HP0-A116 Q&As

HP ArcSight ESM 6.5 Security Administrator and Analyst

Pass HP HP0-A116 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/hp0-a116.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

QUESTION 1

Which statements are true about Session Lists? (Select two)

A. They always have Start Time, End Time, and Creation Time fields.

B. They must have a key field and a time value.

C. They can share entries with other Session Lists.

D. They can be used as a basis for Trend Queries.

E. They can be used to populate Active Lists.

Correct Answer: CE

QUESTION 2

What can you use to change the stage of a Case?

A. Event annotations

B. Case Editor

C. Query Viewer

D. Common Conditions Editor

Correct Answer: B

QUESTION 3

Which processes occur in the first phase of the event lifecycle? (Select two.)

A. evaluating event data

B. applying event categories

C. applying hashing to event data

D. correlating event data

E. normalizing event data

Correct Answer: BE

QUESTION 4

Preserve Raw Events, Turbo Mode, and Limit Event Processing Rate are all examples of which type of Connector

options?

A. Processing options

B. Aggregation options

C. Filter conditions

D. Preservation options

Correct Answer: A

QUESTION 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.

Correct Answer: D

QUESTION 6

Which command is used to modify retention periods?

A. Arcsight archive install

B. Arcsight database create

C. Arcsight retention create

D. Arcsight database pc

Correct Answer: D

QUESTION 7

What is the "focus" of a Focus report?

A. events that have been missed based on additional criteria

B. the differences between two similar report outputs

C. a subset of a larger (for example, monthly or quarterly) report

D. high priority Correlation events only

Correct Answer: C

QUESTION 8

What Is the ArcSight Event Schema?

A. a format into which event data is normalized prior to persistence into storage

B. a collection of SmartConnectors that provide data to the ArcSight Manager

C. a set of events with a common format, collected over a user-defined time period

D. a map correlating IP addresses with devices to designate the source of events

Correct Answer: C

QUESTION 9

Why would you lock a Case?

A. to close and archive a Case

B. to prevent others from modifying the Case while you edit or attach something to the Case

C. to prevent the Case from being seen in the Resource List

D. to preserve the state of the Case

Correct Answer: B

QUESTION 10

Where are the resource settings located that determine ArcSight ESM User Password Policy?

A. in the User E2 80 99s Access Control List

B. in the server.defaults.properties file

C. in the server.properties file

D. in either ArcSight Console or Command Center

Correct Answer: B

QUESTION 11

What is a function of the Variable GetSessionData?

A. retrieves data fields from a Session List

B. sends session details to the ArcSight Manager

C. populates a Session List

D. investigates session details in the audit log

Correct Answer: A

QUESTION 12

Which output formats are available when running a report? (Select two.)

A. XML

B. HTML

C. PDF

D. JPEG

Correct Answer: BC

QUESTION 13

Which statements are true about SmartConnectors and batching? (Select two.)

A. Batches can be sent when they reach a certain size.

B. Batches can be sent on command.

C. Batches can be sent in priority order by severity.

D. Batches can be sent by Connector type.

Correct Answer: AC

QUESTION 14

What happens when a Connector upgrade that was initiated from within the ArcSight Console fails?

A. The Connector automatically rolls back to the previously working version.

B. The Connector does not respond to the failed upgrade.

C. The Connector reports to the Manager that the upgrade failed and then died.

D. The Connector automatically attempts the upgrade again.

Correct Answer: A

QUESTION 15

Which statements are true about escalation levels? (Select two.)

A. Custom escalation levels can be added at anytime.

B. They must be defined separately for each notification type.

C. New escalation levels are added to the beginning of an escalation level sequence.

D. They are contained in notification group configurations.

E. They must be created in the order in which you want escalation to proceed.

Correct Answer: BE