The Best Splunk SPLK-1002 Study Guides and Dumps of 2022 [Q23-Q44

The Best Splunk SPLK-1002 Study Guides and Dumps of 2022 Top Splunk SPLK-1002 Exam Audio Study Guide! Practice Questions Edition

Difficulty in writing splk-1002 Exam

Many candidates appear to take the Splunk Core Certified Power User Exam but could not manage to pass in their first attempt. There could be many reasons behind the failure of the candidates who try to take the Splunk splk-1002 exam, such as the lack of study material or lack of practice, etc. But the most important factor that causes the failure of the candidates is that they don't use the proper learning material. To pass the splk-1002 exam, you should use a reliable preparation source that contains complete information about the splk-1002 exam.

Splunk Core Certified Power User is the most powerful certification that candidates can have on their resume. But for this, they will have to pass splk-1002 questions. splk-1002 is a challenging exam to pass this exam Candidates will have to work hard with the help of the right focus and preparation material passing this exam is an achievable goal. ExamsLabs help candidates by providing the most relevant and updated splk-1002 exam dumps. Furthermore, We also provide the splk-1002 practice test that will be much beneficial in the preparation. ExamsLabs aims to provide the best splk-1002 exam dumps that are verified by the Splunk experts. If Candidates feel any doubt in the splk-1002 practice test then our team is always there to help them. **splk-1002 exam dumps** are the perfect way to prepare splk-1002 exam with good grades in the just first attempt. So, Candidates want instant success in the splk-1002 exam with quality splk-1002 training material then ExamsLabs is the best option for them because our management is well trained in it and we update each question of all exams on regular basis after consulting recent updates with our Splunk certified professionals.

Who should take the splk-1002 exam

The Splunk Core Certified Power User **splk-1002 Exam** certification is an internationally-recognized validation that identifies persons who earn it as possessing skilled as Splunk Core Certified Power Users.

NEW QUESTION 23

Which of the following is the correct way to use the data model command to search field in the data model within the web dataset?
* | datamodel web search | filed web *
* | Search datamodel web web | filed web*
* | datamodel web web field | search web*
* Datamodel=web | search web | filed web*

NEW QUESTION 24

Which one of the following statements about the search command is true?
* It does not allow the use of wildcards.
* It treats field values in a case-sensitive manner.
* It can only be used at the beginning of the search pipeline.
* It behaves exactly like search strings before the first pipe.

NEW QUESTION 25

Which one of the following statements about the search command is true?
* It does not allow the use of wildcards.
* It treats field values in a case-sensitive manner.
* It can only be used at the beginning of the search pipeline.
* It behaves exactly like search strings before the first pipe.

NEW QUESTION 26

Which of the following statements about data models and pivot are true? (select all that apply)
* They are both knowledge objects.
* Data models are created out of datasets called pivots.
* Pivot requires users to input SPL searches on data models.
* Pivot allows the creation of data visualizations that present different aspects of a data model.

NEW QUESTION 27

Which of the following statements describe the Common Information Model (CIM)? (select all that apply)
* CIM is a methodology for normalizing data.
* CIM can correlate data from different sources.
* The Knowledge Manager uses the CIM to create knowledge objects.
* CIM is an app that can coexist with other apps on a single Splunk deployment.

NEW QUESTION 28

Data model fields can be added using the Auto-Extracted method. Which of the following statements describe Auto-Extracted

fields? (select all that apply)
* Auto-Extracted fields can be hidden in Pivot.
* Auto-Extracted fields can have their data type changed.
* Auto-Extracted fields can be given a friendly name for use in Pivot.
* Auto-Extracted fields can be added if they already exist in the dataset with constraints.

NEW QUESTION 29

When can a pipe follow a macro?
* A pipe may always follow a macro.
* The current user must own the macro.
* The macro must be defined in the current app.
* Only when sharing is set to global for the macro.

NEW QUESTION 30

When should transaction be used?
* Only in a large distributed Splunk environment.
* When calculating results from one or more fields.
* When event grouping is based on start/end values.
* When grouping events results in over 1000 events in each group.
Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Search/Abouttransactions

NEW QUESTION 31

What is the correct syntax to search for a tag associated with a value on a specific fiedsd?
* Tag-<field?
* Tag<filed(tagname.)
* Tag=<filed>::<tagname>
* Tag::<filed>=<tagname>

NEW QUESTION 32

Which search would limit an &#8220;alert&#8221; tag to the &#8220;host&#8221; field?
* tag=alert
* host::tag::alert
* tag==alert
* tag::host=alert

NEW QUESTION 33

When using the transactioncommand, what does the argument maxspando?
* Sets the maximum total time between events in a transaction.
* Sets the maximum length of all the events within a transaction.
* Sets the maximum total time between the earliest and latest events in a transaction.
* Sets the maximum length that any single event can reach to be included in the transaction.
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/SearchReference/Transaction

NEW QUESTION 34

After you create a pivot you can save it as a ___________. (Select all that apply.)
* tag
* eventtype
* report
* dashboard panel

NEW QUESTION 35

Which of the following Statements about macros is true? (select all that apply)
* Arguments are defined at execution time.
* Arguments are defined when the macro is created.
* Argument values are used to resolve the search string at execution time.
* Argument values are used to resolve the search string when the macro is created.

NEW QUESTION 36

A data model consists of which three types of datasets?
* Constraint, field, value.
* Events, searches, transactions.
* Field extraction, regex, delimited.
* Transaction, session ID, metadata.
The building block of a data model. Each data model is composed of one or more data model datasets. Each dataset within a data model defines a subset of the dataset represented by the data model as a whole.

Data model datasets have a hierarchical relationship with each other, meaning they have parent-child relationships. Data models can contain multiple dataset hierarchies. There are three types of dataset hierarchies: event, search, and transaction.

https://docs.splunk.com/Splexicon:Datamodeldataset

NEW QUESTION 37

Which of the following searches show a valid use of macro? (Select all that apply)
* index=main source=mySource oldField=* |&#8217;makeMyField(oldField)&#8217;| table _time newField
* index=main source=mySource oldField=* | stats if(&#8216;makeMyField(oldField)&#8217;) | table _time newField
* index=main source=mySource oldField=* | eval newField=&#8217;makeMyField(oldField)&#8217;| table _time newField
* index=main source=mySource oldField=* | &#8220;&#8216;newField(&#8216;makeMyField(oldField)&#8217;)'&#8221; | table _time newField
Reference:

https://answers.splunk.com/answers/574643/field-showing-an-additional-and-not-visible-value-1.html

NEW QUESTION 38

Which of the following can be used with the eval command tostring function (select all that apply)
* &#8221;hex&#8221;
* &#8221;commas&#8221;
* &#8221;Decimal&#8221;
* &#8221;duration&#8221;

Explanation

https://docs.splunk.com/Documentation/Splunk/8.1.0/SearchReference/ConversionFunctions#tostring.28X.2CY.

NEW QUESTION 39

What do events in a transaction have In common?
- All events In a transaction must have the same timestamp.
- All events in a transaction must have the same sourcetype.
- All events in a transaction must have the exact same set of fields.
- All events in a transaction must be related by one or more fields.

NEW QUESTION 40

Data model fields can be added using the Auto-Extracted method. Which of the following statements describe Auto-Extracted fields? (select all that apply)
- Auto-Extracted fields can be hidden in Pivot.
- Auto-Extracted fields can have their data type changed.
- Auto-Extracted fields can be given a friendly name for use in Pivot.
- Auto-Extracted fields can be added if they already exist in the dataset with constraints.

NEW QUESTION 41

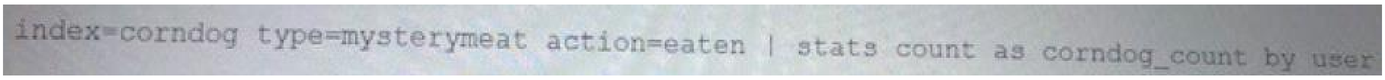
This function of the stats command allows you to return the middle-most value of field X.
- Median(X)
- Eval by X
- Fields(X)
- Values(X)

NEW QUESTION 42

Which of the following statements describe calculated fields? (select all that apply)
- Calculated fields can be used in the search bar.
- Calculated fields can be based on an extracted field.
- Calculated fields can only be applied to host and sourcetype.
- Calculated fields are shortcuts for performing calculations using the eval command.

NEW QUESTION 43

What does the following search do?



```
index=corndog type=mysterymeat action=eaten | stats count as corndog_count by user
```

- Creates a table of

the total count of users and split by corndogs. * Creates a table of the total count of mystery

The Bes

meat corndogs split by user.
* Creates a table with the count of all types of corndogs eaten

The Bes

split by user. * Creates a table that groups the total number of users by vegetarian corndog

The Bes

s.

NEW QUESTION 44

When using timechart, how many fields can be listed after a by clause?

* because timechart doesn&#8217;t support using a by clause.
* because _time is already implied as the x-axis.
* because one field would represent the x-axis and the other would represent the y-axis.
* There is no limit specific to timechart.

Exam Details **SPLK-1002 has 65 multiple-select and multiple-choice questions that should be answered in 57 minutes, with an addition of 3 minutes that are given one to get familiar with the exam agreement. Taking this test will cost $ The applicants will be rated on a variety of knowledge areas, such as the following:** - Macros- Tags as well as event types- Data models- Knowledge objects- Correlating events- Transformation of commands as well as visualizations- Filtering as well as formatting of results

Candidates are advised to take the training courses provided by the vendor when preparing for SPLK-1002 exam. To succeed on the first attempt, they should tackle all the lectures, hands-on sessions, and practice questions to ensure they are adequately ready.

Valid SPLK-1002 Exam Updates - 2022 Study Guide:
https://www.examslabs.com/Splunk/Splunk-Core-Certified-Power-User/best-SPLK-1002-exam-dumps.html]