Splunk

Exam Questions SPLK-1004

Splunk Core Certified Advanced Power User

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
How is a cascading input used?

A. As part of a dashboard, but not in a form.
B. Without notation in the underlyin
C. XML.
D. As a way to filter other input selections.
E. As a default way to delete a user role.

Answer: C

Explanation:
A cascading input is used as a way to filter other input selections within a dashboard or form (Option C). It enables a dynamic user interface where the selection made in one input (e.g., a dropdown menu) determines the available options in another input. This setup allows for more intuitive and relevant user interactions, as each choice narrows down the subsequent options to ensure they are contextually appropriate.

NEW QUESTION 2
Which of the following has a schema or structure embedded in the data itself?

A. Dark data
B. Unstructured data
C. Embedded data
D. Self-describing data

Answer: D

Explanation:
Self-describing data (Option D) refers to data that includes information about its own structure or schema within the data itself. This characteristic makes it easier to understand and process the data because the structure and meaning of the data are embedded with the data, reducing the need for external definitions or mappings. Examples of self- describing data formats include JSON and XML, where elements and attributes describe the data they contain.

NEW QUESTION 3
What is one way to troubleshoot dashboards?

A. Run the | previous_searches command to troubleshoot your SPL queries.
B. Go to the Troubleshooting dashboard of me Searching and Reporting app.
C. Delete the dashboard and start over.
D. Create an HTML panel using tokens to verify that they are being set.

Answer: B

Explanation:
To troubleshoot dashboards in Splunk, one effective approach is to go to the Troubleshooting dashboard of the Search & Reporting app (Option B). This dashboard provides insights into the performance and potential issues of other dashboards and searches, offering a centralized place to diagnose and address problems. This method allows for a structured approach to troubleshooting, leveraging built-in tools and reports to identify and resolve issues.

NEW QUESTION 4
When possible, what is the best choice for summarizing data to improve search performance?

A. Us the fieldsummary command.
B. Data model acceleration
C. Report acceleration
D. Summary indexing

Answer: D

NEW QUESTION 5
which function of the stats command creates a multivalue entry?

A. mvcombine
B. eval
C. makemv
D. list

Answer: D

NEW QUESTION 6
What is returned when Splunk finds fewer than the minimum matches for each lookup value?

A. The default value NULL until the minimum match threshold is reached.
B. The default match value until the minimum match threshold Is reached.
C. The first match unless the time_field attribute is specified.
D. Only the first match.

Answer: A

Explanation:
When Splunk's lookup feature finds fewer than the minimum matches specified for each lookup value, it returns the default value NULL for those unmatched entries until the minimum match threshold is reached (Option A). This behavior ensures that lookups return consistent and expected results, even when the available data does not meet the specified criteria for a minimum number of matches.

NEW QUESTION 7
Where does the output of an append command appear in the search results?

A. Added as a column to the right of the search results.
B. Added as a column to the left of the search results.
C. Added to the beginning of the search results.
D. Added to the end of the search results.

Answer: D

Explanation:
The output of an append command in Splunk search results is added to the end of the search results (Option D). The append command is used to concatenate the results of a subsearch to the end of the current search results, effectively extending the result set with additional data. This can be particularly useful for combining related datasets or adding contextual information to the existing search results.

NEW QUESTION 8
Which predefined drilldown token passes a clicked value from a table row?

A. $rowclic
B. <fieldname>$
C. $tableclick .< fieldname>$
D. $ro
E. <fieldname>$
F. $table .< fieldname>$

Answer: A

Explanation:
The predefined drilldown token that passes a clicked value from a table row in Splunk dashboards is $row.<fieldname>$ (Option A). This token syntax is used within the drilldown configuration of a dashboard panel to capture the value of a specific field from a row where the user clicks. This value can then be passed to another dashboard panel or used within the same panel to dynamically update the content based on the user's interaction, enhancing the interactivity and relevance of dashboard data presentations.

NEW QUESTION 9
How is regex passed to the makemv command?

A. makemv be preceded by the erex command.
B. It is specified by the delim argument.
C. It Is specified by the tokenizer argument.
D. Makemv must be preceded by the rex command.

Answer: B

Explanation:
The regex is passed to the makemv command in Splunk using the delim argument (Option B). This argument specifies the delimiter used to split a single string field into multiple values, effectively creating a multivalue field from a field that contains delimited data.

NEW QUESTION 10
What capability does a power user need to create a Log Event alert action?

A. edit_search_server
B. edit udp
C. edit_tcp
D. edit_alerts

Answer: D

Explanation:
To create a Log Event alert action in Splunk, a power user needs the edit_alerts capability (Option D). This capability allows the user to configure and manage alert actions, including setting up alerts to log specific events based on predefined conditions within Splunk's alerting framework.

NEW QUESTION 10
Which syntax is used when referencing multiple CSS files in a view?

A. <dashboard stylesheet="custom.css, userapps.css">
B. <dashboard style="custom.css, userapps.css">
C. <dashboard stylesheet=custom.css stylesheet=userapps.css>
D. <dashboard stylesheet="custom.css | userapps.css">

Answer: C

Explanation:

When referencing multiple CSS files in a Splunk dashboard view (within Simple XML), the correct approach is to include separate stylesheet attributes for each CSS file. The syntax for this would be similar to <dashboard stylesheet="custom.css" stylesheet="userapps.css"> (Option C). This method allows the dashboard to load and apply the styles from both CSS files, enhancing the dashboard's visual appearance and user interface design.

NEW QUESTION 13
What command is used la compute find write summary statistic, to a new field in the event results?

A. tstats
B. stats
C. eventstats
D. transaction

Answer: C

Explanation:
The eventstats command in Splunk is used to compute and add summary statistics to all events in the search results, similar to the stats command, but without grouping the results into a single event(Option C). This command adds the computed summary statistics as new fields to each event, allowing those fields to be used in subsequent search operations or for display purposes. Unlike the transaction command, which groups events into transactions, eventstats retains individual events while enriching them with statistical information.

NEW QUESTION 16
Which of the following would exclude all entries contained in the lookup file baditems. csv from search results?

A. NOT [inputlookup baditems.csv]
B. NOT (lookup baditems.csv OUTPUT item)
C. WHERE item NOT IN (baditems.csv)
D. [NOT inputlookup baditems.csv]

Answer: A

Explanation:
The correct syntax to exclude all entries contained in the lookup file baditems.csv from search results is NOT [inputlookup baditems.csv]. This syntax uses a subsearch with the inputlookup command to retrieve the contents of the baditems.csv lookup file and then uses the NOT operator to exclude those results from the main search. This approach is efficient for filtering out unwanted data based on a predefined list of criteria stored in a lookup file.

NEW QUESTION 19
When using a nested search macro, how can an argument value be passed to the inner macro?

A. The argument value may be passed to the outer macro.
B. An argument cannot be used with an inner nested macro.
C. An argument cannot be used with an outer nested macro.
D. The argument value must be specified in the outer macro.

Answer: A

Explanation:
When using a nested search macro in Splunk, an argument value can be passed to the inner macro by specifying the argument in the outer macro's invocation (Option A). This allows the outer macro to accept arguments from the user or another search command and then pass those arguments into the inner macro, enabling dynamic and flexible macro compositions that can adapt based on input parameters.

NEW QUESTION 20
What is the correct hierarchy of XML elements in a dashboard panel?

A. <panel><dashboard><row>
B. <dashboard><row><panel>
C. <dashboard><panel><row>
D. <panel><row><dashboard>

Answer: B

Explanation:
In a Splunk dashboard, the correct hierarchy of XML elements for a dashboard panel is
<dashboard><row><panel> (Option B). A Splunk dashboard is defined within the
<dashboard> element. Within this, <row> elements are used to organize the layout into rows, and each <panel> element within a row defines an individual panel that can contain visualizations, searches, or other content. This hierarchical structure allows for organized and customizable layouts of dashboard elements, facilitating clear presentation of data and analyses. The other options provided do not represent the correct hierarchical order for defining dashboard panels in Splunk's XML dashboard syntax.

NEW QUESTION 25
......

Relate Links

100% Pass Your SPLK-1004 Exam with Exambible Prep Materials

https://www.exambible.com/SPLK-1004-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/