SPLK-1002 Lerntipps - SPLK-1002 Prüfungsfrage

Übrigens, Sie können die vollständige Version der ZertPruefung SPLK-1002 Prüfungsfragen aus dem Cloud-Speicher herunterladen: https://drive.google.com/open?id=1rAtacHQtKbqOAFkANep6rYwTWMS4CC63

Die Fragenkataloge von ZertPruefung enthalten die Lernmaterialien und Simulationsfragen zur Splunk SPLK-1002 Zertifizierungsprüfung. Noch wichtiger bieten wir die originalen SPLK-1002 Fragen Und Antworten.

Um die Splunk SPLK-1002-Prüfung zu bestehen, müssen Kandidaten ein tiefes Verständnis der Splunk-Plattform und ihrer verschiedenen Fähigkeiten demonstrieren. Die Prüfung besteht aus 65 Multiple-Choice- und Matching-Fragen, und die Kandidaten haben 90 Minuten Zeit, um sie zu absolvieren. Um die Prüfung zu bestehen, ist eine Punktzahl von mindestens 70% erforderlich, und erfolgreiche Kandidaten erhalten die Splunk Core Certified Power User-Zertifizierung. Diese Zertifizierung wird in der IT-Branche hoch angesehen und kann für Einzelpersonen, die ihre Karriere in IT-Operationen, Sicherheit oder Datenanalyse vorantreiben möchten, von großem Nutzen sein.

Die SPLK-1002 Prüfung ist für Power User gedacht, die ihre Expertise in der Verwendung von Splunk Core validieren möchten. Die Prüfung misst die Fähigkeit des Kandidaten, fortgeschrittene Suchtechniken durchzuführen, Dashboards zu erstellen und die Suchleistung zu optimieren. Die Prüfung ist im proctorierten Multiple-Choice-Format und Kandidaten haben 90 Minuten Zeit, um sie abzuschließen.

Die SPLK-1002-Zertifizierungsprüfung ist eine umfassende Prüfung, die eine breite Palette von Themen im Zusammenhang mit Splunk Core abdeckt. Die Prüfung testet das Wissen des Kandidaten über die Splunk Search Processing Language (SPL) sowie erweiterte Suchtechniken, Datenmodelle und Erstellen von Berichten und Dashboards. Darüber hinaus behandelt die Prüfung auch Themen wie Datennormalisierung, Fehlerbehebung und Benutzerverwaltung. Die Zertifizierung richtet sich an Fachleute, die ein tiefes Verständnis von Splunk Core haben und sie verwenden können, um komplexe Geschäftsprobleme zu lösen.

>> SPLK-1002 Lerntipps <<

Splunk SPLK-1002 Prüfungsfrage - SPLK-1002 Probesfragen

Viele Webseiten bieten Splunk SPLK-1002 Zertifizierungsunterlagen und andere Unterlagen. Aber wir ZertPruefung sind die einzige Website, die besten Splunk SPLK-1002 Zertifizierungsunterlagen zu bieten. Mit der Hilfe von ZertPruefung können Sie nur einmal Splunk SPLK-1002 Zertifizierungsprüfung zu bestehen. Die Splunk SPLK-1002 Prüfungsfragen und Testantworten von ZertPruefung sind von reichen Erfahrungen und Kenntnissen gesammelt. Diese bieten Ihnen eine gute Chance, in IT-Industrie zu entwickeln.

Splunk Core Certified Power User Exam SPLK-1002 Prüfungsfragen mit Lösungen (Q67-Q72):

67. Frage
What do events in a transaction have In common?

- A. All events in a transaction must have the same sourcetype.
- B. All events in a transaction must have the exact same set of fields.
- C. All events In a transaction must have the same timestamp.
- D. All events in a transaction must be related by one or more fields.

Antwort: A

68. Frage
Which of the following data models are included in the Splunk Common Information Model (CIM) add-on?
(select all that apply)

- A. User permissions
- B. Alerts
- C. Email
- D. Databases

Antwort: B,C

Begründung:
The Splunk Common Information Model (CIM) Add-on includes a variety of data models designed to normalize data from different sources to allow for cross-source reporting and analysis. Among the data models included, Alerts (Option B) and Email (Option D) are part of the CIM. The Alerts data model is used for data related to alerts and incidents, while the Email data model is used for data pertaining to email messages and transactions. User permissions (Option A) and Databases (Option C) are not data models included in the CIM; rather, they pertain to aspects of data access control and specific types of data sources, respectively, which are outside the scope of the CIM's predefined data models.

69. Frage
Which of the following transforming commands can be used with transactions?

- A. chart, timecha:t, stats, pivot
- B. chart, timeehart, datamodel, pivot
- C. chart, timechart, stats, eventstats
- D. chart, timechart, stats, diff

Antwort: C

Begründung:
Transforming commands are commands that change the format of the search results into a table or a chart. They can be used to perform statistical calculations, create visualizations, or manipulate data in various ways1.
Transactions are groups of events that share some common values and are related in some way. Transactions can be defined by

using the transaction command or by creating a transaction type in the transactiontypes.conf file2.
Some transforming commands can be used with transactions to create tables or charts based on the transaction fields. These commands include:
chart: This command creates a table or a chart that shows the relationship between two or more fields. It can be used to aggregate values, count occurrences, or calculate statistics3.
timechart: This command creates a table or a chart that shows how a field changes over time. It can be used to plot trends, patterns, or outliers4.
stats: This command calculates summary statistics on the fields in the search results, such as count, sum, average, etc. It can be used to group and aggregate data by one or more fields5.
eventstats: This command calculates summary statistics on the fields in the search results, similar to stats, but it also adds the results to each event as new fields. It can be used to compare events with the overall statistics.
These commands can be applied to transactions by using the transaction fields as arguments. For example, if you have a transaction type named "login" that groups events based on the user field and has fields such as duration and eventcount, you can use the following commands with transactions:
| chart count by user : This command creates a table or a chart that shows how many transactions each user has.
| timechart span=1h avg(duration) by user : This command creates a table or a chart that shows the average duration of transactions for each user per hour.
| stats sum(eventcount) as total_events by user : This command creates a table that shows the total number of events for each user across all transactions.
| eventstats avg(duration) as avg_duration : This command adds a new field named avg_duration to each transaction that shows the average duration of all transactions.
The other options are not valid because they include commands that are not transforming commands or cannot be used with transactions. These commands are:
diff: This command compares two search results and shows the differences between them. It is not a transforming command and it does not work with transactions.
datamodel: This command retrieves data from a data model, which is a way to organize and categorize data in Splunk. It is not a transforming command and it does not work with transactions.
pivot: This command creates a pivot report, which is a way to analyze data from a data model using a graphical interface. It is not a transforming command and it does not work with transactions.
Explanation:
The correct answer is
Reference:
About transforming commands
About transactions
chart command overview
timechart command overview
stats command overview
[eventstats command overview]
[diff command overview]
[datamodel command overview]
[pivot command overview]

70. Frage
Highlighted search terms indicate _____ search results in Splunk.

- A. Display as selected fields.
- B. Matching
- C. Charted based on time
- D. Sorted

Antwort: B

Begründung:
Explanation
Highlighted search terms indicate matching search results in Splunk, which means that they show which parts of your events match your search string2. For example, if you search for error OR fail, Splunk will highlight error or fail in your events to show which events match your search string2. Therefore, option D is correct, while options A, B and C are incorrect because they are not indicated by highlighted search terms.

71. Frage
The Field Extractor (FX) is used to extract a custom field. A report can be created using this custom field. The created report can then be shared with other people in the organization. If another person in the organization runs the shared report and no results are returned, why might this be? (select all that apply)

- A. The person in the organization running the report does not have access to the index.
- B. The extraction is private-
- C. Fast mode is enabled.
- D. The dashboard is private.

Antwort: A,B

Begründung:
The Field Extractor (FX) is a tool that helps you extract fields from your events using a graphical interface2. You can create a report using a custom field extracted by the FX and share it with other users in your organization2. However, if another user runs the shared report and no results are returned, there could be two possible reasons. One reason is that the extraction is private, which means that only you can see and use the extracted field2. To make the extraction available to other users, you need to make it global or app-level2. Therefore, option C is correct. Another reason is that the other user does not have access to the index where the events are stored2. To fix this issue, you need to grant the appropriate permissions to the other user for the index2. Therefore, option D is correct. Options A and B are incorrect because they are not related to the field extraction or the report.

72. Frage
.....

- Das neueste SPLK-1002, nützliche und praktische SPLK-1002 pass4sure Trainingsmaterial □ Suchen Sie jetzt auf ➤ www.pass4test.de □ nach 【 SPLK-1002 】 um den kostenlosen Download zu erhalten □SPLK-1002 Online Prüfung
- wanderlog.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.4shared.com, 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, demo.emshost.com, Disposable vapes

Übrigens, Sie können die vollständige Version der ZertPruefung SPLK-1002 Prüfungsfragen aus dem Cloud-Speicher herunterladen: https://drive.google.com/open?id=1rAtacHQtKbqOAFkANep6rYwTWMS4CC63