![Pass2Lead](https://www.pass2lead.com)
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.pass2lead.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

Which functions does a non-event based Data Monitor perform?

A. evaluates the event stream and creates Correlation events when anomalies are discovered

B. monitors and displays rule and filter data flow thresholds and latencies

C. summarizes and displays event-based Data Monitor statistics

D. monitors and displays ArcSight ESM system and platform status

Correct Answer: D

QUESTION 2

Which ArcStght Console user settings can be changed in the Preferences Editor?

A. default time period of Active Channels

B. maximum number of viewable assets

C. date and time format

D. number of rows displayed in an Active Channel

Correct Answer: D

QUESTION 3

In Network Modeling, what are SmartConnectors bound to? (Select two.)

A. zones

B. networks

C. devices

D. customers

Correct Answer: BD

QUESTION 4

Which three attributes are used to describe an Asset Model?

A. vulnerabilities, locations, and asset categories

B. locations, asset categories, and threats

![Pass2Lead](https://Pass2Lead.com)
C. asset types, asset categories, and locations

D. vulnerabilities, addresses, and threats

Correct Answer: A

QUESTION 5

What is the name of the resource you can use to override the default ArcSight mapping IP addresses to geographic regions?

A. zones

B. destinations

C. locations

D. categories

Correct Answer: C

QUESTION 6

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 7

Which host user should own the .tararchive from which the ArcSight ESM Suite bin file containing ESM components, and installation and configuration wizards is extracted?

A. any user with admin group privilege

B. root user

C. arcsight user

D. archive user

Correct Answer: B

QUESTION 8

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

A. Continuously Evaluate

B. Evaluate Continuously from Attach Time

C. Evaluate $NOW-1h

D. Evaluate Once at Attach Time

Correct Answer: C

QUESTION 9

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.

Correct Answer: B

QUESTION 10

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 11

Which ArcSight resource objects do Field Sets correspond to?

A. attributes in a Query Viewer

B. variables in a Rule configuration

C. components in a Network Model

D. columns in an Active Channel Grid view

Correct Answer: D

QUESTION 12

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.

Correct Answer: C

QUESTION 13

Which statement is true about SmartConnectors and FlexConnectors?

A. FlexConnectors allow creation of SmartConnectors that are tailored to individualized custom situations and specific security event data.

B. FlexConnectors are plug-and-play, self-programming SmartConnectors.

C. SmartConnectors do not include tools for customizing FlexConnectors.

D. SmartConnectors are vendor-specific and must be purchased through the individual device vendors.

Correct Answer: A

QUESTION 14

The Packages view in the ArcSight Console Navigator provides access to all discrete resources that are part of a package in a single view. The dependency view toggle in the Package tree header shows required packages, which are packages on which other packages depend. What is the visual indicator of this dependency?

A. The package name is underlined.

B. The package name is shown in hold font.

C. The package icon contains a red asterisk.

D. The package icon is highlighted in yellow.

Correct Answer: A

QUESTION 15

Which statement best describes how baselines are established and used in Query Viewers?

A. Baselines are created using query results, which are fed into the Image Editor for filtering and display in the related Data Monitor.

B. Baselines are created using rules. After the rule is triggered, the resulting action establishes a baseline against which future rules are evaluated in the Query Viewer.

C. Baselines are created using query results. When a query has one or more baselines available, you can compare the current results with a baseline.

D. Baselines are created using query results. The baseline from the query is used to create a new field set definition that can be run against future events.

Correct Answer: B

[HP0-A116 VCE Dumps](#) [HP0-A116 Practice Test](#) [HP0-A116 Braindumps](#)