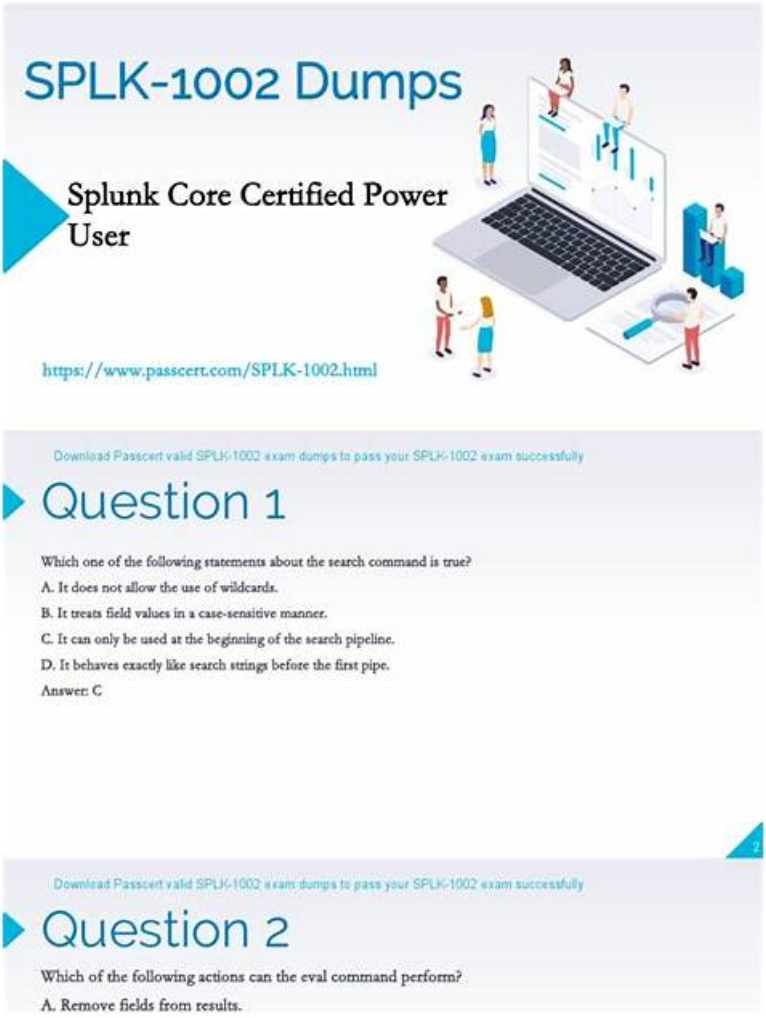
SPLK-1002 Schulungsunterlagen, SPLK-1002 Demotesten



Außerdem sind jetzt einige Teile dieser ZertSoft SPLK-1002 Prüfungsfragen kostenlos erhältlich: https://drive.google.com/open?id=1iOJau42tXr92XUA6HFTTsh9S6OmLuDPA

In Bezug auf die Splunk SPLK-1002 Zertifizierungsprüfung ist die Zuverlässigkeit nicht zu ignorieren. Die Schulungsmaterialien zur SPLK-1002 Zertifizierungsprüfung von ZertSoft werden besonders entworfen, um Ihre Effizienz zu erhöhen. Unsere Website hat weltweit die höchste Erfolgsquote.

Die Splunk SPLK-1002-Zertifizierungsprüfung ist ein wertvoller Berechtigungsnachweis für IT-Fachkräfte, die ihre Expertise bei der Verwendung von Splunk-Software nachweisen möchten, um Erkenntnisse aus großen Datenmengen zu extrahieren. Das Zertifizierungsprogramm bietet Einzelpersonen die Möglichkeit, ihre Karriereaussichten zu verbessern und sich in einem wettbewerbsfähigen Arbeitsmarkt abzuheben.

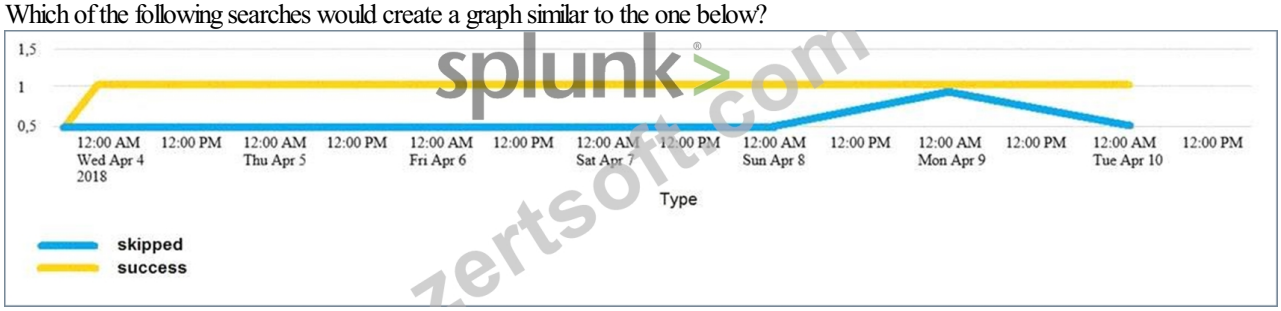
>> SPLK-1002 Schulungsunterlagen <<

SPLK-1002 Demotesten & SPLK-1002 Deutsche Prüfungsfragen

ZertSoft wird nicht nur Ihren Wunsch erfüllen, sondern Ihnen einen einjährigen kostenlosen Update-Service und Kundendienst bieten. Die Prüfungsfragen von ZertSoft sind alle richtig, die Ihnen beim Bestehen der Splunk SPLK-1002 Zertifizierungsprüfung helfen. Im ZertSoft können Sie kostenlos einen Teil der Fragen und Antworten zur Splunk SPLK-1002 Zertifizierungsprüfung als Probe herunterladen.

Splunk Core Certified Power User Exam SPLK-1002 Prüfungsfragen mit Lösungen (Q92-Q97):

92. Frage
Which of the following searches would create a graph similar to the one below?



- A. index_internal seourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan-id | start count states
- B. None of these searches would generate a similart graph.
- C. index_internal seourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan-id | timechart count by status
- D. index_internal seourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan-id | chart count states by -time

Antwort: C

Begründung:
The following search would create a graph similar to the one below:
index_internal sourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan=1d | timechart count by status The search does the following:
It uses index_internal to specify the internal index that contains Splunk logs and metrics.
It uses sourcetype=Savesplunker to filter events by the sourcetype that indicates the Splunk Enterprise Security app.
It uses fields sourcetype, status to keep only the sourcetype and status fields in the events.
It uses transaction status maxspan=1d to group events into transactions based on the status field with a maximum time span of one day between the first and last events in a transaction.
It uses timechart count by status to create a time-based chart that shows the count of transactions for each status value over time.
The graph shows the following:
It is a line graph with two lines, one yellow and one blue.
The x-axis is labeled with dates from Wed, Apr 4, 2018 to Tue, Apr 10, 2018.
The y-axis is labeled with numbers from 0 to 15.
The yellow line represents "shipped" and the blue line represents "success".
The yellow line has a steady increase from 0 to 15, while the blue line has a sharp increase from 0 to 5, then a decrease to 0, and then a sharp increase to 10.
The graph is titled "Type".
Therefore, option C is the correct answer.

93. Frage
Which of the following statements about calculated fields in Splunk is true?

- A. Calculated fields can be chained together to create more complex fields.
- B. Calculated fields can only be used in saved reports.
- C. Calculated fields can only be used in dashboards.
- D. Calculated fields cannot be chained together to create more complex fields

Antwort: A

Begründung:
The correct answer is B. Calculated fields can be chained together to create more complex fields.
Calculated fields are fields that are added to events at search time by using eval expressions. They can be used to perform calculations with the values of two or more fields already present in those events. Calculated fields can be defined with Splunk Web or in the props.conf file.They can be used insearches, reports, dashboards, and data models like any other extracted field1.

Calculated fields can also be chained together to create more complex fields. This means that you can use a calculated field as an input for another calculated field. For example, if you have a calculated field namedtotalthat sums up the values of two fields namedpriceandtax, you can use thetotalfield to create another calculated field nameddiscountthat applies a percentage discount to thetotalfield. To do this, you need to define thediscountfield with an eval expression that references thetotalfield, such as:
discount = total * 0.9
This will create a new field nameddiscountthat is equal to 90% of thetotalfield value for each event2.
References:
About calculated fields
Chaining calculated fields

94. Frage
In which of the following scenarios is an event type more effective than a saved search?

- A. When a search should always include the same time range.
- B. When the search string needs to be used in future searches.
- C. When a search needs to be added to other users' dashboards.
- D. When formatting needs to be included with the search string.

Antwort: B

95. Frage
When should the delimiter method be used in the Field Extractor?

- A. When the events need to be calculated using special characters.
- B. When the events need a regular expression to define the matching pattern.
- C. When the events do not have the correct permissions set.
- D. When the events are separated by a consistent character or set of characters.

Antwort: D

Begründung:
The delimiter method in the Field Extractor should be used when fields in events are separated consistently by a specific character (such as a comma, tab, or pipe). This method simplifies extraction without requiring complex regular expressions.
Reference:
Splunk Power User Study Guide, Field Extraction Section
Splunk Docs: Using the Field Extractor
"Use the delimiter extraction method when your data fields are consistently separated by a specific delimiter character."

96. Frage
There are several ways to access the field extractor. Which option automatically identifies data type, source type, and sample event?

- A. Settings > Field Extractions > New Field Extraction
- B. Event Actions > Extract Fields
- C. Fields sidebar > Extract New Field
- D. Settings > Field Extractions > Open Field Extraction

Antwort: C

Begründung:
There are several ways to access the field extractor. The option that automatically identifies data type, source type, and sample event is Fields sidebar > Extract New Field. The field extractor is a tool that helps you extract fields from your data using delimiters or regular expressions. The field extractor can generate a regex for you based on your selection of sample values or you can enter your own regex in the field extractor. The field extractor can be accessed by using various methods, such as:
Fields sidebar > Extract New Field: This is the easiest way to access the field extractor. The fields sidebar is a panel that shows all available fields for your data and their values. When you click on Extract New Field in the fields sidebar, Splunk will automatically identify the data type, source type, and sample event for your data based on your current search criteria. You can then use the field extractor to select sample values and generate a regex for your new field.

Event Actions > Extract Fields: This is another way to access the field extractor. Event actions are actions that you can perform on individual events in your search results, such as viewing event details, adding to report, adding to dashboard, etc. When you click on Extract Fields in the event actions menu, Splunk will use the current event as the sample event for your data and ask you to select the source type and data type for your data. You can then use the field extractor to select sample values and generate a regex for your new field.
Settings > Field Extractions > New Field Extraction: This is a more advanced way to access the field extractor. Settings is a menu that allows you to configure various aspects of Splunk, such as indexes, inputs, outputs, users, roles, apps, etc. When you click on New Field Extraction in the Settings menu, Splunk will ask you to enter all the details for your new field extraction manually, such as app context, name, source type, data type, sample event, regex, etc. You can then use the field extractor to verify or modify your regex for your new field.

97. Frage
.....

ZertSoft ist eine Website, die alle Informationen zur verschiedenen Splunk -Zertifizierungsprüfungen bieten kann. ZertSoft kann die besten und neuesten Prüfungsressourcen für Sie bereitstellen. Wenn Sie ZertSoft wählen, können Sie sich unbesorgt auf Ihre Splunk SPLK-1002 Zertifizierungsprüfung vorbereiten. Unsere Prüfungsunterlagen garantieren Ihnen, dass Sie 100% die Splunk SPLK-1002 Zertifizierungsprüfung bestehen können. Wenn nicht, geben wir Ihnen eine volle Rückerstattung oder akutualisieren schnell die Splunk SPLK-1002 Prüfungsfragen- und antworten. ZertSoft kann Ihnen Hilfe bei der Splunk SPLK-1002 Zertifizierungsprüfung sowie bei Ihrer zukünftigen Arbeit bieten. Zwar gibt es viele Möglichkeiten, die Ihnen zu Ihrem Ziel verhelfen, aber es ist die klügste Wahl, wenn Sie ZertSoft wählen. Mit ZertSoft können Sie mit wenigem Geld die Prüfung sicherer bestehen. Außerdem bieten wir Ihnen einjährigen kostenlosen Update-Service.

https://drive.google.com/open?id=1iOJau42tXr92XUA6HFTTsh9S6OmLuDPA