1. What determines how the report output looks?

Answer: Report Template

2. When you will create first user in Arcsight?

Answer: While installing ESM

3. In command center dashboards can be drill down to what?

Answer: To Only Dashboard

4. Report time, output format, email recipient and user all these options are available in which tab?

Answer: Report Parameters

5. What all presentation options are available in dashboard?

Answer: Zoomin/Zoomout, Slideshow

6. Which user own the .tar file containing the ESM installer file

Answer: Arcsight user

7. Reports can be generated in which all format

Answer: HTML, csv, xls, pdf.

8. What action a rule can perform

Answer: execute a command, sent notification

9. What all option is available in right click menu of an active channel?

Answer: Show event details, annotations

10. What is Fieldset?

Answer: columns in a grid view of active channel

11. Which all authentication mechanism you can configure through Command Center

Answer: password based auth or password based or ssl client based auth

12. Which all activities you can perform through Command Center

Answer: license upgrade,

13. What all fields will be there in a session list?

Answer: Refer Hp0-M54.

14. How to end a session in a session list?

Answer: automatically expire, configure a rule.

15. What is base line in a query viewer?

Answer: Refer HP0-M54.

16. Other than Dashboard and Active channel what all things you can view in viewer panel

Answer: Resource View, result view.

17. When you will use a scheduled rule?

Answer: To minimize the resource utilization.

18. What is true about active list?

Answer: Refer hp0 m54.

19. When a package is having dependencies with another package how it will show in Arcsight console navigator

Answer: Yellow

20. What happens when you select auto update in 2 minutes in a search?

Answer: Search query will be executed again.

21. What port used for Arcsight command center

Answer: 8443

22. Why you need to lock a case?

Answer: If you want to prevent editing by someone else while you are doing something on it.

23. Which are 3 different types of data monitors?

Answer: Event based, correlation, non-event based

24. What is the focus in a focused report?

Answer: it is in M54

25. What is true about ACL (Access control List)?

Answer: specific user group to specific user resource.

26. Where the arcsight password policy settings are defined?

Answer: server. Properties

27. What are the 3 parts in an active channel?

Answer: 1.Header, 2.radar, 3.Grid (Need to check)

28. What all option we can't be performing through arcsight web?

Answer: data monitor can't be added to dashboard

29. What happens when you save a filter?

Answer: Named filter

30. How the escalations work in ESM

Answer:

31. Can we create our own custom escalation levels?

Answer: escalation level is in sequence, can be customized during any time.

32. IF you have missed to install a ESM solutions package while installing an ESM, how you will be able to install it later?

Answer: Right click and install

33. What is ESM event schema?

Answer: normalize and backbone of the data structure. The data collected from devices in your network is parsed into ESM's normalized schema

34. Dashboard can be drilled down to what in command centre

Answer: dashboard only

35. A report can be generated from what

Answer: query, trend, session list, active list)

36. When a connector start caching events

Answer: When connector services restarting, when it losses connection with destination.

37. What does the start time and end time in a notification destination means

Answer: In between the start and end time notification can be sent.

38. What works like a GPS for a privileged user monitoring?

Answer: Identity view.

39. What you will select if you want to receive real time events in an active channel

Answer: continuously evaluate

40. In a peered manager setup once the username and password has given for the remote peer, when we need to provide the username and password once again?

Answer: when it loses the connection

41. How can we reset all the console modifications and go back to default one

Answer: copy the console.default.properties file to console. Properties

42. Two examples for CIP (Compliance Insight Packages)

Answer: PCI, Sox

43. What is start time and end time in notification?

Answer: decide when to send notification to destination.

44. What will you see preference option

Answer: date and time

45. Which statement is true about report?

Answer: it can be scheduled daily weekly or .. , report can be created using active channel session list query.

46. Green light

Answer: it will add that thing to query.

47. While saving sewarch in command centre what happen when you check save to command centre.

Answer: it saves the report in local host.

48. When do we use constraints in search?

Answer: It limit the scope of search

49. Command center + peer+ content management.

Answer: manager work as a publisher

50. When you define storage group and command centre you can't change what?

Answer: storage name

51. If your db is down we use send utility command to send logs, how will you send log when manager is down.

Answer: arcdt command

52. Where will you see preference option?

Answer: Edit Option

53. What all option available when right clicks an event?

Answer: Annotate event, Investigate event)

54. What does a non event based data monitor do.

Answer: Shows system health)

55. Where can we edit the details regarding case?

Answer: (case editor)

56. What all types are used for Authentication?

Answer: (Radius, Microsoft AD, LDAP, JAAS plug in)

A simple search query consists of these elements:

#Query expression

#Time range

#Fieldset

You can enter a simple keyword, such as, hostA.companyxyz.com or a complex query

That includes Boolean expressions, keywords, fields, and regular expressions.

Which file Contains troubleshooting information?

Answer: server.log

What type of user can access ESM console, Web client and command centre

Answer: normal user

What must you do prior to applying a patch to the ArcSight Manager?

Answer: stops the ArcSight Manager Service

One of the benefits of SSL technology is authentication. What does authentication do?

D. ensures that clients send information to the actual intended server, not a machine pretending to be that server

---

What all thing can we see in command center. (The ArcSight Command Center provides a streamlined interface formanaging users, storage, and event data; monitoring events and running reports; and configuring storage, updating licenses, managing component authentication, and setting up storage notifications.)

What all functions are available in command center (2 answer)

what all function are available through session list.

What all function available through query viewer (Options: reports, dashboard etc.)

What is event schema

What is the first phase happens in Connector (Event normalisation etc)

Data gathered by a query viewer can be added to dashboards, published as reports, and made accessible for viewing in the ArcSight Web client.

The ArcSight Command Center provides a streamlined interface for managing users, storage, and event data; monitoring events and running reports; and configuring storage, updating licenses, managing component authentication, and setting up storage notifications.

With content management, you can establish peer relationships with other ESM installations, search, and synchronize ESM content across peers. Searches ranging from simple to complex are easy to configure and saved for regular use

ArcSight Web provides a secure web-based interface to the Manager. ArcSight Web provides event monitoring and drill-down capabilities in dashboards and active channels, reporting, case management, and notifications for Security Analysts. As a security feature, ArcSight Web does not allow authoring or administration functions.

The ArcSight Web version must match the Manager version so that the security certificate between the Manager and ArcSight Web match.

----------*****----------*****----------*****----------

Important Topics (Read Carefully Once)

>Focus report

>TTl

>Query viewer

>Query Viewer Usage

>Report Scheduling

>ACL Administration

-User Group

-Storage Group

Storage resource

>Work Flow Management

>Commmand center And **important>command center main tabs**

>CIP

>PCI

>Sarbanes Oxley act(Sox)

>Export Search results

>Arcsight Password Policy

>ESM SW Tarball,connector SW

>Identity View

---

*views are associated with the Viewer Panel-(Resource views,Results views,Active Channel views,Dashboard)

*In active channel when we select Time range (Start time- $Now-1d) in attribute

This type of time is known as -

a. custom

b. Dynamic

c. By default

d. Static

*Which resources can be displayed in the ArcSight Web interface(Reports and Dashboards,Cases, Notifications, and Active Channels)

*Which command is a valid investigate command? -- Add [Attribute=Value] to Filter

* One diagram based question-- source event -> Source Ip->Host-> Target Ip(Event graph)

*What is a criteria factor within the ArcSight Priority Formula-Model confidence

*Priority Formula calculation run on?-the Manager only

*What is the default port used by the command center to connect to the ArcSight Web Console?--9443

*What do the start and end times associated with a notification destination indicate?--the period of time during which the notification can be sent

*QUestin no- 57 (M-55 Dump)

*command For modify retention periods?-(Arcsight database pc)

*your db is down we use send utilioty command to send logs, how will you send log when manager is down.

ans.. (arcdt command)

*RADIUSAuthentication Port-(1812)

*all types are used for Authentication (RADIUSAuthentication,Microsoft Active Directory,Simple LDAP SSL,JAAS Plug-in)

*To turn archiving on or off:-(Click Administration > Storage and Archive, and then

open the Storage tab.>Click Status On to turn archiving off. Click Status Off to turn

archiving on.)

*In Command Center When You Retrieve a log Then Which Type Of User yoU have Must>(You must be an administrative user to access this feature)

*ESM Foundation package

*applications such as reporting on

attacks by division, or for compliance monitoring as in reporting the number of compromise

events directed at-(Sarbanes Oxley act)

*ESM Installation >System.properties

*Question No 15 (A100 Dump)

*What is Default Time Range Of active Channel To Retrieve A event Log ?

* Pushing Content Packages (Command Center>Administrator>Content management) *****Read Once Whole Topic

*Rerunning the Suite Installer(Install Guide)--

(1 Remove all install.dir.xxxx directories from the /tmp directory.

2 Remove all directories and files in the /opt/arcsight directory.

3 Rerun the installer.)