IT认证电子书

质量更高　服务更好

半年免费升级服务

http://www.itrenzheng.com

Exam : NSE5_FSM-6.3

Title : Fortinet NSE 5 - FortiSIEM 6.3

Version : DEMO

1.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 settings addresses

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.

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

2.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.

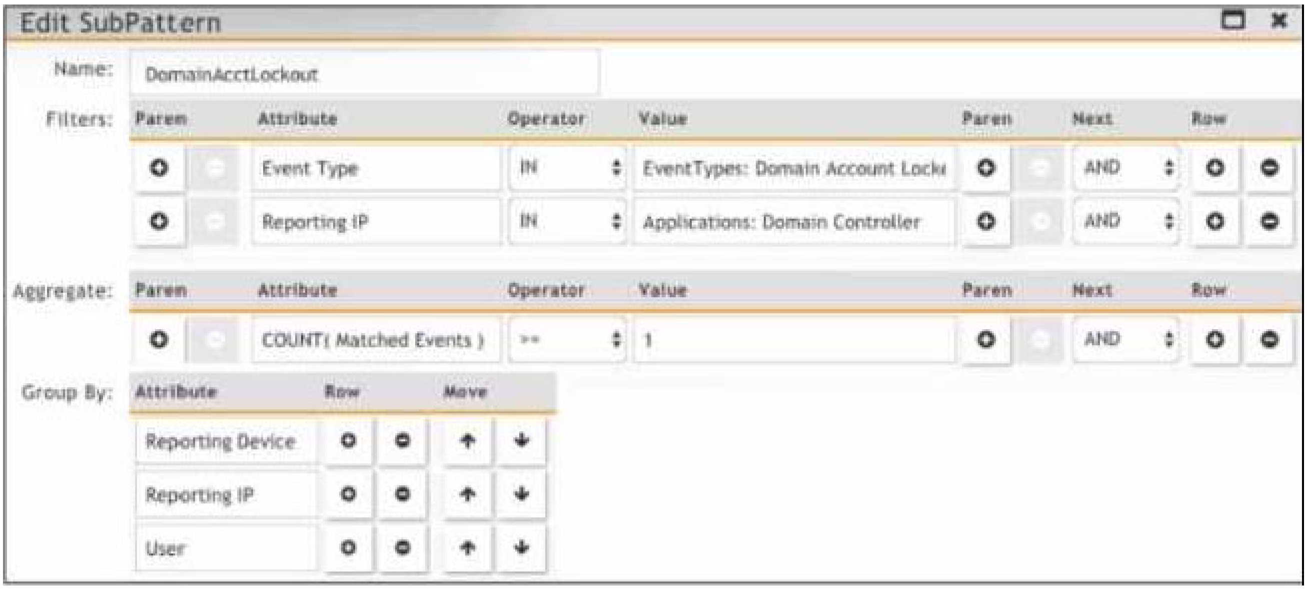
phgetUUID: This command retrieves the universally unique identifier (UUID) for the FortiSIEM system.

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.

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

3.Refer to the exhibit.



Name: DomainAcctLockout

Filters:

Paren	Attribute	Operator	Value	Paren	Next	Row
	Event Type	IN	EventTypes: Domain Account Locke		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: C

Explanation:

Incident Creation in FortiSIEM: Incidents in FortiSIEM are created based on specific patterns and conditions defined within the system.

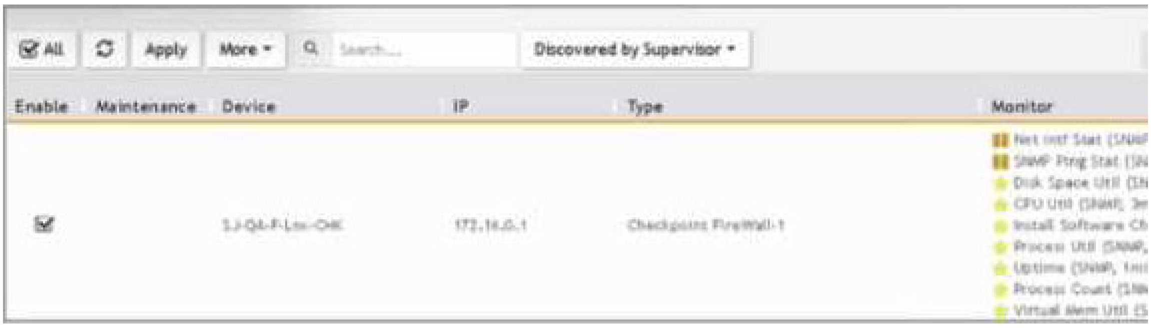
Group By Function: The "Group By" section in the "Edit SubPattern" window specifies how the data should be grouped for analysis and incident creation.

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.

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

4.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, 1mi ☆ 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.

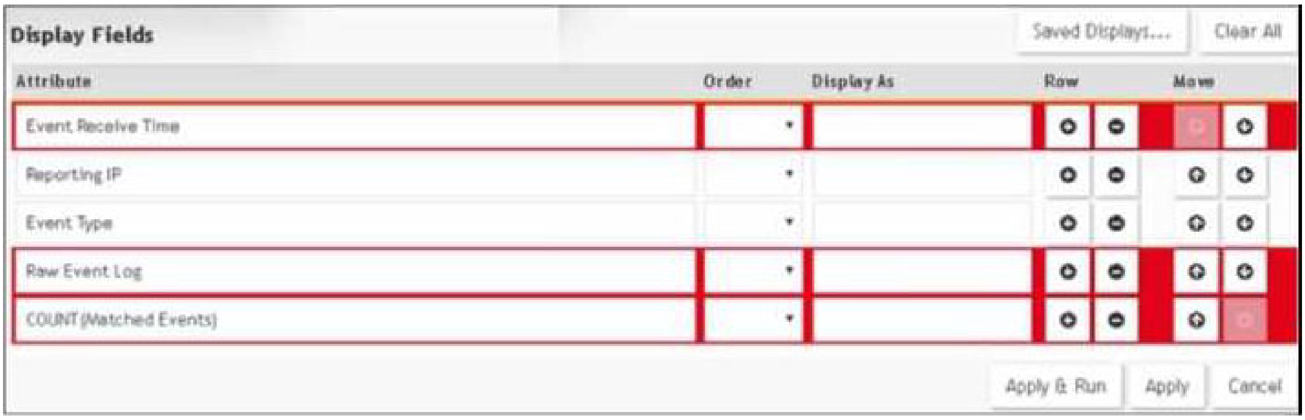
Pause Icon: The pause icon specifically indicates that data collection is paused, but this can happen due to several reasons.

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.

Reference: FortiSIEM 6.3 User Guide, Device Management and Data Collection Status Icons section, which explains the different icons and their meanings.

5.Refer to the exhibit.



Display Fields

Attribute	Order	Display As	Row	Move
Event Receive Time	▾		⊕ ⊖	⊙
Reporting IP	▾		⊕ ⊖	⊙ ⊙
Event Type	▾		⊕ ⊖	⊙ ⊙
Raw Event Log	▾		⊕ ⊖	⊙ ⊙
COUNT(Matched Events)	▾		⊕ ⊖	⊙

A FortiSIEM administrator wants to group some attributes for a report, but is not able to do so successfully.

As shown in the exhibit, why are some of the fields highlighted in red?

A. Unique attributes cannot be grouped.

B. The Event Receive Time attribute is not available for logs.

C. The attribute COUNT(Matched events) is an invalid expression.

D. No RAW Event Log attribute is available for devices.

Answer: A

Explanation:

Grouping Attributes in Reports: When creating reports in FortiSIEM, certain attributes can be grouped to summarize and organize the data.

Unique Attributes: Attributes that are unique for each event cannot be grouped because they do not provide a meaningful aggregation or summary.

Red Highlighting Explanation

The red highlighting in the exhibit indicates attributes that cannot be grouped together due to their unique nature. These unique attributes include Event Receive Time, Reporting IP, Event Type, Raw Event Log, and COUNT (Matched Events).

Attribute Characteristics:

Event Receive Time is unique for each event.
Reporting IP and Event Type can vary greatly, making grouping them impractical in this context.
Raw Event Log represents the unprocessed log data, which is also unique.
COUNT (Matched Events) is a calculated field, not suitable for grouping.
Reference: FortiSIEM 6.3 User Guide, Reporting section, explains the constraints on grouping attributes in reports.