Free Questions for SPLK-1002 by vceexamstest

Shared by Clements on 15-04-2024

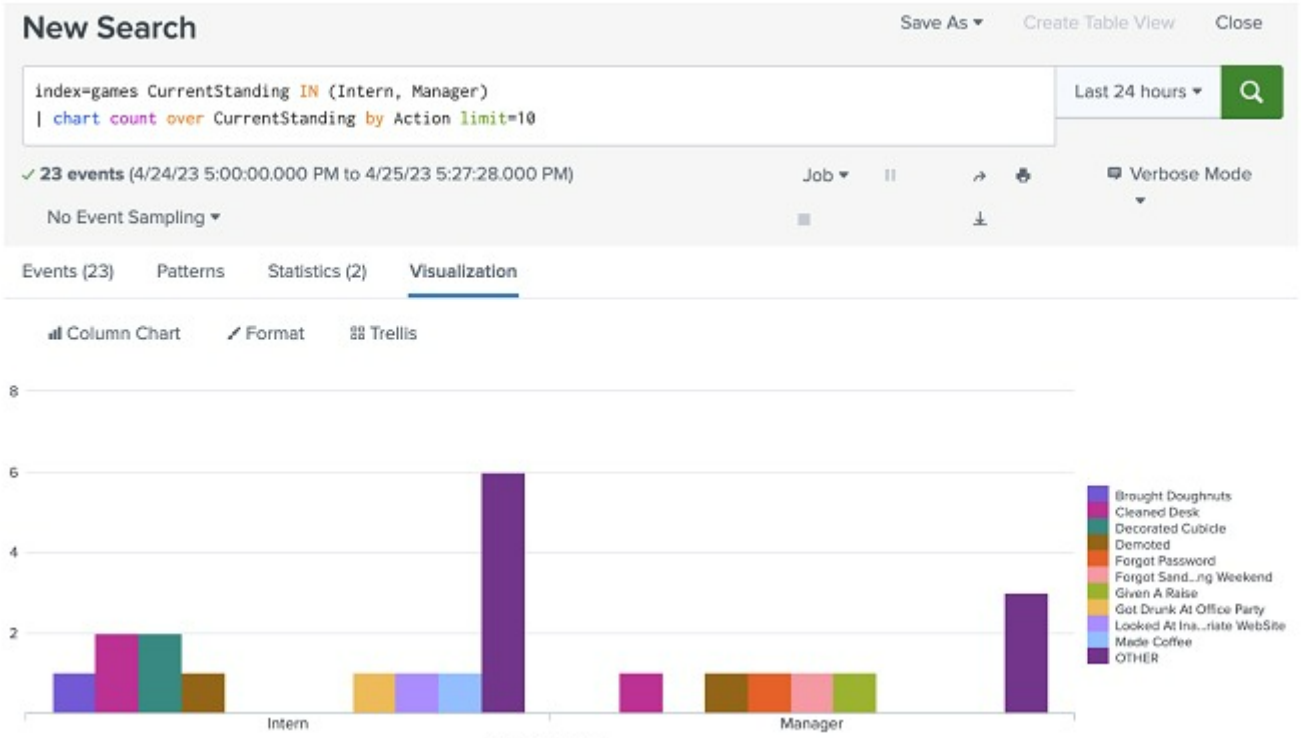
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

How could the following syntax for the chart command be rewritten to remove the OTHER category? (select all that apply)



Options:

A- | chart count over CurrentStanding by Action useother=f

B- | chart count over CurrentStanding by Action usenull-f useother-t

C- | chart count over CurrentStanding by Action limit=10 useother=f

D- | chart count over CurrentStanding by Action limit-10

Answer:

A, C

Explanation:

In Splunk, when using the chart command, the useother parameter can be set to false (f) to remove the 'OTHER' category, which is a bucket that Splunk uses to aggregate low-cardinality groups into a single group to simplify visualization. Here's how the options break down:

A) | chart count over CurrentStanding by Action useother=f This command correctly sets the useother parameter to false, which would prevent the 'OTHER' category from being displayed in the resulting visualization.

B) | chart count over CurrentStanding by Action usenull=f useother=t This command has useother set to true (t), which means the 'OTHER' category would still be included, so this is not a correct option.

C) | chart count over CurrentStanding by Action limit=10 useother=f Similar to option A, this command also sets useother to false, additionally imposing a limit to the top 10 results, which is a way to control the granularity of the chart but also to remove the 'OTHER' category.

D) | chart count over CurrentStanding by Action limit-10 This command has a syntax error (limit-10 should be limit=10) and does not include the useother=f clause. Therefore, it would not remove the 'OTHER' category, making it incorrect.

The correct answers to rewrite the syntax to remove the 'OTHER' category are options A and C, which explicitly set useother=f.

Question 2

Question Type: **MultipleChoice**

Which of the following can be saved as an event type?

Options:

A- index-server_472 sourcetype-BETA_494 code-488 I stats count by code

B- index=server_472 sourcetype=BETA_494 code=488 [I inputlookup append=t servercode.csv]

C- index=server_472 sourcetype=BETA_494 code=488 I stats where code > 200

D- index=server_472 sourcetype=BETA_494 code-488

Answer:

D

Explanation:

Event types in Splunk are saved searches that categorize data, making it easier to search for specific patterns or criteria within your data. When saving an event type, the search must essentially filter events based on criteria without performing operations that transform or aggregate the data. Here's a breakdown of the options:

A) The search index-server_472 sourcetype-BETA_494 code-488 | stats count by code performs an aggregation operation (stats count by code), which makes it unsuitable for saving as an event type. Event types are meant to categorize data without aggregating or transforming it.

B) The search index=server_472 sourcetype=BETA_494 code=488 [| inputlookup append=t servercode.csv] includes a subsearch and input lookup, which is typically used to enrich or filter events based on external data. This complexity goes beyond simple event categorization.

C) The search index=server_472 sourcetype=BETA_494 code=488 | stats where code > 200 includes a filtering condition within a transforming command (stats), which again, is not suitable for defining an event type due to the transformation of data.

D) The search index=server_472 sourcetype=BETA_494 code-488 is the correct answer as it purely filters events based on index, sourcetype, and a code field condition without transforming or aggregating the data. This is what makes it suitable for saving as an event type, as it categorizes data based on specific criteria without altering the event structure or content.

Question 3

Question Type: MultipleChoice

Using the Field Extractor (FX) tool, a value is highlighted to extract and give a name to a new field. Splunk has not successfully extracted that value from all appropriate events. What steps can be taken so Splunk successfully extracts the value from all appropriate events? (select all that apply)

Options:

A- Select an additional sample event with the Field Extractor (FX) and highlight the missing value in the event.

B- Re-ingest the data and attempt to extract from a new dataset.

C- Click on the event where the field was not extracted and choose "Change to Delimited'.

D- Edit the regular expression manually.

Answer:

A, D

Explanation:

When using the Field Extractor (FX) tool in Splunk and the tool fails to extract a value from all appropriate events, there are specific steps you can take to improve the extraction process. These steps involve interacting with the FX tool and possibly adjusting the extraction method:

A) Select an additional sample event with the Field Extractor (FX) and highlight the missing value in the event. This approach allows Splunk to understand the pattern better by providing more examples. By highlighting the value in another event where it wasn't extracted, you help the FX tool to learn the variability in the data format or structure, improving the accuracy of the field extraction.

D) Edit the regular expression manually. Sometimes the FX tool might not generate the most accurate regular expression for the field extraction, especially when dealing with complex log formats or subtle nuances in the data. In such cases, manually editing the regular expression can significantly improve the extraction process. This involves understanding regular expression syntax and how Splunk extracts fields, allowing for a more tailored approach to field extraction that accounts for variations in the data that the automatic process might miss.

Options B and C are not typically related to improving field extraction within the Field Extractor tool. Re-ingesting data (B) does not directly impact the extraction process, and changing to a delimited extraction method (C) is not always applicable, as it depends on the specific data format and might not resolve the issue of missing values across events.

Question 4

Question Type: MultipleChoice

How can an existing accelerated data model be edited?

Options:

A- An accelerated data model can be edited once its .tsidx file has expired.

B- An accelerated data model can be edited from the Pivot tool.

C- The data model must be de-accelerated before edits can be made to its structure.

D- It cannot be edited. A new data model would need to be created.

Answer:

C

Explanation:

An existing accelerated data model can be edited, but the data model must be de-accelerated before any structural edits can be made (Option C). This is because the acceleration process involves pre-computing and storing data, and changes to the data model's structure could invalidate or conflict with the pre-computed data. Once the data model is de-accelerated and edits are completed, it can be re-accelerated to optimize performance.

Question 5

Question Type: MultipleChoice

When would transaction be used instead of stats?

Options:

A- To see results of a calculation.

B- To group events based on start/end values.

C- To have a faster and more efficient search.

D- To group events based on a single field value.

Answer:

B

Explanation:

The transaction command is used instead of stats to group events based on start/end values (Option B). This is particularly useful in scenarios where related events span across multiple log entries and need to be analyzed as a single transaction, such as user sessions or multi-step transaction processes.

Question 6

Question Type: MultipleChoice

Where are the descriptions of the data models that come with the Splunk Common Information Model (CIM) Add-on documented?

Options:

A- Search and reporting user manual.

B- CIM Add-on manual.

C- Pivot users manual.

D- Datamodel command reference guide.

Answer:

B

Explanation:

The descriptions of the data models that come with the Splunk Common Information Model (CIM) Add-on are documented in the CIM Add-on manual (Option B). This manual provides detailed information about the data models, including their structure, the types of data they are designed to normalize, and how they can be used to facilitate cross-sourcing reporting and analysis.

Question 7

Question Type: MultipleChoice

Which of the following is true about a datamodel that has been accelerated?

Options:

A- They can be used with Pivot, the | tstats command, or the | datamodel command.

B- They can still be used in the Pivot tool but only with the accelerate_pivot capability.

C- They can no longer be used in the Pivot tool.

D- They can be used with the |tstats command, but will only return that data which has been accelerated.

Answer:

A

Explanation:

A data model that has been accelerated can be used with Pivot, the | tstats command, or the | datamodel command (Option A). Acceleration pre-computes and stores results for quicker access, enhancing the performance of searches and analyses that utilize the data model, especially for large datasets. This makes accelerated data models highly efficient for use in various analytical tools and commands within Splunk.

Question 8

Question Type: MultipleChoice

A user wants to create a workflow action that will retrieve a specific field value from an event and run a search in a new browser window in the user's Splunk instance. What kind of workflow action should they create?

Options:

A- A Run workflow action, because the user is running a new search with a specific field value from an event returned in the user's search.

B- A Search workflow action, because the user is running a new search with a specific field value from an event returned in the user's

search.

C- A POST workflow action, because the search is being sent to the user's current Splunk instance.

D- A GET workflow action, because a field value needs to be retrieved from the events returned in the user's search.

Answer:

B

Explanation:

A Search workflow action is the appropriate choice when a user wants to retrieve a specific field value from an event and run a search in a new browser window within their Splunk instance (Option B). This type of workflow action allows users to define a search that utilizes field values from selected events as parameters, enabling more detailed investigation or context-specific analysis based on the original search results.

To Get Premium Files for SPLK-1002 Visit

https://www.p2pexams.com/products/splk-1002

For More Free Questions Visit

https://www.p2pexams.com/splunk/pdf/splk-1002