

HP

Exam HP0-A116

HP ArcSight ESM 6.5 Security Administrator and Analyst

Version: Demo

[Total Questions: 10]

Question No : 1

What is the impact of checking Auto Update on the Search Results header, and selecting a time of 2 minutes?

- A.** The time span for this search to complete is limited to 2 minutes, and the current results are displayed.
- B.** The current field set is refreshed, and any results that changed in the grid are flagged with a highlight.
- C.** The current search query is rerun every 2 minutes following selection of the Auto Update check box
- D.** ArcSight Command Center checks for any new software updates occurring in the previous 2 minutes.

Answer: B

Question No : 2

During Connector install, which statement is true about the ArcSight Manager's host name or IP address?

- A.** It must match the host name or IP address in the ArcSight Manager's SSL certificate.
- B.** The host name or IP address is used as an encryption key.
- C.** It can be any legitimate host name or IP address.
- D.** It must contain a combination of alpha-numeric characters.

Answer: A

Question No : 3

What are functions of Query-Viewers? (Select two.)

- A.** displaying the Boolean logic and conditions linkage behind filters and rules criteria
- B.** providing a baseline analysis of events against which future queries can be compared
- C.** determining which devices are off-line at any given point in time by querying their status
- D.** providing a quick way to run SQL queries and identify trends without running reports
- E.** presenting detailed comparisons of report elements, not possible with reporting tools

Answer: B,D

Question No : 4

What is the default port used when connecting to the ArcSight Web interface?

- A. TCP 9443
- B. UDP 9443
- C. TCP 8443
- D. UDP 8443

Answer: A

Question No : 5

How do asset categorization and event categorization relate to each other?

- A. Asset categorization and event categorization are the same.
- B. Asset categorization and event categorization use the same field set to apply categories to assets and events.
- C. Asset categorization requires custom FlexConnectors; event categorization uses standard SmartConnectors.
- D. Asset categorization is the fingerprint of an asset; event categorization is a set of criteria that describes an event.

Answer: D

Question No : 6

Which statement is true about join rules and chained rules?

- A. Join rules link simple rules together; chained rules link join rules.
- B. Join rules use Session Lists; chained rules use Active Lists.
- C. Chained rules may or may not be join rules that also use Active Lists or rely on Correlation events generated by other rules.
- D. Chained rules result in detailed chains; join rules result in simple chains.

Answer: C

Question No : 7

What is the primary function of the ArcSight Manager?

- A.** It accepts correlated, prioritized events from SmartConnectors with instructions from the ArcSight Console, and writes events to the database.
- B.** It manages bottlenecks between the connectors, the ArcSight Console, and the ESM Database.
- C.** It writes incoming events to the database while simultaneously processing events through the Correlation engine.
- D.** It restores the rule definitions that drive the functioning of ArcSight ESM.

Answer: C

Question No : 8

Which statement is true about Connectors that are in a Paused state?

- A.** Paused Connectors are responding to the Manager but not sending or caching events.
- B.** Paused Connectors are responding to the Manager but events are being cached.
- C.** Paused Connectors are responding to the Manager and sending events.
- D.** Paused Connectors are not responding to the Manager.

Answer: B

Question No : 9

What is the "focus" of a Focus report?

- A.** the differences between two similar reports
- B.** a subset of a larger (e.g., monthly or quarterly) report
- C.** events that have been missed
- D.** high priority Correlation events only

Answer: B

Question No : 10

Which statement is true about starting and stopping ArcSight SmartConnector services?

- A.** They are started and stopped independently of the other ArcSight component services.
- B.** The order in which they are started and stopped is based on event flow.
- C.** How they are started and stopped depends on whether or not the ArcSight Manager is running.
- D.** They are started and stopped in conjunction with the Oracle database services.

Answer: A

Thank You For Trying HP0-A116 PDF Demo

To try our HP0-A116 Premium Files visit link below:

<https://examsland.com/latest-exam-questions/HP0-A116/>

Start Your HP0-A116 Preparation

Use Coupon **EL25 for extra 25% discount on the purchase of Practice Test Software.**