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.passapply.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 procedure allows you to terminate a session within a Session List? (Select two)

A. Exceed the time-out based on entry expiration time

B. Configure a rule action to explicitly terminate a session

C. Manually close the session using the right-click menu.

D. Adjust the Session setting in Console Preferences.

E. Close the session by exiting the ArcSight Console.

Correct Answer: AE

QUESTION 2

During your ESM installation and configuration, none of the Foundation Packages were selected in the Configuration Wizard. What should you do to install the Foundation Packages?

A. Manually upload the Foundation Packages to ESM using .arb files exported from another ESM instance

B. Reapply the ESM product license from Arc Sight Command Center to install the the Foundation Packages

C. Rerun the Configuration Wizard using Manager setup and select the Foundation Packages to install

D. Install the Foundation Packages from the ArcSight Console Resource Navigator right- click menus

Correct Answer: D

Reference:

https://h10120.www1.hp.com/expertone/datacard/Exam/HP0-A116

QUESTION 3

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

QUESTION 4

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 5

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

HP0-A116 PDF Dumps   HP0-A116 Practice Test   HP0-A116 Exam Questions