Free Questions for NSE5_FSM-6.3 by dumpssheet

Shared by Hurley on 10-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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.

Options:

A- External Event Receive Protocol

B- Event Received Proto Agents

C- External Event Receive Raw Logs

D- External Event Receive Agents

Answer:

D

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.

References: FortiSIEM 6.3 User Guide, Event Search and Filters section, which describes the available attributes and their usage for filtering search results.

Question 2

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.

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

Question 3

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.

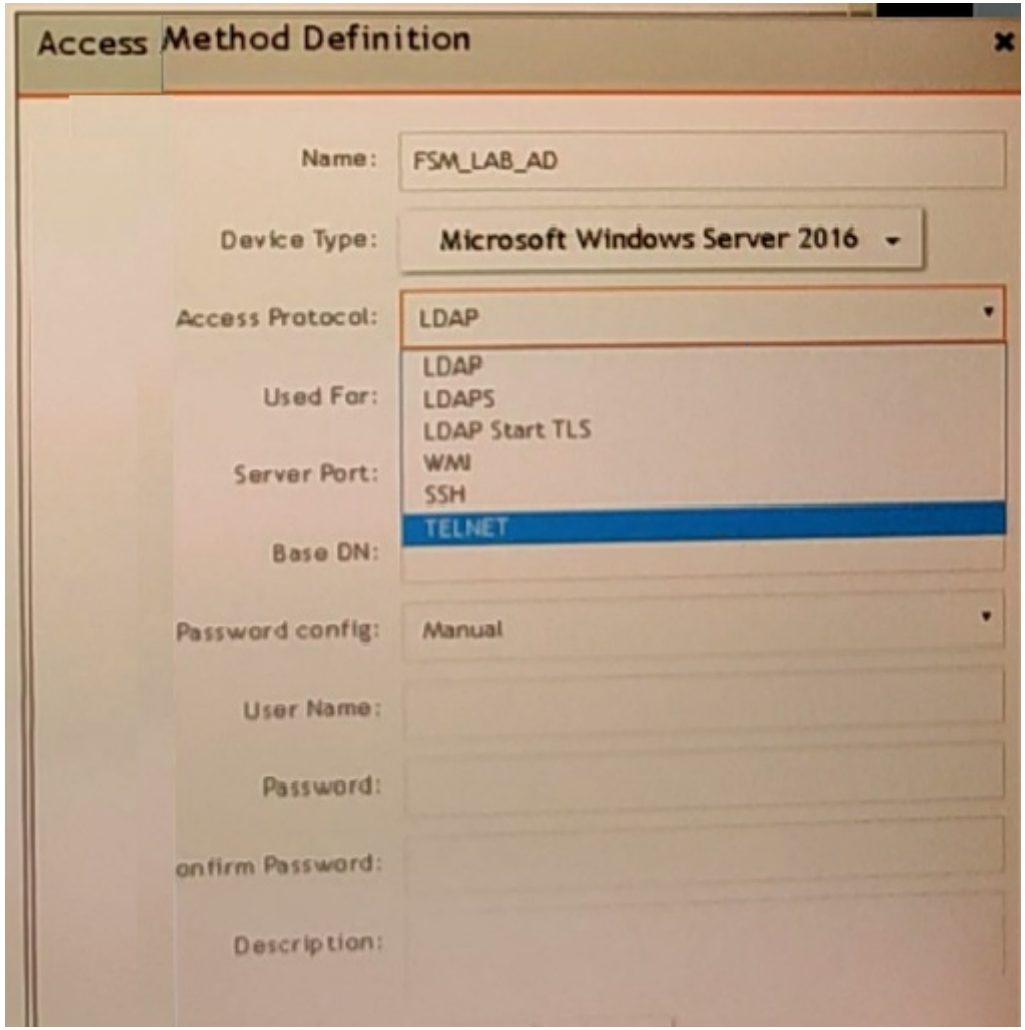
Significance: Storing anomaly data in the Profile DB allows FortiSIEM to perform advanced analytics and alerting based on deviations from established baselines.

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.

Question 4

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.

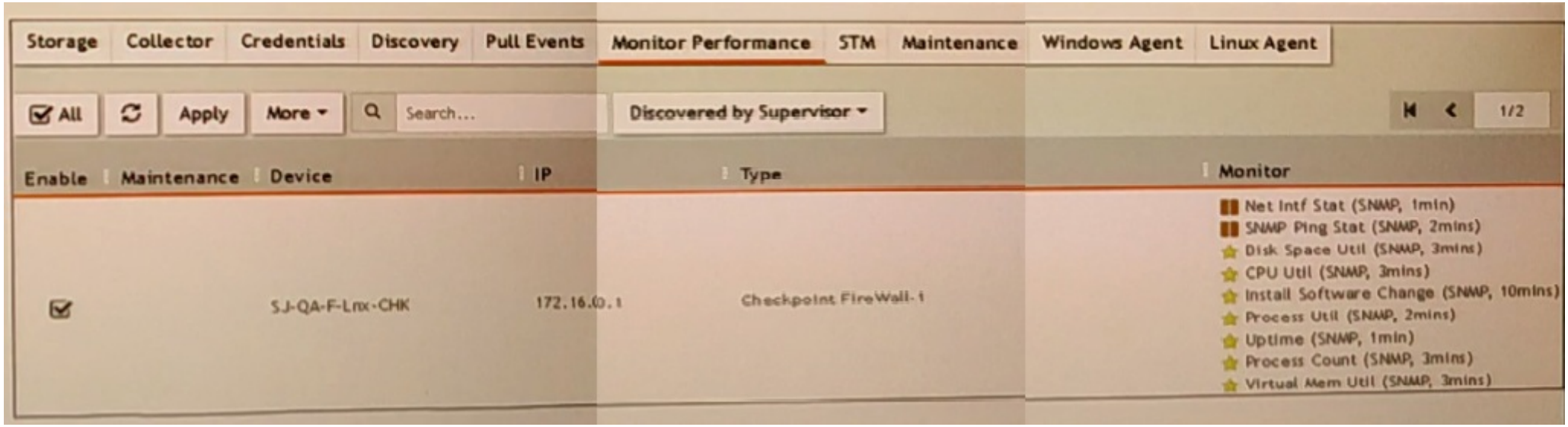
Comprehensive Data Collection: Using WMI ensures that both types of data are collected efficiently from the Windows server.

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.

Question 5

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.

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

Question 6

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.

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

Question 7

Question Type: MultipleChoice

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?

Options:

A- CMDB scan

B- L2 scan

C- Range scan

D- Smart scan

Answer:

B

Explanation:

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.

Question 8

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.

References: FortiSIEM 6.3 User Guide, Linux Agent Installation and Management section, which includes commands for managing the Linux agent.

Question 9

Question Type: MultipleChoice

Which FortiSIEM components can do performance availability and performance monitoring?

Options:

A- Supervisor, worker, and collector

B- Supervisor and workers only

C- Supervisor only

D- Collectors only

Answer:

A

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.

References: FortiSIEM 6.3 User Guide, Performance and Availability Monitoring section, which explains the roles of the supervisor, worker, and collector in monitoring tasks.

Question 10

Question Type: MultipleChoice

Device discovery information is stored in which database?

Options:

A- CMDB

B- Profile DB

C- Event DB

D- SVN DB

Answer:

A

Explanation:

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.

Question 11

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.

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

To Get Premium Files for NSE5_FSM-6.3 Visit

https://www.p2pexams.com/products/nse5_fsm-6.3

For More Free Questions Visit

https://www.p2pexams.com/fortinet/pdf/nse5-fsm-6.3