[May 22, 2022 Free Splunk Enterprise Security Certified Admin SPLK-3001 Exam Question [Q37-Q53

[May 22, 2022] Free Splunk Enterprise Security Certified Admin SPLK-3001 Exam Question
SPLK-3001 dumps & Splunk Enterprise Security Certified Admin sure practice dumps

What skills and knowledge would you gain from a Splunk SPLK-3001?

The SPLK-3001 will develop your skills to the next level with regard to data analysis, software architecture and databases. With this certification, you'll gain the following skills:
The fundamental knowledge of how to design and set the architecture for a Splunk Enterprise deployment.Many days of learning regarding how Hadoop works and how it can be integrated into your database.
There are many advantages that you can get from becoming a certified Splunk SPLK-3001. The most important advantage is the assurance of benefits from your employer. So if you have a Splunk SPLK-3001 certification, employers expect you to be able to understand complex information quickly and accurately.
In addition, a Splunk SPLK-3001 certification will help you in quickly grabbing the attention of potential clients and employers. This certification indicates that you are not only experienced in Splunk, but also in all other aspects of the software industry. These employers will certainly make you an attractive candidate for their hiring needs.

NO.37 Where is it possible to export content, such as correlation searches, from ES?
* Content exporter
* Configure -> Content Management
* Export content dashboard

* Settings Menu -> ES -> Export
Explanation

Explanation/Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Export

NO.38 A newly built custom dashboard needs to be available to a team of security analysts In ES. How is It possible to Integrate the new dashboard?
* Add links on the ES home page to the new dashboard.
* Create a new role Inherited from es_analyst, make the dashboard permissions read-only, and make this dashboard the default view for the new role.
* Set the dashboard permissions to allow access by es_analysts and use the navigation editor to add it to the menu.
* Add the dashboard to a custom add-in app and install it to ES using the Content Manager.

NO.39 Which correlation search feature is used to throttle the creation of notable events?
* Schedule priority.
* Window interval.
* Window duration.
* Schedule windows.
Reference:

https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Configurecorrelationsearches

NO.40 At what point in the ES installation process should Splunk_TA_ForIndexes.splbe deployed to the indexers?
* When adding apps to the deployment server.
* Splunk_TA_ForIndexers.splis installed first.
* After installing ES on the search head(s) and running the distributed configuration management tool.
* Splunk_TA_ForIndexers.spl is only installed on indexer cluster sites using the cluster master and the splunk apply cluster-bundlecommand.
Explanation/Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallTechnologyAdd-ons

NO.41 Glass tables can display static images and text, the results of ad-hoc searches, and which of the following objects?
* Lookup searches.
* Summarized data.
* Security metrics.
* Metrics store searches.

NO.42 What is the bar across the bottom of any ES window?
* The Investigator Workbench.
* The Investigation Bar.
* The Analyst Bar.
* The Compliance Bar.

NO.43 When ES content is exported, an app with a .spl extension is automatically created. What is the best practice when exporting and importing updates to ES content?
* Use new app names each time content is exported.
* Do not use the .spl extension when naming an export.
* Always include existing and new content for each export.
* Either use new app names or always include both existing and new content.
Explanation

Either use new app names each time (which could be difficult to manage) or make sure you always include all content (old and new) each time you export.

NO.44 An administrator is provisioning one search head prior to installing ES. What are the reference minimum requirements for OS, CPU, and RAM for that machine?
* OS: 32 bit, RAM: 16 MB, CPU: 12 cores
* OS: 64 bit, RAM: 32 MB, CPU: 12 cores
* OS: 64 bit, RAM: 12 MB, CPU: 16 cores
* OS: 64 bit, RAM: 32 MB, CPU: 16 cores

NO.45 To observe what network services are in use in a network’s activity overall, which of the following dashboards in Enterprise Security will contain the most relevant data?
* Intrusion Center
* Protocol Analysis
* User Intelligence
* Threat Intelligence

Explanation/Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/NetworkProtectionDomaindashboards

NO.46 When investigating, what is the best way to store a newly-found IOC?
* Paste it into Notepad.
* Click the “Add IOC” button.
* Click the “Add Artifact” button.
* Add it in a text note to the investigation.

NO.47 What does the risk framework add to an object (user, server or other type) to indicate increased risk?
* An urgency.
* A risk profile.
* An aggregation.
* A numeric score.

NO.48 An administrator is provisioning one search head prior to installing ES. What are the reference minimum requirements for OS, CPU, and RAM for that machine?
* OS: 32 bit, RAM: 16 MB, CPU: 12 cores
* OS: 64 bit, RAM: 32 MB, CPU: 12 cores
* OS: 64 bit, RAM: 12 MB, CPU: 16 cores
* OS: 64 bit, RAM: 32 MB, CPU: 16 cores

Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/8.0.2/Capacity/Referencehardware

NO.49 Which settings indicates that the correlation search will be executed as new events are indexed?
* Always-On
* Real-Time
* Scheduled
* Continuous

Explanation/Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Configurecorrelationsearches

NO.50 Adaptive response action history is stored in which index?
* cim_modactions
* modular_history
* cim_adaptiveactions
* modular_action_history

NO.51 What role should be assigned to a security team member who will be taking ownership of notable events in the incident review dashboard?
* ess_user
* ess_admin
* ess_analyst
* ess_reviewer

Explanation/Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/Triagenotableevents

NO.52 In order to include an eventtype in a data model node, what is the next step after extracting the correct fields?
* Save the settings.
* Apply the correct tags.
* Run the correct search.
* Visit the CIM dashboard.

NO.53 Which settings indicated that the correlation search will be executed as new events are indexed?
* Always-On
* Real-Time
* Scheduled
* Continuous