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

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

A. zones

B. networks

C. devices

D. customers

Correct Answer: BD

QUESTION 2

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 3

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 4

Which file types MUST be included in an Oracle backup? (Select two.)

A. table files

B. data files

C. program files

D. configuration files

Correct Answer: BD

QUESTION 5

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 6

What are valid actions for a rule to take? (Select two.)

A. send notification

B. execute command

C. generate report

D. add to filter

Correct Answer: AB

QUESTION 7

What is a criteria factor within the ArcSight Priority Formula?

A. Assurance

B. Asset Priority

C. Seriousness

D. Model Confidence

Correct Answer: D

QUESTION 8

What stores information about logons, user actions, and the resulting events in the most concise way?

A. Event annotations

B. Session Lists

C. Active Lists

D. Cases

Correct Answer: B

QUESTION 9

Which resource defines what a report will look like when generated?

A. layout

B. query

C. template

D. form

Correct Answer: C

QUESTION 10

Which tablespace is used by ArcSight to store resources?

A. ARC_EVENT_DATA

B. ARC_SYSTEM_INDEX

C. ARC_SYSTEM_DATA

D. ARC_EVENT_INDEX

Correct Answer: C

QUESTION 11

What does Partition Archiving allow you to specify?

A. the number of partitions to keep offline

B. the number of partitions that remain online

C. the compression ratio to be used in partitioning

D. the amount of data to store in a partition

Correct Answer: A

QUESTION 12

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 13

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

A. assets

B. data monitors

C. dashboards

D. zones

Correct Answer: AD

QUESTION 14

What is a good way for an operator or analyst to quickly determine which events must be addressed first?

A. check the priority rating in a Dashboard or Active Channel

B. run a report of High Priority Threats

C. ask more senior analysts or architects

D. view the Event Grid and Correlation categories

Correct Answer: A

QUESTION 15

What do you use to establish identity, ownership, and criticality of the assets you have installed on your network?

A. asset types

B. asset groups

C. asset categories

D. asset ranges

Correct Answer: C

Latest HP0-A116 Dumps   HP0-A116 VCE Dumps   HP0-A116 Practice Test