

Fortinet

Exam Questions NSE5_FSM-6.3

Fortinet NSE 5 - FortiSIEM 6.3



NEW QUESTION 1

What is a prerequisite for FortiSIEM Linux agent installation?

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

Answer: B

Explanation:

Explanation

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

Prerequisite for Installation: 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.

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

NEW QUESTION 2

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

Answer: A

Explanation:

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.

References: FortiSIEM 6.3 User Guide, Database Architecture section, which describes the purpose and contents of the Profile DB in storing anomaly and baseline data.

NEW QUESTION 3

An administrator is in the process of renewing a FortiSIEM license. Which two commands will provide the system ID? (Choose two.)

- A. phgetHWID
- B. ./phLicenseTool - support
- C. phgetUUID
- D. ./phLicenseTool-show

Answer: AC

Explanation:

License Renewal Process: When renewing a FortiSIEM license, it is essential to provide the system ID, which uniquely identifies the FortiSIEM instance.

Commands to Retrieve System ID:

phgetHWID: This command retrieves the hardware ID of the FortiSIEM appliance.

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

phgetUUID: This command retrieves the universally unique identifier (UUID) for the FortiSIEM system.

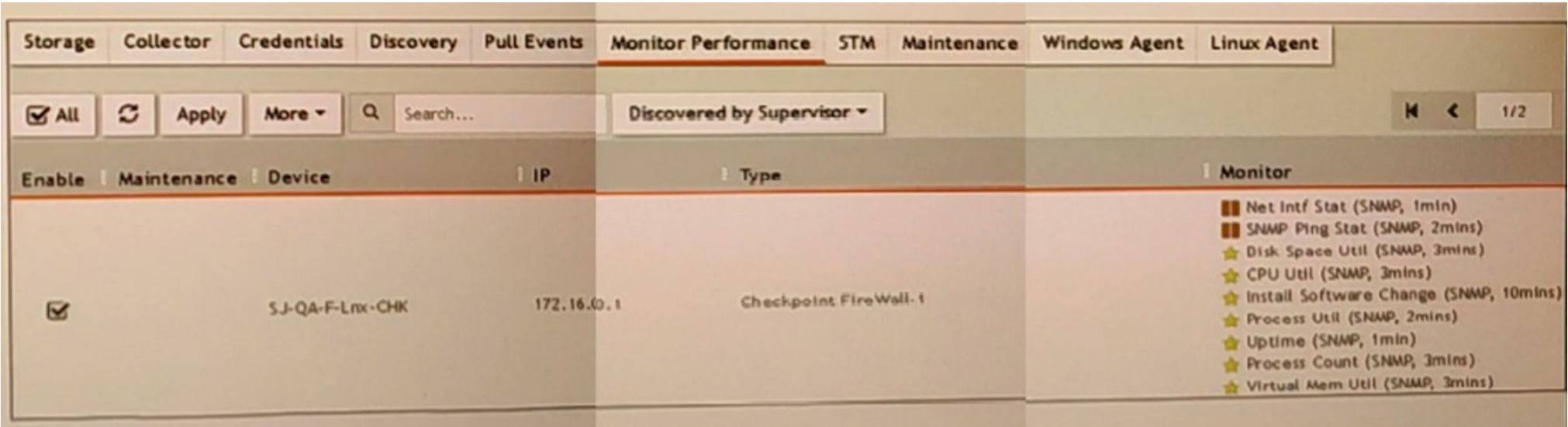
Usage: Run the command phgetUUID in the CLI to obtain the UUID.

Verification: Both phgetHWID and phgetUUID are valid commands for retrieving the necessary system IDs required for license renewal.

References: FortiSIEM 6.3 Administration Guide, Licensing section details the commands and procedures for obtaining system identification information necessary for license renewal.

NEW QUESTION 4

Refer to the exhibit.



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

- A. A yellow star indicates that a metric was applied during discovery, and data has been collected successfully
- B. A yellow star indicates that a metric was applied during discovery, but data collection has not started
- C. A yellow star indicates that a metric was applied during discovery, but FortiSIEM is unable to collect data.
- D. A yellow star indicates that a metric was not applied during discovery and, therefore, FortiSEIM was unable to collect data.

Answer: A

Explanation:

Monitor Column Indicators: In FortiSIEM, the Monitor column displays the status of various metrics applied during the discovery process.
Yellow Star Meaning: A yellow star next to a metric indicates that the metric was successfully applied during
Successful Data Collection: This visual indicator helps administrators quickly identify which metrics are active and have data available for analysis.
References: FortiSIEM 6.3 User Guide, Device Monitoring section, which explains the significance of different icons and indicators in the Monitor column.

NEW QUESTION 5

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

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

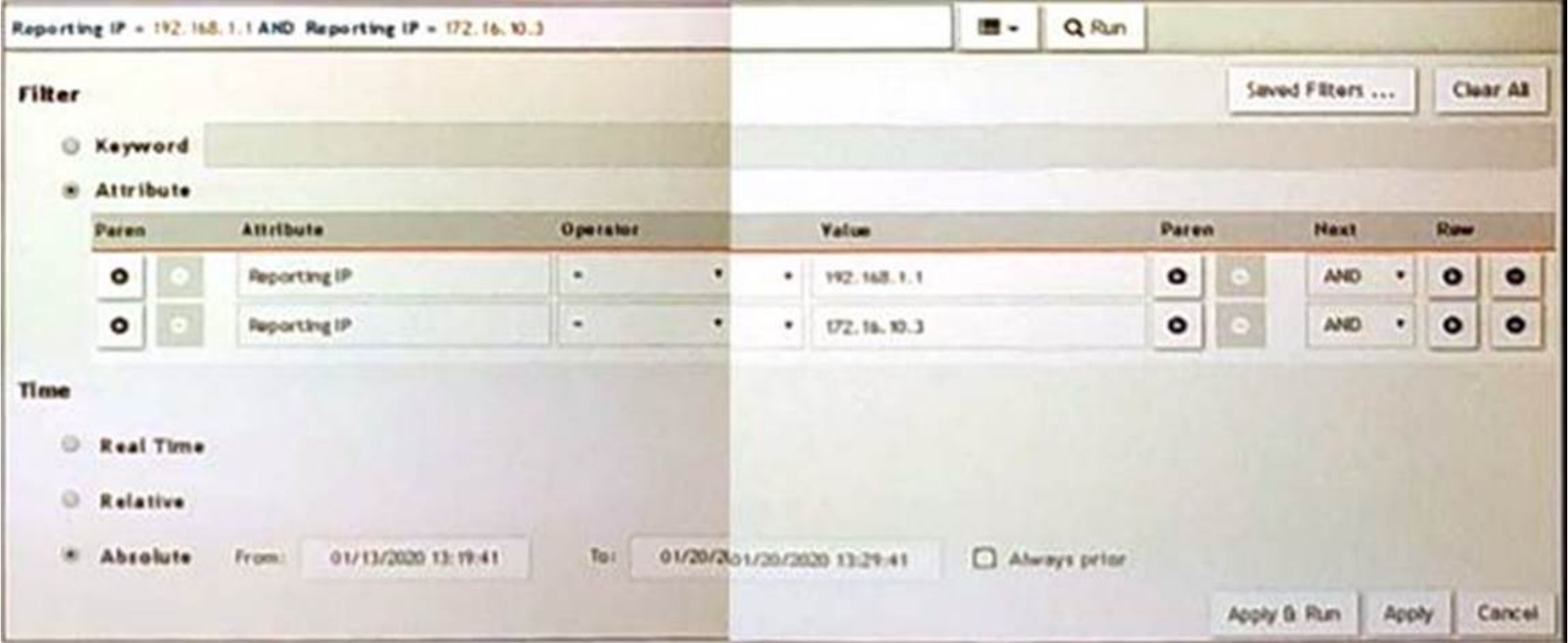
Answer: CDE

Explanation:

Advanced Analytical Rules Engine: FortiSIEM's rules engine allows for complex event correlation using multiple subpatterns.
Operations for Referencing Subpatterns:
FOLLOWED_BY: This operation is used to indicate that one event follows another within a specified time window.
OR: This logical operation allows for the inclusion of multiple subpatterns, where the rule triggers if any of the subpatterns match.
AND: This logical operation requires all referenced subpatterns to match for the rule to trigger.
Usage: These operations allow for detailed and precise event correlation, helping to detect complex patterns and incidents.
References: FortiSIEM 6.3 User Guide, Advanced Analytics Rules Engine section, which explains the use of different operations to reference subpatterns in rules.

NEW QUESTION 6

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?

- A. Parenthesis are missing

- B. The wrong boolean operator is selected in the Next column
- C. The wrong option is selected in the Operator column
- D. An invalid IP subnet is typed in the Value column

Answer: B

NEW QUESTION 7

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

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

Answer: D

NEW QUESTION 8

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

- A. Two hours have passed since the incident occurred and the incident has not reoccurred.
- B. A clear condition set on a rule was satisfied.
- C. A security rule issue has been resolved.
- D. The incident was cleared by an operator.

Answer: B

NEW QUESTION 9

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

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

Answer: B

NEW QUESTION 10

What is a prerequisite for a FortiSIEM supervisor with a worker deployment, using the proprietary flat file database?

- A. The CMDB database must be on NFS
- B. The event database must be on NFS
- C. The event database must be on a local disk
- D. The \archive mount must be on a local disk

Answer: B

NEW QUESTION 10

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

NSE5_FSM-6.3 Practice Exam Features:

- * NSE5_FSM-6.3 Questions and Answers Updated Frequently
- * NSE5_FSM-6.3 Practice Questions Verified by Expert Senior Certified Staff
- * NSE5_FSM-6.3 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE5_FSM-6.3 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

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