

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.leads4pass.com/hp0-a116.html>

100% Passing Guarantee
100% Money Back Assurance

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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



QUESTION 1

In network modeling, what are SmartConnectors bound to? (Select two.)

- A. zones
- B. assets
- C. devices
- D. customers
- E. networks

Correct Answer: DE

QUESTION 2

Which statements are true about event lifecycle data collection and the event processing phase? (Select two.)

- A. Model confidence is determined, based on details provided by the event source.
- B. Each line of incoming log data is processed as a separate event.
- C. Event severity is determined, based on an Active List of recent severity factors.
- D. Values are normalized and entered into the ArcSight Event Schema.

Correct Answer: BD

QUESTION 3

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 4

What is an example of an event-based Data Monitor?

- A. rules partial match

- B. last n events
- C. session reconciliation
- D. moving average

Correct Answer: B

QUESTION 5

Which components does a Network Model include? (Select two.)

- A. assets
- B. data monitors
- C. dashboards
- D. zones

Correct Answer: AD

QUESTION 6

One of the benefits of SSL technology is authentication. What does authentication do?

- A. validates client logins using advanced identity detection technology
- B. encrypts information sent between clients and servers
- C. adds a hashing algorithm to prevent data modification between client and server
- D. ensures that clients send information to the actual intended server, not a machine pretending to be that server

Correct Answer: D

QUESTION 7

What must be done first to restore the database from an online backup?

- A. run the Oracle restore wizard
- B. ensure that the archived redo logs are located in the archive log destination
- C. bring the affected tablespaces online
- D. reinstall the Oracle installation

Correct Answer: B

QUESTION 8

What is an example of an event-based Data Monitor?

- A. moving average
- B. rules partial match
- C. last n events
- D. session reconciliation

Correct Answer: C

QUESTION 9

You want your Active Channel to automatically display new events as they arrive at ESM. Which time parameter should you use to accomplish this?

- A. Evaluate Once at Attach Time
- B. Evaluate \$NOW-1h
- C. Continuously Evaluate
- D. Evaluate Continuously from Attach Time

Correct Answer: C

QUESTION 10

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 11

Which functions are on the right-click menu for an event in the ConsoleViewer panel? (Select two.)

- A. Correlate Events
- B. Show Event Details

C. Show Event Chart

D. Annotate Events

E. Prioritize Events

Correct Answer: CE

QUESTION 12

Which resources can be displayed in the ArcSight Web interface? (Select two.)

A. Reports and Dashboards

B. Queries and Partitions

C. Cases, Notifications, and Active Channels

D. Knowledge Base articles and Templates

Correct Answer: AC

QUESTION 13

There are three types of ArcSight SmartConnectors. Which type is used primarily to execute commands on a device to retrieve, modify, or analyze its configuration?

A. Event Connectors

B. Scanner Connectors

C. CounterACT Connectors

D. SNMP Connectors

Correct Answer: C

QUESTION 14

Which three attributes are used to describe an Asset Model?

A. vulnerabilities, locations, and asset categories

B. locations, asset categories, and threats

C. asset types, asset categories, and locations

D. vulnerabilities, addresses, and threats

Correct Answer: A

QUESTION 15

Which statements are true about reports? (Select two.)

- A. Reports can be based on Cases, Trends, Session Lists, and Events.
- B. Archived reports must be restored before they can be used again
- C. Reports can be scheduled to run yearly, monthly, weekly, daily, or hourly.
- D. Reports cannot be based on Session Lists.
- E. Only scheduled reports can be archived.

Correct Answer: BD

[Latest HP0-A116 Dumps](#)

[HP0-A116 Study Guide](#)

[HP0-A116 Braindumps](#)