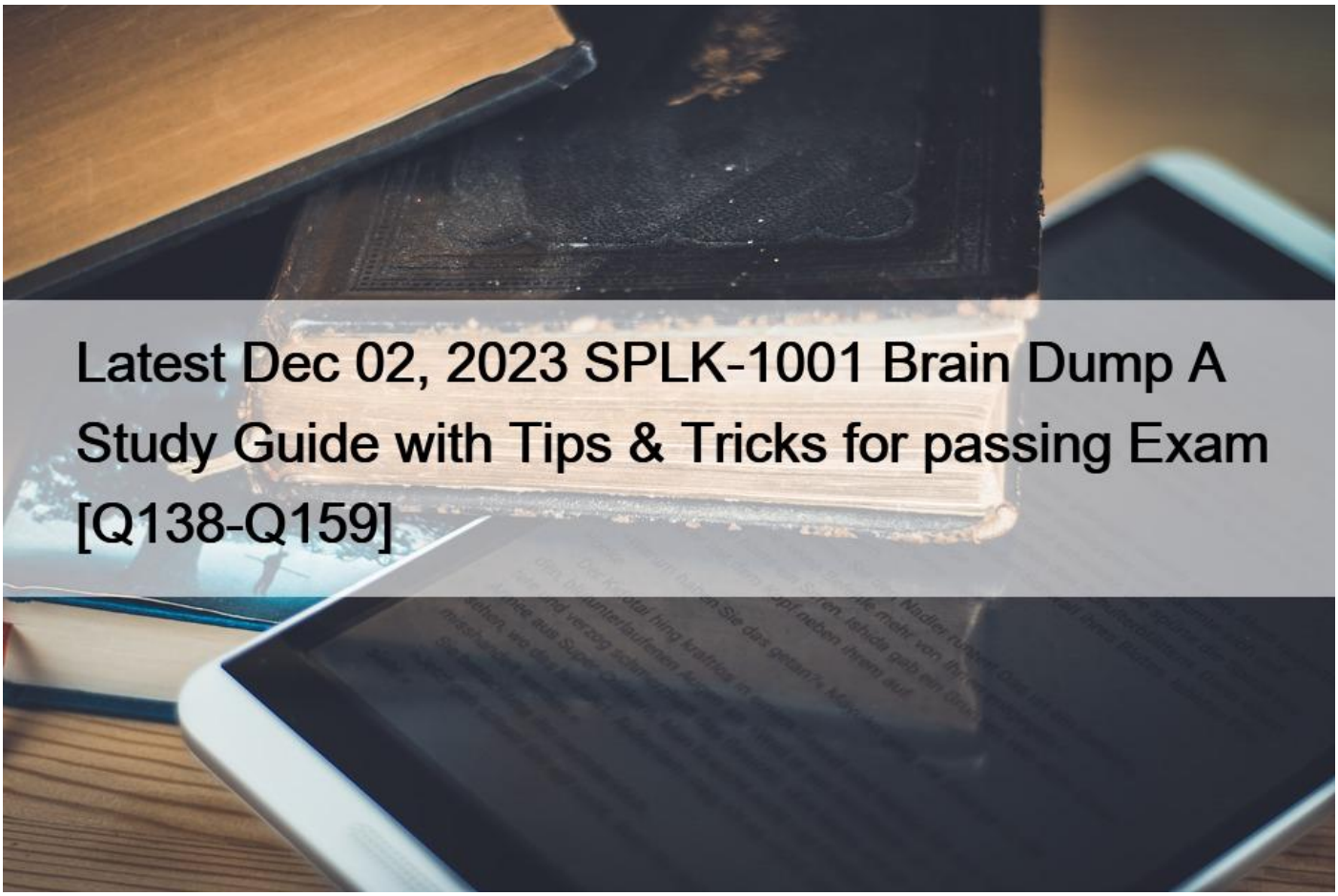
Latest Dec 02, 2023 SPLK-1001 Brain Dump A Study Guide with Tips & Tricks for passing Exam [Q138-Q159



Latest Dec 02, 2023 SPLK-1001 Brain Dump: A Study Guide with Tips & Tricks for passing Exam
SPLK-1001 Question Bank: Free PDF Download Recently Updated Questions

Q138. Which of the following is an option after clicking an item in search results?
* Saving the item to a report
* Adding the item to the search.
* Adding the item to a dashboard
* Saving the search to a JSON file.

Q139. In a deployment with multiple indexes, what will happen when a search is run and an index is not specified in the search string?
* No events will be returned.
* Splunk will prompt you to specify an index.
* All non-indexed events to which the user has access will be returned.
* Events from every index searched by default to which the user has access will be returned.

Explanation

Q140. What options do you get after selecting timeline? (Choose four.)
* Zoom to selection
* Format Timeline
* Deselect
* Delete
* Zoom Out

Explanation/Reference:

Q141. You can on-board data to Splunk using following means (Choose four.):
* Props
* CLI
* Splunk Web
* savedsearches.conf
* Splunk apps and add-ons
* indexes.conf
* inputs.conf
* metadata.conf

Q142. What are the two most efficient search filters?
* _time and host
* _time and index
* host and sourcetype
* index and sourcetype

This is the correct answer because these two filters can help you limit the amount of data that Splunk retrieves from disk, which is the key to fast searching1. The _time filter allows you to specify a narrow time window for your search, which reduces the number of buckets that Splunk scans2. The index filter allows you to specify which index or indexes contain the data that you want to search, which reduces the number of files that Splunk reads3.

Q143. Splunk Parses data into individual events, extracts time, and assigns metadata.
* False
* True

Q144. These users can create global knowledge objects. (Select all that apply.)
* users
* power users
* administrators

Q145. Which of the following searches would return events with failure in index netfw or warn :r critical in index netops?
* (index=netfw failure) AND index=netops warn OR critical
* (index=netfw failure) OR (index=netops (warn OR critical))
* (index=netfw failure) AND (index=r.etops (warn OR critical))
* (index=netfw failure) OR index=r.etops OR (warn OR critical)

Q146. In the Search and Reporting app, which is a default selected field?
* index
* action
* _time
* host

Explanation

In the Search and Reporting app, _time is a default selected field. This means that it is always displayed in the events list and table views, unless explicitly deselected. Other default selected fields are host, source, and sourcetype. Index and action are not default selected fields, but they can be added to the list of selected fields by clicking on All Fields4.

Q147. Which Field/Value pair will return only events found in the index named security?
* Index=Security
* index=Security
* Index=security
* index!=Security

Explanation/Reference: https://answers.splunk.com/answers/712164/why-are-the-wineventlogssecurity-indexing-in- diffe.html

Q148. What is the proper SPL terminology for specifying a particular index in a search?
* indexer-index_name
* indexer name-index_name
* index=index_name
* index name=index_name

This means that you can use the index field to filter your search results by the name of the index that contains the events you want to see.

For example, if you want to search for events in the index named “gcp_logs”, you can use the following SPL:

index=gcp_logs

You can also specify multiple indexes by using the OR operator, such as:

index=gcp_logs OR index=oswin

Q149. Which of the following is a best practice when writing a search string?
* Include all formatting commands before any search terms.
* Include at least one function as this is a search requirement.
* Include the search terms at the beginning of the search string.
* Avoid using formatting clauses, as they add too much overhead.

Q150. Monitor option in Add Data provides _____.
* Only continuous monitoring.
* Only One-time monitoring.
* None of the above.
* Both One-time and continuous monitoring

Q151. When looking at a dashboard panel that is based on a report, which of the following is true?
* You can modify the search string in the panel, and you can change and configure the visualization.
* You can modify the search string in the panel, but you cannot change and configure the visualization.
* You cannot modify the search string in the panel, but you can change and configure the visualization.
* You cannot modify the search string in the panel, and you cannot change and configure the visualization.

When looking at a dashboard panel that is based on a report, you cannot modify the search string in the panel, but you can change and configure the visualization. This is because the dashboard panel inherits the search string from the report, and any changes to the search string will affect the report as well. However, you can customize the visualization settings for the dashboard panel without affecting the report. Reference: Splunk Core User Certification Exam Study Guide, page 37.

Q152. Which of the following is the best way to create a report that shows the last 24 hours of events?

* Use earliest=-1d@d latest=@d
* Set a real-time search over a 24-hour window
* Use the time range picket to select “Yesterday”
* Use the time range picker to select “Last 24 hours”

Explanation/Reference: https://answers.splunk.com/answers/153100/how-to-get-the-event-count-for-the-last-24-hours-as-a-scheduled-report.html

Q153. According to Splunk best practices, which placement of the wildcard results in the most efficient search?
* f*il
* *fail
* fail*
* *fail*

Explanation

Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Search/Wildcards

Q154. Which of the following searches would return events with failurein index netfwor warn or criticalin index netops?
* (index=netfw failure) AND index=netops warn OR critical
* (index=netfw failure) OR (index=netops (warn OR critical))
* (index=netfw failure) AND (index=netops (warn OR critical))
* (index=netfw failure) OR index=netops OR (warn OR critical)

Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Aboutsubsearches

Q155. Which is a primary function of the timeline located under the search bar?
* To differentiate between structured and unstructured events in the data
* To sort the events returned by the search command in chronological order
* To zoom in and zoom out. although this does not change the scale of the chart
* To show peaks and/or valleys in the timeline, which can indicate spikes in activity or downtime

Q156. In monitor option you can select the following options in GUI.
* Only HTTP Event Collector (HEC) and TCP/UDP
* None of the above
* Only TCP/UDP
* Only Scripts
* Filed & Directories, HTTP Event Collector (HEC), TCP/UDP and Scripts

Q157. @ Symbol can be used in advanced time unit option.
* No
* Yes

Q158. What is Splunk?
* Splunk is a software platform to search, analyze and visualize the machine-generated data.
* Database management tool.
* Security Information and Event Management (SIEM).
* Cloud based application that help in analyzing logs.

Q159. Splunk extracts fields from event data at index time and at search time.
* True
* False

Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.2.3/SearchTutorial/Usefieldstosearch

New SPLK-1001 Exam Dumps with High Passing Rate: https://www.actualtests4sure.com/SPLK-1001-test-questions.html]