Fortinet

Exam Questions NSE5_FSM-6.3

Fortinet NSE 5 - FortiSIEM 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
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 3
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 4
An administrator is in the process of renewing a FortiSIEM license. Which two commands will provide the system ID? (Choose two.)

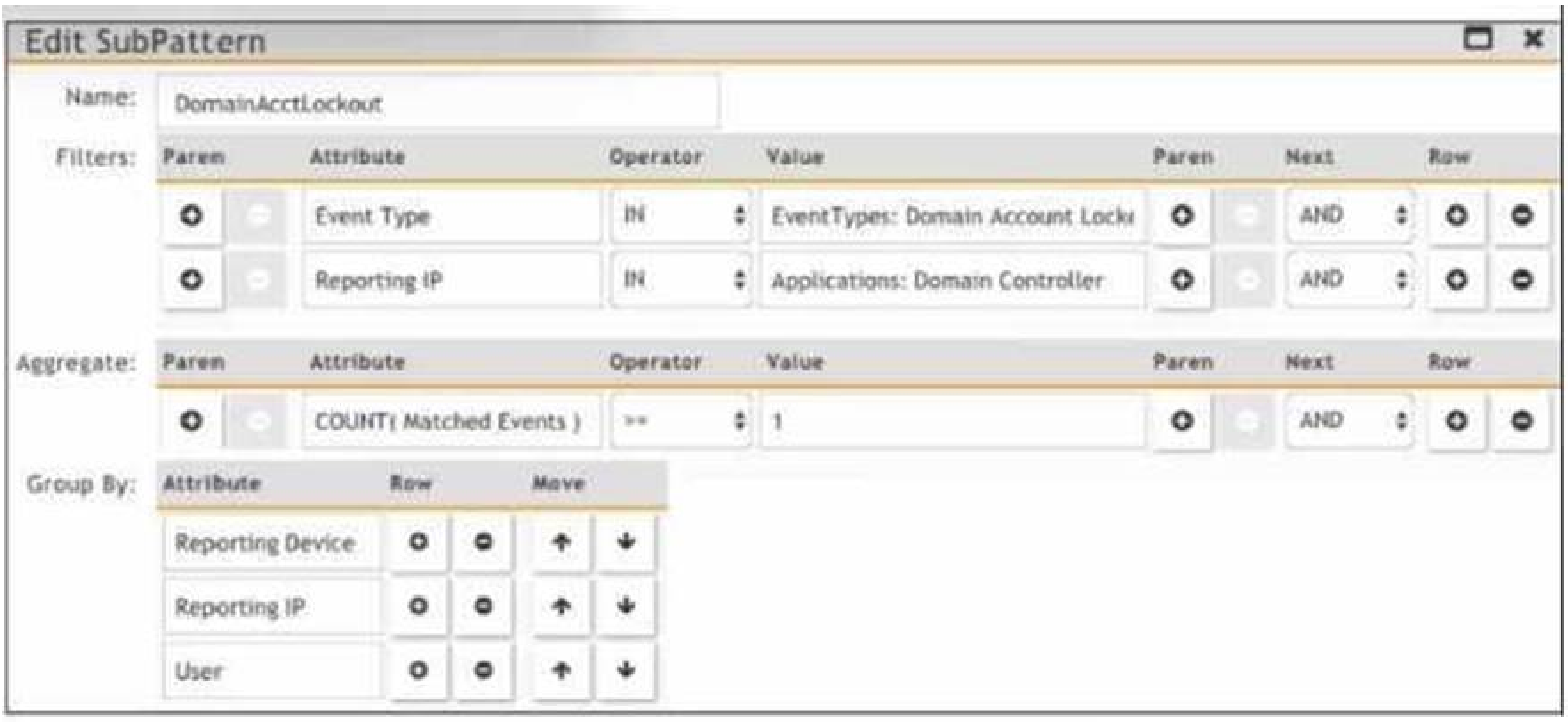
A. phgetHWID
B. ./phLicenseTool - support
C. phgetUUID
D. ./phLicenseTool-show

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 5
Refer to the exhibit.



Edit SubPattern

Name: DomainAcctLockout

Filters:

Paren	Attribute	Operator	Value	Paren	Next	Row
	Event Type	IN	EventTypes: Domain Account Lock		AND	
	Reporting IP	IN	Applications: Domain Controller		AND	

Aggregate:

Paren	Attribute	Operator	Value	Paren	Next	Row
	COUNT(Matched Events)	>=	1		AND	

Group By:

Attribute	Row	Move
Reporting Device		
Reporting IP		
User		

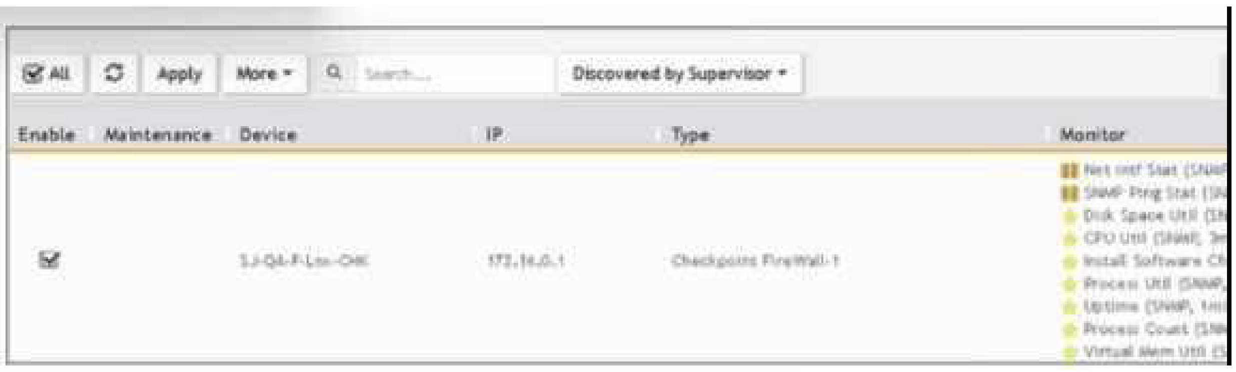
Which section contains the sortings that determine how many incidents are created?

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 6
Refer to the exhibit.



Enable	Maintenance	Device	IP	Type	Monitor
☑		SJ-QA-F-Lnx-CHK	172.16.0.1	Checkpoint FireWall-1	Net Intf Stat (SNMP SNMP Ping Stat (SN Disk Space Util (SN CPU Util (SNMP, 3m Install Software Ch Process Util (SNMP, Uptime (SNMP, 1m Process Count (SNM Virtual Mem Util (S

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

Explanation:
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 7
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

Explanation:
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 8
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

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.
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 9
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. CMDB Report Conditions
B. Data Conditions
C. UI Access

Answer: B

NEW QUESTION 10
Which protocol is almost always required for the FortiSIEM GUI discovery process?

A. SNMP
B. WMI
C. Syslog
D. Telnet

Answer: A

NEW QUESTION 10
To determine SNMP discovery issues, which is the best command from the backend?

A. snmpwalk
B. phSNMPTest
C. snmptest
D. ssh

Answer: A

NEW QUESTION 14
Which two export methods are available for FortiSIEM analytics results? (Choose two.)

A. CSV
B. PNG
C. HTML
D. PDF

Answer: AD

NEW QUESTION 17
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 22
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 25
Which item is required to register a FortiSIEM appliance license?

A. Static storage
B. Static MAC address
C. Static IP address
D. Static Hardware ID

Answer: D

NEW QUESTION 29
To determine whether or not syslog is being received from a network device, which is the best command from the backend?

A. tcpdump
B. phDeviceTest
C. netcat
D. phSyslogRecorder

Answer: A

NEW QUESTION 30
Device discovery information is stored in which database?

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

Answer: A

NEW QUESTION 31
......