# Pass4sure.HP0-A116_60.questions

Number: HP0-A116
Passing Score: 800
Time Limit: 120 min
File Version: 19.05

## HP HP0-A116

## HP ArcSight ESM 6.5 Security Administrator and

- This VCE covers all syllabus. After preparing it anyone pass the exam in high grades.
- Questions and Answers material is updated in highly outclass manner on regular basis
- This is a new VCE file with new questions.All the questions are super valid.
- Pretty much all the questions we study that may have multiple answers, no answer is in doubt, I got on the test.

**Exam A**

**QUESTION 1**
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
**Section: (none)**
**Explanation**

**Explanation/Reference:**
answer is verified.

**QUESTION 2**
If a username and password are used for authenticating a remote peer, when would you need to use those credentials a second time?

A. if credential caching expires and the auto-refresh option is not enabled
B. only if the peer relationship is broken and you need to authenticate the peer again
C. only for a content management subscriber manual synchronization
D. every time a distributed search is run and results are exported to the remote peer

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 3**
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
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 4**
Which visualization display functions are possible with Dashboards? (Select two.)

A. fade in/out
B. slide show
C. annotate
D. zoom in/out
E. crop

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 5**
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
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 6**
Which TCP/IP port is the default when a web browser is used to connect to the ArcSight Command Center?

A. 443
B. 6443
C. 9443
D. 8443

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 7**
Why is it sometimes necessary to lock a Case?

A. to prevent the Case from being seen in the Resource Tree
B. to prevent others from modifying the Case while you edit or attach something to the Case
C. to close and archive a Case
D. to preserve the state of the Case

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 8**
Which ArcSight Solution works as a GPS for privileged user activity that identifies unusual hehavior?

A. ThreatDetector
B. Pattern Discovery
C. IdentityView
D. ldentityCorrelation

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 9**
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
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 10**
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
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 11**
What are the three major display components of an Active Channel in the Viewer Panel?

A. Channels, Dashboards, and Reports
B. Summary, Event Graph, and Grid
C. Header, Radar, and Grid

D. Events. Data Monitors, and Radar

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 12**
Where are the resource settings located that determine ArcSight ESM User Password Policy?

A. in the User E2 80 99s Access Control List
B. in the server.defaults.properties file
C. in the server.properties file
D. in either ArcSight Console or Command Center

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
answer is verified.

**QUESTION 13**
In ESM, what allows contextual information to be added to an individual event or group of events in support of workflow or operational metrics?

A. Knowledge Base
B. Templates
C. Annotations
D. Rules

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 14**
Which resources are optional ArcSight compliance solutions delivered as packages? (Select two.)

A. SOX - Sarbanes Oxley Act
B. PCI - Penetration Culprit Identification
C. PCI - Payment Card industry
D. SOX- Secure Obfuscation Extensions
E. SOX - Security Operations Exposition
F. PCI - Payload Content Information

**Correct Answer:** BE
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 15**
How are ESM Global Variables created?

A. from within the Manager's server.properties file by using the System Global Variable link
B. from the Fields and Global Variable tab in the Field SetResource or by promoting a Local Variable
C. from the System Tools menu by using the Create System Global Variable option
D. from the Local Variables tab of the Filter Resource and only by promoting a Local Variable

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 16**
Which authenticators are configurable by ArcSight Command Center?

A. RADIUS Authentication, Microsoft Active Directory, LDAP, Custom JAASPlugin, or Password- Based/SSL Client Authentication
B. RADIUS Authentication, Microsoft Active Directory, Simple LDAP, or Built-in Authentication
C. RADIUS Authentication, Microsoft Active Directory, Simple LDAP, or SSL Client Authentication
D. RADIUS Authentication, Microsoft Active Directory, Custom JAAS Plugin, or Password- Based/SSL Client Authentication

**Correct Answer:** B

**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 17**
Which statementis considered best practice for ESM Content Management?

A. Designateonly one Manager as publisher.
B. Schedule package pushes during normal work hours.
C. Schedule frequent automatic package pushes
D. Do not retry on a failed automatic package push.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 18**
Which statement about drill down Query Viewers is true?

A. Drilldowns require an Active List for data comparison.
B. Drilldowns can be created only from Query Viewer results in chart format.
C. Drilldowns are selected by the right-click Investigate menu on Viewer Panel results displays.
D. A drilldown is always based on another Query Viewer.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 19**
What Is the ArcSight Event Schema?

A. a format into which event data is normalized prior to persistence into storage

B. a collection of SmartConnectors that provide data to the ArcSight Manager
C. a set of events with a common format, collected over a user-defined time period
D. a map correlating IP addresses with devices to designate the source of events

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 20**
Which ArcSight ESM user type provides full privileges to use the Command Center, the ArcSight Console, the Arcsight Web client, and all tools?

A. Web User
B. Normal User
C. Connector Installer
D. Management Tool

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 21**
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
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 22**
What is the effect of the constraints used in an event search query?

A. They maintain search criteria within the range of data specified by the filter
B. They provide a shorthand view when defining field sets.
C. They limit the range or focus of data sources to be searched.
D. They establish the time range for the search query

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 23**
Besides managing user accounts, user groups, event storage, and notifications, what else does the ArcSight Command Center allow you to do?

A. Update the ESM product license, and access the ArcSight Web interface.
B. Status Connectors, configure authentication; monitor events and resources from Dashboards, and update the ESM product license.
C. Configure Connectors, notifications, and authentication; monitor events and resources from Dashboards, and access the ArcSight Web interface.
D. Update the ESM product license, monitor resources, and investigate events from Dashboards

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 24**
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

**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 25**
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
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 26**
Which statements are true about Session Lists? (Select two)

A. They always have Start Time, End Time, and Creation Time fields.
B. They must have a key field and a time value.
C. They can share entries with other Session Lists.
D. They can be used as a basis for Trend Queries.
E. They can be used to populate Active Lists.

**Correct Answer:** CE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 27**
Active Channel views and Dashboard views are examples of ArcSight Console Viewer Panel views. Which other views are associated with the Viewer

Panel? (Select two)

A. Simple views
B. Asset views
C. Results views
D. Resource views
E. Combined views

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 28**
Which statements are true about Active Lists? (Select two.)

A. They can store data over longer periods of time than rules or Data Monitors.
B. They can incur processing overhead if not properly scheduled.
C. They always include start time and end time fields.
D. They can be manually populated using the right-click context menu.
E. They can neither be exported nor imported.

**Correct Answer:** AC
**Section: (none)**
**Explanation**

**Explanation/Reference:**
answer is modified.

**QUESTION 29**
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 is the fingerprint of an asset; event categorization is a set of criteria that describes an event.
D. Asset categorization and event categorization use the same field set to apply categories to assets and events

**Correct Answer:** D

**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 30**
What are valid actions for a rule to take? (Select two.)

A. generating a report
B. executing a command
C. sending a notification
D. Creating a vulnerability
E. adding a condition to a filter

**Correct Answer:** CE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 31**
Of the 17 event field groups defined in the ArcSight Event Schema, in which group can data fields describing an event's importance as assessed by ArcSight ESM be found?

A. Category
B. Attacker
C. Event
D. Threat

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 32**
What is the "focus" of a Focus report?

A. events that have been missed based on additional criteria
B. the differences between two similar report outputs
C. a subset of a larger (for example, monthly or quarterly) report
D. high priority Correlation events only

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 33**
Which statements are true about reports? (Select two.)

A. Reports can be based on Cases, Trends, Session Lists, and Events.
B. Archived reports must be restored before they can be used again
C. Reports can be scheduled to run yearly, monthly, weekly, daily, or hourly.
D. Reports cannot be based on Session Lists.
E. Only scheduled reports can be archived.

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 34**
When is it useful to schedule rules rather than have them run in real time?

A. when a network device is down
B. when events are occurring less frequently than usual
C. when you anticipate a worm or virus attack
D. when you need to minimize impact on system performance

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 35**
Using ESM 6.5 ArcSight Command Center, which drill down type is available?

A. query viewer drilldowns into other query viewers only
B. query viewer drilldowns into channels, reports, dashboards, or other query viewers
C. dashboard drilldowns into channels, reports, query viewers, or other dashboards
D. dashboard drilldowns into other dashboards only

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 36**
When exporting search results, what does the "Save to ArcSight Command Center" option do?

A. automatically exports the file to the Administration > Saved Searches > Saved Search Files path
B. opens a dialog allowing the user to specify a download location on the browser host system
C. opens the appropriate output format application to view and optionally save the results on the user's host
D. automatically exports the file to the ESM host <arcsight home>/logger/userdata/savedsearch directory

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 37**
Command Center Event Search consists of which search syntax methods?

A. SQL query, regular expression, and complex expression search
B. field-query search, simple query search, and complex expression search
C. full-field search, Boolean search, and regular expression search
D. field-based search, full-text search, and regular expression

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 38**
Under which circumstances does a Connector use its cache? (Select two.)

A. when a burst of events exceeds what the Manager can handle
B. when the Connector is performing a service restart
C. when the Connector is stopped or disabled
D. when the Connector cannot communicate with its destination
E. when the Connector cannot communicate with the event source

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 39**
Which statements are true about escalation levels? (Select two.)

A. Custom escalation levels can be added at anytime.
B. They must be defined separately for each notification type.
C. New escalation levels are added to the beginning of an escalation level sequence.
D. They are contained in notification group configurations.
E. They must be created in the order in which you want escalation to proceed.

**Correct Answer:** BE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 40**
What is an example of an event-based Data Monitor?

A. rules partial match
B. last n events
C. session reconciliation
D. moving average

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 41**
Report run start time, output format for report results, email distribution for report results, and report filters are all examples of what?

A. report parameters
B. report formats
C. report data sources
D. report attributes

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
answer is corrected.

**QUESTION 42**
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

**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 43**
Which pairs of resources can be displayed in the ArcSight Web interface? (Select two.)

A. Search Filters and Saved Searches
B. Queries and Cases
C. Reports and Dashboards
D. Notifications and Active Channels
E. Knowledge Base articles and Templates

**Correct Answer:** CE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 44**
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
**Section: (none)**
**Explanation**

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

**QUESTION 45**
What are functions of Query-Viewers? (Select two.)

A. displaying the Boolean logic and conditions linkage behind filters ana rules criteria
B. providing a baseline analysis of events against which future queries can be compared
C. determining which devices are off-line at any given point in time by querying their status
D. providing a quick way to run SQL queries and identify trends without running reports
E. presenting detailed comparisons of report elements, not possible with reporting tools

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 46**
By default, which TCP/IP port is used by ArcSight Command Center to communicate with a web browser client?

A. 1521
B. 9443
C. 8443
D. 443

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
http://eromang.zataz.com/2011/06/26/arcsight-logger-and-smartconnectors-questions-and- answers/

**QUESTION 47**
Which four basic Event Search elements affect what is displayed in the Search results?

A. filter, constraints, time range, and field set
B. filter, constraints, time range, and row limit
C. filter, time range, variables, and field set
D. filter, time range, time zone, and field set

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 48**
Which access type is provided with ESM Access Control Lists?

A. Specific User read and write access to specific Resource Groups
B. Specific User Group read and write access to a specific Resource
C. Specific User Group read and write access to specific Resource Groups
D. Specific User read and write access to a specific Resource

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 49**
Which statements are true about results in Query Viewers? (Select two.)

A. Results can be displayed as tables or charts, and added to Dashboards
B. Results can be used in event searches.
C. Results can be used to generate reports.
D. Results can be used as event filters.
E. Results can be forwarded as notifications.

**Correct Answer:** AC
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 50**
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
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 51**
Which processes occur in the first phase of the event lifecycle? (Select two.)

A. evaluating event data
B. applying event categories
C. applying hashing to event data
D. correlating event data
E. normalizing event data

**Correct Answer:** BE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 52**
What do the start and end times associated with a notification destination indicate?

A. the period of time that the system waits for a notification response
B. the period of time during which the notification can be received
C. the period of time during which the destination is expected to respond
D. the period of time during which the notification can be sent to the destination

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 53**
Which component determines how a report looks when it is generated?

A. Query
B. Layout
C. Form
D. Template

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 54**
What are the three general types of Data Monitors?

A. event-based, correlation, and non-event based
B. event-based, correlation, and aggregation matching
C. event-based, matching conditions and non-event based
D. event-based, event graph, and non-event based

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 55**
What is the impact of checking Auto Update on the Search Results header, and selecting a time of 2 minutes?

A. The time span for this search to complete is limited to 2 minutes, and the current results are displayed.
B. The current field set is refreshed, and any results that changed in the grid are flagged with a highlight.
C. The current search query is rerun every 2 minutes following selection of the Auto Update check box
D. ArcSight Command Center checks for any new software updates occurring in the previous 2 minutes.

**Correct Answer:** B
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 56**
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
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 57**
During which process is the first user created for access to ESM?

A. during initial configuration of server-side SSL trust store
B. during the authentication phase of the SmartConnector Installation
C. during installation of the ArcSight Console
D. during installation of the ArcSight Manager

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 58**
ESM components fail to consistently restart after a system reboot and require individual intervention with repeated arcsight_services component restart commands. Which log file offers troubleshooting information that will help resolve this issue?

A. monit.log

B. server.log
C. arcsight_services.log
D. server.status.log

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 59**
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
**Section: (none)**
**Explanation**

**Explanation/Reference:**
answer is updated.

**QUESTION 60**
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
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation: