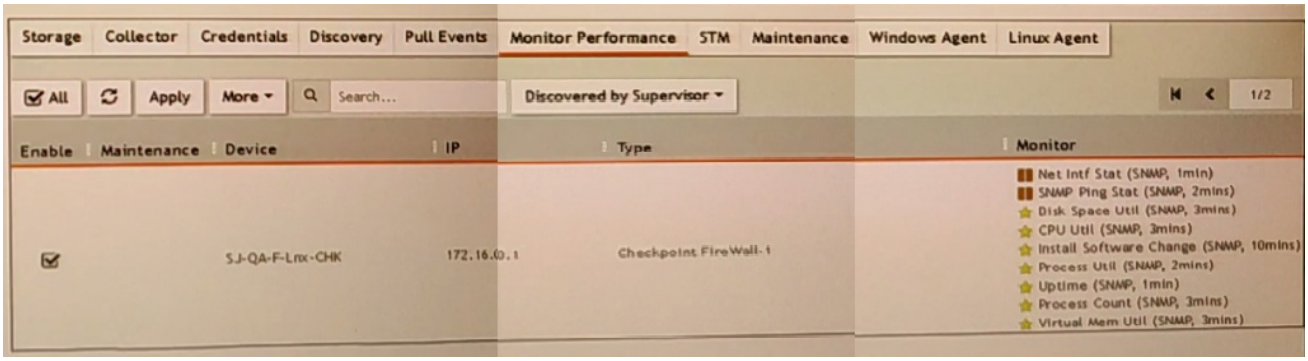
Usage: This data is used by FortiSIEM to compare real-time metrics against the established baselines to identify anomalies.

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 11

Question Type: MultipleChoice

Refer to the exhibit.



What do the yellow stars listed in the Monitor column indicate?

Options:

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 discovery and data has been collected for that metric.

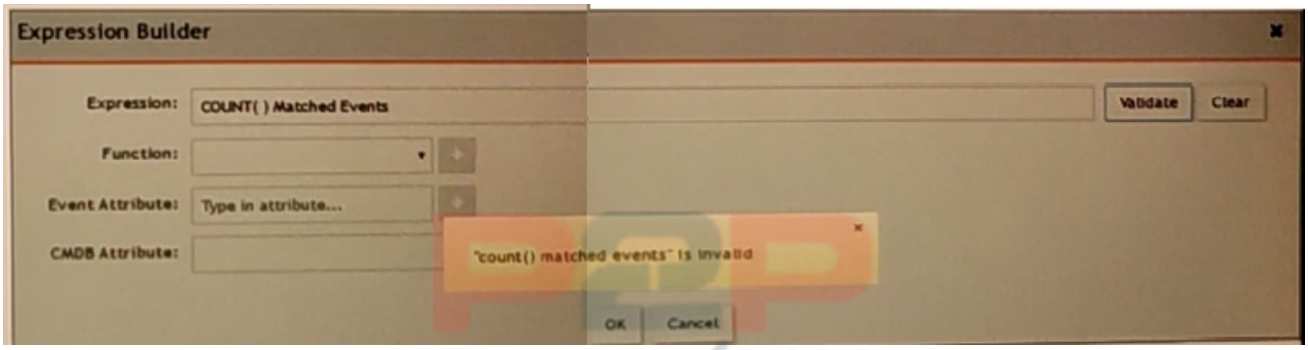
Successful Data Collection: This visual indicator helps administrators quickly identify which metrics are active and have data available for analysis.

Reference: FortiSIEM 6.3 User Guide, Device Monitoring section, which explains the significance of different icons and indicators in the Monitor column.

Question 12

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.

Reference: FortiSIEM 6.3 User Guide, Expression Builder section, which explains the correct syntax and usage for creating valid expressions for event analysis.