HP ArcSight ESM 6.5 Security Administrator and Analyst

1. What does the Priority Formula calculation run on?

A. the Manager only

B. SmartConnectors only

C. FlexConnectors

D. both SmartConnectors and the Manager

Answer(s): A

---

2. What happens when a Connector upgrade that was initiated from within the ArcSight Console fails?

A. The Connector automatically attempts the upgrade again.

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 rolls back to the previously working version.

Answer(s): D

---

3. Which component determines how a report looks when it is generated?

A. Template

B. Layout

C. Form

D. Query

Answer(s): D

---

4. Which statements are true about results in Query Viewers? (Select two.)

A. Results can be forwarded as notifications.

B. Results can be used to generate reports.

C. Results can be used in event searches.

D. Results can be displayed as tables or charts, and added to Dashboards

E. Results can be used as event filters.

Answer(s): B,D

---

5. Which method is used to back up an Oracle database without shutting down the database?

A. offline backup

B. sequential backup

C. standalone backup

D. online backup

Answer(s): D

---

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

A. Prioritize Events

B. Annotate Events

C. Correlate Events

D. Show Event Details

Answer(s): B,D

---

7. How are ESM Global Variables created?

A. from the Fields and Global Variable tab in the Field SetResource or by promoting a Local Variable

B. from the Local Variables tab of the Filter Resource and only by promoting a Local Variable

C. from within the Manager's server.properties file by using the System Global Variable link

D. from the System Tools menu by using the Create System Global Variable option

Answer(s): B

---

8. How do asset categorization and event categorization relate to each other?

A. Asset categorization requires custom FlexConnectors; event categorization uses standard SmartConnectors.

B. Asset categorization and event categorization are the same.

C. Asset categorization and event categorization use the same field set to apply categories to assets and events.

D. Asset categorization is the fingerprint of an asset; event categorization is a set of criteria that describes an event.

Answer(s): D

---

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

A. PDF

B. HTML

C. XML

D. JPEG

Answer(s): A,B

---

10. Which statements are true about assets? (Select two.)

A. Assets can be grouped in folders called asset ranges.

B. Assets can include bridges, routers, web servers, or anything with an IP or MAC address.

C. Assets require a MAC address to be categorized properly.

D. An asset is any endpoint considered significant enough to characterize with details to help with correlation and reporting.

Answer(s): B,D

---

11. What is the default port used to connect the ArcSight Manager to the ArcSight ESM Database (Oracle)?

A. 443

B. 1443

C. 8443

D. 1521

Answer(s): D

---

12. What are functions of Query-Viewers? (Select two.)

A. presenting detailed comparisons of report elements, not possible with reporting tools

B. providing a quick way to run SQL queries and identify trends without running reports

C. displaying the Boolean logic and conditions linkage behind filters ana rules criteria

D. providing a baseline analysis of events against which future queries can be compared

E. determining which devices are off-line at any given point in time by querying their status

Answer(s): B,D

---

13. ArcSight SmartConnectors send event data directly to what?

A. ArcSight Console

B. ArcSight Web Server

C. ArcSight Database

D. ArcSight Manager

Answer(s): D

---

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

A. Case Editor

B. Event Annotations

C. Notifications Editor

D. Common Conditions Editor

Answer(s): A

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

A. send notification

B. add to filter

C. execute command

D. generate report

Answer(s): A,C

---

16. Which statement is true about the ArcSight Web interface?

A. Reports cannot be formatted in the ArcSight Web interface.

B. Inline filters cannot be used in the ArcSight Web interface.

C. Cases cannot be modified in the ArcSight Web interface.

D. Data Monitors cannot be added to a Dashboard in the ArcSight Web interface.

Answer(s): D

---

17. 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. CounterACT Connectors

B. Event Connectors

C. Scanner Connectors

D. SNMP Connectors

Answer(s): A

18. Which visualization display functions are possible with Dashboards? (Select two.)

A. slide show

B. annotate

C. zoom in/out

D. crop

E. fade in/out

Answer(s): A,C

---

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

A. Notifications and Active Channels

B. Search Filters and Saved Searches

C. Knowledge Base articles and Templates

D. Reports and Dashboards

E. Queries and Cases

Answer(s): C,D

---

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

A. Evaluate Once at Attach Time

B. Evaluate $NOW-1h

C. Continuously Evaluate

D. Evaluate Continuously from Attach Time

Answer(s): B
