SPLK-1002 Übungstest: Splunk Core Certified Power User Exam & SPLK-1002 Braindumps Prüfung

BONUS!!! Laden Sie die vollständige Version der ZertPruefung SPLK-1002 Prüfungsfragen kostenlos herunter: https://drive.google.com/open?id=1x5nJUbt6Wf69h0pyouSUgele1KeokrMq

Viele IT-Leute sind sich einig, dass Splunk SPLK-1002 Zertifikat ein Sprungbrett zu dem Höhepunkt der IT-Branche ist. Deshalb kümmern sich viele IT-Experten um die Splunk SPLK-1002 Zertifizierungsprüfung.

Splunk SPLK-1002 Exam Syllabus Topics:

Section	Weight	Objectives
Topic 1: Using the Common Information Model (CIM) Add-On	10%	- Describe the use of the CIM Add-On - Describe the Splunk CIM
Topic 2: Creating Field Aliases and Calculated Fields	10%	- Describe, create, and use calculated fields - Describe, create, and use field aliases
Topic 3: Creating Data Models	10%	- Create a data model - Describe the relationship between data models and pivot - Identify data model attributes
Topic 4: Filtering and Formatting Results	10%	- The fillnull command - Use the search and where commands to filter results - The eval command
Topic 5: Creating and Using Workflow Actions	10%	- Create a Search workflow action - Describe the function of GET, POST, and Search workflow actions - Create a POST workflow action - Create a GET workflow action
Topic 6: Creating and Using Macros	10%	- Create and use a basic macro - Describe macros - Add and use arguments with a macro - Define arguments and variables for a macro
Topic 7: Creating and Managing Fields	10%	- Perform regex field extractions using the Field Extractor (FX) - Perform delimiter field extractions using the FX

Topic 8: Correlating Events	15%	- Search with transactions - Identify transactions - Group events using fields and time - Group events using fields - Determine when to use transactions vs. stats - Report on transactions
Topic 9: Creating Tags and Event Types	10%	- Create an event type - Describe event types and their uses - Create and use tags
Topic 10: Using Transforming Commands for Visualizations	5%	- Use the chart command - Use the timechart command

>> SPLK-1002 Lernressourcen <<

SPLK-1002 Praxisprüfung - SPLK-1002 Originale Fragen

Sie können im Internet teilweise die Fragenkataloge zur Splunk SPLK-1002 Zertifizierungsprüfung von ZertPruefung kostenlos herunterladen. Dann würden Sie sich ganz gelassen auf Ihre Prüfung voebereiten. Wählen Sie die zielgerichteten Schulungsunterlagen, können Sie ganz leicht die Splunk SPLK-1002 Zertifizierungsprüfung bestehen.

Splunk Core Certified Power User Exam SPLK-1002 Prüfungsfragen mit Lösungen (Q193-Q198):

193. Frage
What is the purpose of a calculated field?

- A. To automatically add fields to the index using an eval expression rather than manually including an eval command.
- B. To automatically add fields at search time using an eval expression rather than manually including an eval command.
- C. To manually add and remove fields at search time related to statistical functions.
- D. To manually add fields at search time and check for syntax errors.

Antwort: B

Begründung:
A calculated field in Splunk is designed to automatically add fields at search time using an eval expression. This feature allows users to define new fields based on existing data without needing to manually include an eval command in every search. Calculated fields simplify repeated search tasks by embedding the eval logic directly into the field configuration.
Reference:
Splunk Docs: Calculated fields
Splunk Answers: Purpose of calculated fields

194. Frage
Which of the following statements best describes a macro?

- A. A macro is a portion of a search that can be reused in multiple place
- B. A macro is a way to associate an additional (new) name with an existing field name.
- C. A macro is a method of categorizing events based on a search.
- D. A macro is a knowledge object that enables you to schedule searches for specific events.

Antwort: A

Begründung:
The correct answer is C. A macro is a portion of a search that can be reused in multiple places.
A macro is a way to reuse a piece of SPL code in different searches. A macro can be any part of a search, such as an eval statement or a search term, and does not need to be a complete command. A macro can also take arguments, which are variables that can be replaced by different values when the macro is called. A macro can also contain another macro within it, which is called a nested macro1.

To create a macro, you need to define its name, definition, arguments, and description in the Settings > Advanced Search > Search Macros page in Splunk Web or in the macros.conf file. To use a macro in a search, you need to enclose the macro name in backtick characters (`) and provide values for the arguments if any1.
For example, if you have a macro named my_macro that takes one argument named object and has the following definition:
search sourcetype= object
You can use it in a search by writing:
my_macro(web)
This will expand the macro and run the following SPL code:
search sourcetype=web
The benefits of using macros are that they can simplify complex searches, reduce errors, improve readability, and promote consistency1.
The other options are not correct because they describe other types of knowledge objects in Splunk, not macros. These objects are:
A) An event type is a method of categorizing events based on a search. An event type assigns a label to events that match a specific search criteria. Event types can be used to filter and group events, create alerts, or generate reports2.
B) A field alias is a way to associate an additional (new) name with an existing field name. A field alias can be used to normalize fields from different sources that have different names but represent the same data. Field aliases can also be used to rename fields for clarity or convenience3.
D) An alert is a knowledge object that enables you to schedule searches for specific events and trigger actions when certain conditions are met. An alert can be used to monitor your data for anomalies, errors, or other patterns of interest and notify you or others when they occur4.
Reference:
About event types
About field aliases
About alerts
Define search macros in Settings
Use search macros in searches

195. Frage
For the following search, which command would further filter for only IP addresses present more than five times?

- A. index=games I search IP > 5
- B. index=games | search IP_Count > 5
- C. index=games | where IP > 5
- D. index=games I stats count as IP_count by IP B. | where IP_count > 5

Antwort: D

Begründung:
To filter for only IP addresses that appear more than five times in the search results for index=games, you can use a combination of the stats and where commands. The stats command counts the occurrences of each IP address and assigns the count to IP_count. The where command then filters the results to include only those IP addresses with a count greater than five.
Here is how the complete search would look:
index=games | stats count as IP_count by IP | where IP_count > 5
References:
* Splunk Docs: stats command
* Splunk Docs: where command
* Splunk Answers: Filtering results using stats and where commands

196. Frage
Which of the following searches will return all clientip addresses that start with 108?

- A. ... | search clientip=108
- B. ... | where (clientip, "108. %")
- C. ... | where like (clientip, "108.%)
- D. ... | where (clientip=108. %)

Antwort: C

197. Frage
Which of the following describes this search?
New Search
'third_party_outages(EMEA,-24h)'

- A. This search will find all events for the third_party_outages event type that have "EMEA" or "-24h" in the raw event data.
- B. This search will run the third_party_outages macro and pass the arguments EMEA and -24h to the macro definition.
- C. This search will run the third_party_outages saved search and filter for events containing "EMEA" and "-24h" in the raw event data.
- D. This search will find all events in the third_party_outages index with the tags EMEA and -24h.

Antwort: B

Begründung:
This search will run the third_party_outages macro and pass the arguments EMEA and -24h to the macro definition. A search macro is a reusable chunk of SPL that can be inserted into other searches. A search macro can take arguments that are used to resolve the search string at execution time. The syntax for using a search macro is macro_name (argument1, argument2, ...).ReferencesSee Use search macros in searches and Search macro examples in the Splunk Documentation.

198. Frage
.....

SPLK-1002 ist eine Splunk Zertifizierungsprüfung. So ist SPLK-1002 Zertifizierung der erste Schritt zur Splunk Zertifizierung. Deswegen ist die SPLK-1002 Zertifizierungsprüfung kürzlich immer beliebter geworden. Immer mehr Leute haben sich an der Splunk SPLK-1002 Zertifizierungsprüfung beteiligt. Aber die Erfolgsquote in der Prüfung ist nicht so hoch. Wählen Sie auch einschlägige Prüfungskurse, wenn Sie SPLK-1002 Prüfung ablegen möchten?

myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

P.S. Kostenlose und neue SPLK-1002 Prüfungsfragen sind auf Google Drive freigegeben von ZertPruefung verfügbar: https://drive.google.com/open?id=1x5nJUbt6Wf69h0pyouSUgele1KeokrMq