Exam Questions NSE5_FSM-6.3

Fortinet NSE 5 - FortiSIEM 6.3

https://www.2passeasy.com/dumps/NSE5_FSM-6.3/

NEW QUESTION 1
Which FortiSIEM components are capable of performing device discovery?

A. FortiSIEM Windows agent
B. Worker
C. FortiSIEM Linux agent
D. Collector

Answer: D

Explanation:
Explanation
Device Discovery in FortiSIEM: Device discovery is the process by which FortiSIEM identifies and adds devices to its management scope.
Role of Collectors: Collectors are responsible for gathering data from network devices, including discovering new devices in the network.
- Functionality: Collectors use protocols such as SNMP, WMI, and others to discover devices and gather their details.

Capability: While agents (Windows and Linux) primarily gather data from their host systems, the collectors actively discover devices across the network.
References: FortiSIEM 6.3 User Guide, Device Discovery section, which details the role of collectors in discovering network devices.

NEW QUESTION 2
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

Answer: C

Explanation:
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.
References: FortiSIEM 6.3 User Guide, Incident Management section, which details the different categories of incidents and their significance.

NEW QUESTION 3
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.

Answer: D

Explanation:
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.
References: FortiSIEM 6.3 User Guide, Data Collection Methods section, which details the use of WMI for collecting event logs from Windows devices.

NEW QUESTION 4
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 triggere
B. and the First Seen and Last Seen times are updated.
C. A new incident is created based on the Rule Frequency value, and the First Seen and Last Seen times ate updated.
D. The Incident Count value increases, and the First Seen and Last Seen times update.
E. The incident status changes to Repeated, and the First Seen and Last Seen times are updated.

Answer: C

Explanation:
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.

References: FortiSIEM 6.3 User Guide, Incident Management section, explains how FortiSIEM handles recurring incidents and updates the incident table accordingly.

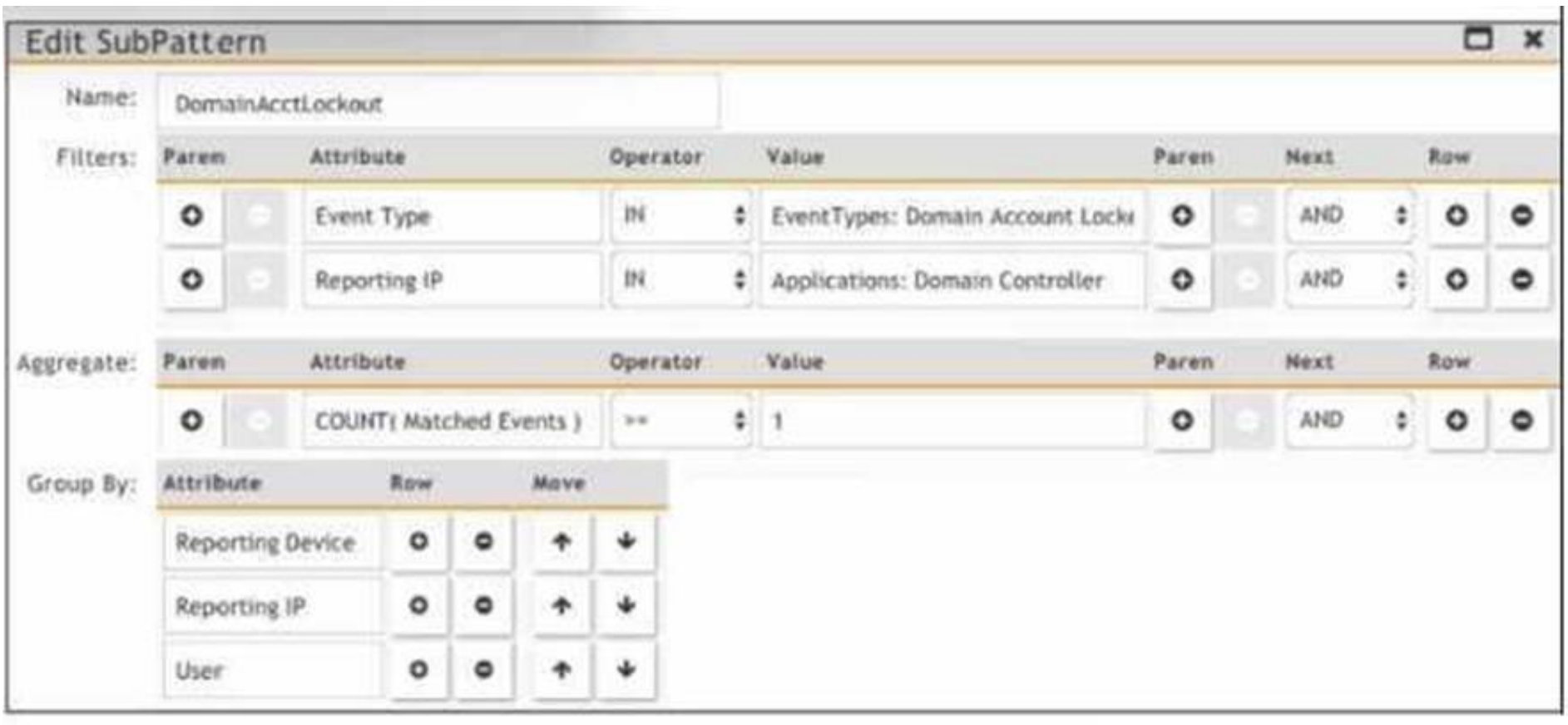
NEW QUESTION 5
When configuring collectors located in geographically separated sites, what ports must be open on a front end firewall?

A. HTTPS, from the collector to the worker upload settings address only
B. HTTPS, from the collector to the supervisor and worker upload settingsaddresses
C. HTTPS, from the Internet to the collector
D. HTTPS, from the Internet to the collector and from the collector to the FortiSIEM cluster

Answer: B

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.
References: FortiSIEM 6.3 Administration Guide, Network Ports section details the necessary ports for communication within the FortiSIEM architecture.

NEW QUESTION 6
Refer to the exhibit.



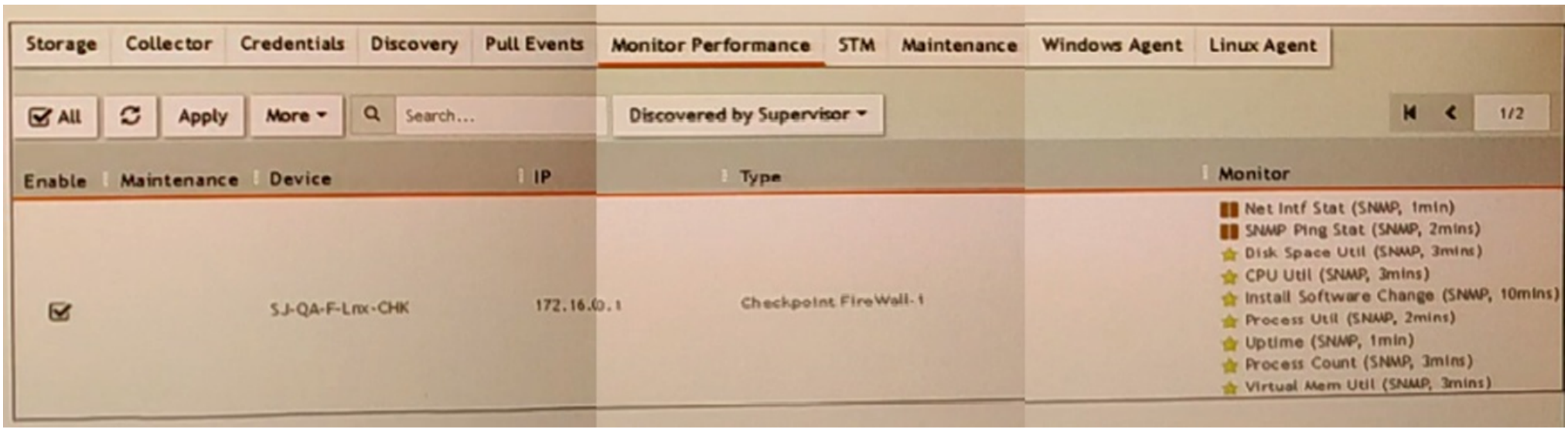
Which section contains the sortings that determine how many incidents are created?

A. Actions
B. Group By
C. Aggregate
D. Filters

Answer: B

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

NEW QUESTION 7
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 8
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

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.

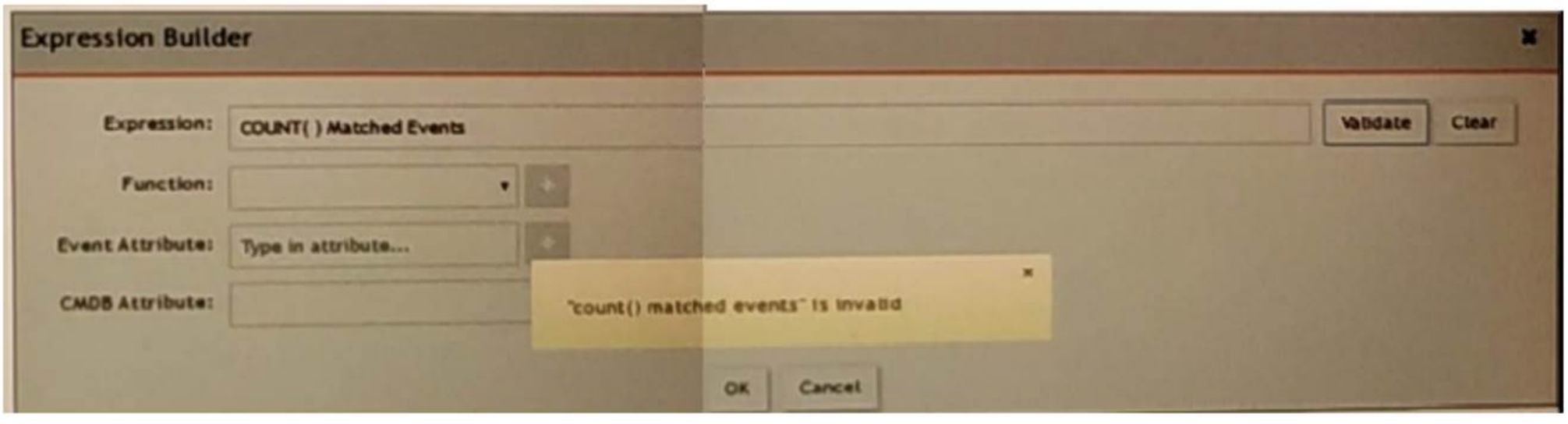
NEW QUESTION 9
Which three ports can be used to send Syslogs to FortiSIEM? (Choose three.)
Options:

A. UDP9999
B. UDP 162
C. TCP 514
D. UDP 514
E. TCP 1470

Answer: CDE

Explanation:
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 10
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

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.
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 10
In the rules engine, which condition instructs FortiSIEM to summarize and count the matching evaluated data?

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

NEW QUESTION 15
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. SVN DB
D. CMDB

Answer: B

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.
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 18
In the advanced analytical rules engine in FortiSIEM, multiple subpatterms 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 23
In FortiSIEM enterprise licensing mode, it the link between the collector and data center FortiSlEM cluster is down, what happens?

A. The collector drops incoming events like syslo
B. but stops performance collection.
C. The collector processes stop, and events ate dropped.
D. The collector continues performance collection of devices, but slops receiving syslog.
E. The collector buffers events

Answer: D

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.
References: FortiSIEM 6.3 User Guide, Data Collection and Buffering section, explains the behavior of collectors during network disruptions.

NEW QUESTION 24
What protocol can be used to collect Windows event logs in an agentless method?

A. SSH
B. SNMP
C. WMI
D. SMTP

Answer: C

NEW QUESTION 25
What operating system is FortiSIEM based on?

A. Cent OS
B. Microsoft Windows
C. RedHat
D. Ubuntu

Answer: A

NEW QUESTION 29
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

Answer: A

NEW QUESTION 33
What is the best discovery scan option for a network environment where ping is disabled on all network devices?

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

Answer: A

NEW QUESTION 34
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: C

NEW QUESTION 36
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: D

NEW QUESTION 40
What are the minimum memory requirements for the FortiSIEM supervisor virtual appliance, when the proprietary flat file database is used?

A. 16GB RAM
B. 32GB RAM
C. 64GB RAM
D. 24GB RAM

Answer: D

NEW QUESTION 41
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 45
Device discovery information is stored in which database?

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

Answer: A

NEW QUESTION 49
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE5_FSM-6.3 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE5_FSM-6.3 Product From:

https://www.2passeasy.com/dumps/NSE5_FSM-6.3/

Money Back Guarantee

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