SPLK-1002 Q&As

Splunk Core Certified Power User

Pass Splunk SPLK-1002 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/splk-1002.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

When performing a regex field extraction with the Field Extractor (FX), a data type must be chosen before a sample event can be selected. Which of the following data types are supported?

A. index or source

B. sourcetype or host

C. index or sourcetype

D. sourcetype or source

Correct Answer: D

When using the Field Extractor (FX) in Splunk for regex field extraction, it\\'s important to select the context in which you want to perform the extraction. The context is essentially the subset of data you\\'re focusing on for your field extraction task. D. Sourcetype or source: This is the correct option. In the initial steps of using the Field Extractor tool, you\\'re prompted to choose a data type for your field extraction. The options available are typically based on the nature of your data and how it\\'s organized in Splunk. "Sourcetype" refers to the kind of data you\\'re dealing with, a categorization that helps Splunk apply specific processing rules. "Source" refers to the origin of the data, like a specific log file or data input. By selecting either a sourcetype or source, you\\'re narrowing down the dataset on which you\\'ll perform the regex extraction, making it more manageable and relevant.

QUESTION 2

By default, how is acceleration configured in the Splunk Common Information Model (CIM) add-on?

A. Turned off

B. Turned on

C. Determined automatically based on the sourcetype.

D. Determined automatically based on the data source.

Correct Answer: D

By default, acceleration is determined automatically based on the data source in the Splunk Common Information Model (CIM) add-on. The Splunk CIM Add-on is an app that provides common data models for various domains, such as network traffic, web activity, authentication, etc. The CIM Add-on allows you to normalize and enrich your data using predefined fields and tags. The CIM Add-on also allows you to accelerate your data models for faster searches and reports. Acceleration is a feature that pre-computes summary data for your data models and stores them in tsidx files. Acceleration can improve the performance and efficiency of your searches and reports that use data models. By default, acceleration is determined automatically based on the data source in the CIM Add-on. This means that Splunk will decide whether to enable or disable acceleration for each data model based on some factors, such as data volume, data type, data model complexity, etc. However, you can also manually enable or disable acceleration for each data model by using the Settings menu or by editing the datamodels.conf file.

QUESTION 3

Which of the following statements are true for this search? (Select all that apply.) SEARCH: sourcetype=access* |fields action productId status

A. is looking for all events that include the search terms: fields AND action AND productId AND status

B. users the table command to improve performance

C. limits the fields are extracted

D. returns a table with 3 columns

Correct Answer: C

QUESTION 4

Calculated fields can be based on which of the following?

A. Tags

B. Extracted fields

C. Output fields for a lookup

D. Fields generated from a search string

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/definecalcfields

A calculated field is a field that you create based on the value of another field or fields1. You can use calculated fields to enrich your data with additional information or to transform your data into a more useful format1. Calculated fields can be based on extracted fields, which are fields that are extracted from your raw data using various methods such as regular expressions, delimiters, or key-value pairs1. Therefore, option B is correct, while options A, C and D are incorrect because tags, output fields for a lookup, and fields generated from a search string are not types of extracted fields.

QUESTION 5

Which search would limit an "alert" tag to the "host" field?

A. tag=alert

B. host::tag::alert

C. tag==alert

D. tag::host=alert

Correct Answer: D

The search below would limit an "alert" tag to the "host" field.

tag::host=alert

The search does the following:

It uses tag syntax to filter events by tags. Tags are custom labels that can be applied to fields or field values to provide additional context or meaning for your data. It specifies tag::host=alert as the tag filter. This means that it will only return

events that have an "alert" tag applied to their host field or host field value. It uses an equal sign (=) to indicate an exact match between the tag and the field or field value.

QUESTION 6

Which of the following searches will return events contains a tag name Privileged?

A. Tag= Priv

B. Tag= Pri*

C. Tag= Priv*

D. Tag= Privileged

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/PCI/4.1.0/Install/PrivilegedUserActivity A tag is a descriptive label that you can apply to one or more fields or field values in your events1. You can use tags to simplify your searches by replacing long or complex field names or values with short and simple tags1. To search for events that contain a tag name, you can use the tag keyword followed by an equal sign and the tag name1. You can also use wildcards (*) to match partial tag names1. Therefore, option B is correct because it will return events that contain a tag name that starts with Pri. Options A and D are incorrect because they will only return events that contain an exact tag name match. Option C is incorrect because it will return events that contain a tag name that starts with Priv, not Privileged.

QUESTION 7

In what order arc the following knowledge objects/configurations applied?

A. Field Aliases, Field Extractions, Lookups

B. Field Extractions, Field Aliases, Lookups

C. Field Extractions, Lookups, Field Aliases

D. Lookups, Field Aliases, Field Extractions

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/WhatisSplunkknowledge

Knowledge objects are entities that you create to add knowledge to your data and make it easier to search and analyze2. Some examples of knowledge objects are field extractions, field aliases and lookups2. Field extractions are methods that extract fields from your raw data using various techniques such as regular expressions, delimiters or key-value pairs2. Field aliases are ways to assign alternative names to existing fields without changing the original field names or values2. Lookups are ways to enrich your data with additional information from external sources such as CSV files or databases2. The order in which these knowledge objects/configurations are applied is as follows: field extractions, field aliases and then lookups2. This means that Splunk first extracts fields from your raw data, then applies

any aliases to the extracted fields and then performs any lookups on the aliased fields2. Therefore, option B is correct, while options A, C and D are incorrect.

QUESTION 8

Selected fields are displayed _____each event in the search results.

A. below

B. interesting fields

C. other fields

D. above

Correct Answer: A

Selected fields are fields that you choose to display in your search results by clicking on them in the Fields sidebar or by using the fields command2. Selected fields are displayed below each event in the search results, along with their values2. Therefore, option A is correct, while options B, C and D are incorrect because they are not places where selected fields are displayed.

QUESTION 9

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

A. because timechart doesn\\'t support using a by clause.

B. because _time is already implied as the x-axis.

C. because one field would represent the x-axis and the other would represent the y-axis.

D. There is no limit specific to timechart.

Correct Answer: B

The timechart command is used to create a time-series chart of statistical values based on your search results2. You can use the timechart command with a by clause to split the results by one or more fields and create multiple series in the chart2. However, you can only list one field after the by clause when using the timechart command because _time is already implied as the x-axis of the chart2. Therefore, option B is correct, while options A, C and D are incorrect.

QUESTION 10

A user wants to convert numeric field values to strings and also to sort on those values.

Which command should be used first, the eval or the sort?

A. It doesn\\'t matter whether eval or sort is used first.

B. Convert the numeric to a string with eval first, then sort.

C. Use sort first, then convert the numeric to a string with eval.

D. You cannot use the sort command and the eval command on the same field.

Correct Answer: C

The eval command is used to create new fields or modify existing fields based on an expression2. The sort command is used to sort the results by one or more fields in ascending or descending order2. If you want to convert numeric field values to strings and also sort on those values, you should use the sort command first, then use the eval command to convert the values to strings2. This way, the sort command will use the original numeric values for sorting, rather than the converted string values which may not sort correctly. Therefore, option C is correct, while options A, B and D are incorrect.

QUESTION 11

What do events in a transaction have In common?

A. All events In a transaction must have the same timestamp.

B. All events in a transaction must have the same sourcetype.

C. All events in a transaction must have the exact same set of fields.

D. All events in a transaction must be related by one or more fields.

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Abouttransactions

A transaction is a group of events that share some common characteristics, such as fields, time, or both. A transaction can be created by using the transaction command or by defining an event type with transactiontype=true in props.conf. Events in a transaction have one or more fields in common that relate them to each other. For example, you can create a transaction based on JSESSIONID, which is a unique identifier for each user session in web logs. Events in a transaction do not have to have the same timestamp, sourcetype, or exact same set of fields. They only have to share one or more fields that define the transaction.

QUESTION 12

What is the purpose of the fillnull command?

A. Replace empty values with a specified value.

B. Create a new field based on the values in an existing field.

C. Rename a specific field in the search results.

D. Replace all values in a specific field with a default value.

Correct Answer: A

The fillnull command in Splunk is used to handle missing data within search results. It plays a crucial role in data normalization and preparation, especially before performing statistical analyses or visualizations. A. Replace empty values with a specified value: This is the correct answer. The fillnull command is specifically designed to replace null

values (empty values) with a specified default value. This is particularly useful in ensuring consistency within your data, especially when performing operations that require numerical values or when you want to distinguish between genuinely missing data and zeroes, for instance. Example Usage: ... | fillnull value=0 This command would replace all null values in the search results with 0.

QUESTION 13

Which of the following statements about data models and pivot are true? (select all that apply)

A. They are both knowledge objects.

B. Data models are created out of datasets called pivots.

C. Pivot requires users to input SPL searches on data models.

D. Pivot allows the creation of data visualizations that present different aspects of a data model.

Correct Answer: D

Data models and pivot are both knowledge objects in Splunk that allow you to analyze and visualize your data in different ways. Data models are collections of datasets that represent your data in a structured and hierarchical way. Data models define how your data is organized into objects and fields. Pivot is a user interface that allows you to create data visualizations that present different aspects of a data model. Pivot does not require users to input SPL searches on data models, but rather lets them select options from menus and forms. Data models are not created out of datasets called pivots, but rather pivots are created from datasets in data models.

QUESTION 14

Which of the following statements describe the search below? (select all that apply) Index=main I transaction clientip host maxspan=30s maxpause=5s

A. Events in the transaction occurred within 5 seconds.

B. It groups events that share the same clientip and host.

C. The first and last events are no more than 5 seconds apart.

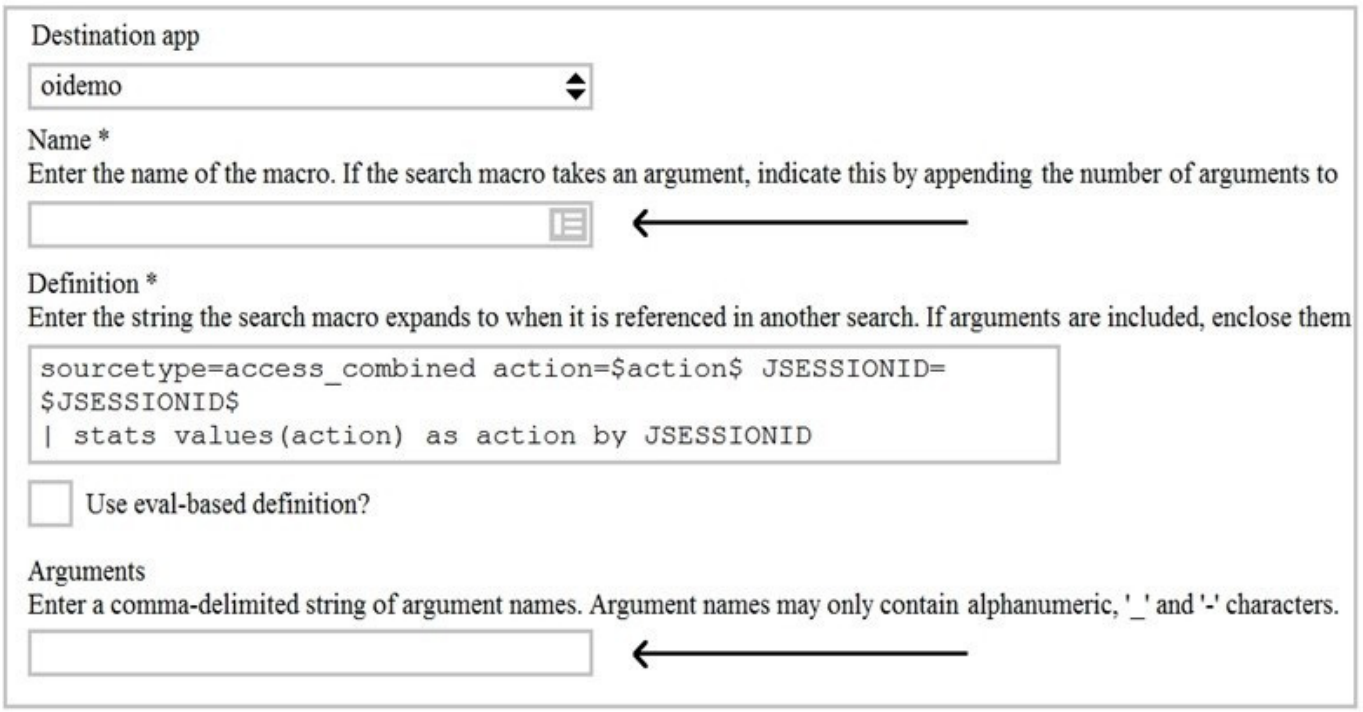
D. The first and last events are no more than 30 seconds apart.

Correct Answer: ABD

The search below groups events by two or more fields (clientip and host), creates transactions with start and end constraints (maxspan=30s and maxpause=5s), and calculates the duration of each transaction. index=main | transaction clientip host maxspan=30s maxpause=5s The search does the following: It filters the events by the index main, which is a default index in Splunk that contains all data that is not sent to other indexes. It uses the transaction command to group events into transactions based on two fields: clientip and host. The transaction command creates new events from groups of events that share the same clientip and host values. It specifies the start and end constraints for the transactions using the maxspan and maxpause arguments. The maxspan argument sets the maximum time span between the first and last events in a transaction. The maxpause argument sets the maximum time span between any two consecutive events in a transaction. In this case, the maxspan is 30 seconds and the maxpause is 5 seconds, meaning that any transaction that has a longer time span or pause will be split into multiple transactions. It creates some additional fields for each transaction, such as duration, eventcount, startime, etc. The duration field shows the time span between the first and last events in a transaction.

QUESTION 15

Given the macro definition below, what should be entered into the Name and Arguments fileds to correctly configured the macro?



A. The macro name is sessiontracker and the arguments are action, JESSIONID.

B. The macro name is sessiontracker(2) and the arguments are action, JESSIONID.

C. The macro name is sessiontracker and the arguments are $action$, $JESSIONID$.

D. The macro name is sessiontracker(2) and the Arguments are $action$, $JESSIONID$.

Correct Answer: B

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Definesearchmacros

The macro definition below shows a macro that tracks user sessions based on two arguments: action and JSESSIONID.

sessiontracker(2)

The macro definition does the following:

It specifies the name of the macro as sessiontracker. This is the name that will be used to execute the macro in a search string. It specifies the number of arguments for the macro as 2. This indicates that the macro takes two arguments when

it is executed.

It specifies the code for the macro as index=main sourcetype=access_combined_wcookie action=$action$ JSESSIONID=$JSESSIONID$ | stats count by JSESSIONID. This is the search string that will be run when the macro is executed. The search string can contain any part of a search, such as search terms, commands, arguments, etc. The search string can also include variables for the arguments using dollar signs around them. In this case, action and JSESSIONID are variables for the arguments that will be replaced by their values when the macro is executed.

Therefore, to correctly configure the macro, you should enter sessiontracker as the name and action, JSESSIONID as the arguments. Alternatively, you can use sessiontracker(2) as the name and leave the arguments blank.