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

QUESTION 1

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 2

What is the procedure to reset all ArcSight Console preferences back to default?

A. In "console.properties" file, locate and edit the line: set default=true.

B. Copy the "console.defaults.properties" file to overwrite the "console.properties" file.

C. Stop the Console, delete or rename the user.ast file, and restart the Console.

D. In the File menu, click on Preferences, and select "Set to Default".

Correct Answer: B

QUESTION 3

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 4

When specifying the attributes of a new Active List, you can set TTL days, hours, and minutes. What is TTL?

A. Total Time Lag

B. Time Threshold Lag

C. Time To Live

D. Total Time Left

Correct Answer: C

QUESTION 5

Which statement is true about how filters are applied by the Connector or by the Manager?

A. When filters are applied by either the Connector or the Manager, events that match the filter conditions are selected and forwarded for further processing.

B. When filters are applied by either the Connector or the Manager, events that match the filter conditions are excluded and are not forwarded for further processing.

C. Events that match the Connector filter are excluded and not forwarded further; events that match the Manager filter are selected for further analysis.

D. Events that match the Connector filter are included and forwarded to the Manager; events that match the Manager filter are excluded.

Correct Answer: C

QUESTION 6

Which statement is true about the ArcSight Web interface?

A. Inline filters cannot be used from the ArcSight Web interface.

B. Data Monitors cannot be added to a Dashboard from the ArcSightWebinterface.

C. Reports cannot be formatted from the ArcSight Web interface.

D. Cases cannot be modified from the ArcSight Web interface.

Correct Answer: B

QUESTION 7

How can you restore a new ArcSight Web installation to a previous configuration?

A. copy the old ArcSight Web installation\\'s config directory and cacerts file into the new installation

B. copy the ArcSight Manager\\'s config directory into the new installation

C. manually reconfigure the new installation

D. connect to the Manager and download the saved configuration

Correct Answer: A

QUESTION 8

What are potential ways of acknowledging notifications? (Select two.)

A. by replying to notification email

B. by calling in to the notification response hotline

C. by sending email to SysAdmin

D. by using the Notifications Manager in the ArcSight Console

Correct Answer: AD

QUESTION 9

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 10

Which document provides the most detailed instructions for applying an Oracle CPU?

A. Oracle CPU release notes

B. ArcSight ESM Administrator\\'s Guide

C. Opatch Readme file

D. ArcSight ESM Installation Guide

Correct Answer: A

QUESTION 11

From where are the local ArcSight Console Preference Settings accessed?

A. File Menu

B. Edit Menu

C. Tools Menu

D. View Menu

Correct Answer: C

QUESTION 12

What is the Reserve Period?

A. the amount of time to allow before compressing event data for storage

B. the number of future partitions to be maintained

C. the amount of time to wait before determining that a device is not operating

D. the maximum length of time archived partitions will be stored

Correct Answer: B

QUESTION 13

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

A. XML

B. HTML

C. PDF

D. JPEG

Correct Answer: BC

QUESTION 14

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 15

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

A. Common Conditions Editor

B. Case Editor

C. Notifications Editor

D. Event Annotations

Correct Answer: B