Vendor: Splunk

Exam Code: SPLK-1002

Exam Name: Splunk Core Certified Power User

Version: DEMO

QUESTION 1
When performing a regular expression (regex) field extraction using the Field Extractor (FX), what happens when the require option is used?

A. The regex can no longer be edited.
B. The field being extracted will be required for all future events.
C. The events without the required field will not display in searches.
D. Only events with the required string will be included in the extraction.

Answer: D
Explanation:
The Field Extractor (FX) allows you to use regular expressions (regex) to extract fields from your events using a graphical interface or by manually editing the regex. When you use the FX to perform a regex field extraction, you can use the require option to specify a string that must be present in an event for it to be included in the extraction. This way, you can filter out events that do not contain the required string and focus on the events that are relevant for your extraction.

QUESTION 2
Which group of users would most likely use pivots?

A. Users
B. Architects
C. Administrators
D. Knowledge Managers

Answer: A
Explanation:
A pivot is a tool that allows you to create reports and dashboards using data models without writing any SPL commands. You can use pivots to explore, filter, split and visualize your data using a graphical interface. Pivots are designed for users who want to analyze and report on their data without having to learn the SPL syntax or the underlying structure of the data. Therefore, option A is correct, while options B, C and D are incorrect because they are not the typical group of users who would use pivots.

QUESTION 3
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.

Answer: B
Explanation:
The timechart command is used to create a time-series chart of statistical values based on your search results. 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 chart. 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 chart.

QUESTION 4

What is the correct syntax to search for a tag associated with a value on a specific fields?

A. Tag-<field?
B. Tag<filed(tagname.)
C. Tag=<filed>::<tagname>
D. Tag::<filed>=<tagname>

Answer: D
Explanation:
A tag is a descriptive label that you can apply to one or more fields or field values in your events. You can use tags to simplify your searches by replacing long or complex field names or values with short and simple tags. To search for a tag associated with a value on a specific field, you can use the following syntax: tag::<field>=<tagname>. For example, tag::status=error will search for events where the status field has a tag named error. Therefore, option D is correct, while options A, B and C are incorrect because they do not follow the correct syntax for searching tags.

QUESTION 5
What functionality does the Splunk Common Information Model (CIM) rely on to normalize fields with different names?

A. Macros.
B. Field aliases.
C. The rename command.
D. CIM does not work with different names for the same field.

Answer: B
Explanation:
The Splunk Common Information Model (CIM) add-on helps you normalize your data from different sources and make it easier to analyze and report on it. One of the functionalities that the CIM add- on relies on to normalize fields with different names is field aliases. Field aliases allow you to assign an alternative name to an existing field without changing the original field name or value. By using field aliases, you can map different field names from different sources or sourcetypes to a common field name that conforms to the CIM standard. Therefore, option B is correct, while options A, C and D are incorrect.

QUESTION 6
When should you use the transaction command instead of the scats command?

A. When you need to group on multiple values.
B. When duration is irrelevant in search results. .
C. When you have over 1000 events in a transaction.
D. When you need to group based on start and end constraints.

Answer: D
Explanation:
The transaction command is used to group events into transactions based on some common characteristics, such as fields, time, or both. The transaction command can also specify start and end constraints for the transactions, such as a field value that indicates the beginning or the end of a transaction. The stats command is used to calculate summary statistics on the events, such as count, sum, average, etc. The stats command cannot group events based on start and end constraints, but only on fields or time buckets. Therefore, the transaction command should be used instead of the stats command when you need to group events based on start and end

constraints.

QUESTION 7
Which of the following statements describes field aliases?

A. Field alias names replace the original field name.
B. Field aliases can be used in lookup file definitions.
C. Field aliases only normalize data across sources and sourcetypes.
D. Field alias names are not case sensitive when used as part of a search.

Answer: B
Explanation:
Field aliases are alternative names for fields in Splunk. Field aliases can be used to normalize data across different sources and sourcetypes that have different field names for the same concept. For example, you can create a field alias for src_ip that maps to clientip, source_address, or any other field name that represents the source IP address in different sourcetypes. Field aliases can also be used in lookup file definitions to map fields in your data to fields in the lookup file. For example, you can use a field alias for src_ip to map it to ip_address in a lookup file that contains geolocation information for IP addresses. Field alias names do not replace the original field name, but rather create a copy of the field with a different name. Field alias names are case sensitive when used as part of a search, meaning that src_ip and SRC_IP are different fields.

QUESTION 8
What does the following search do?

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

A. Creates a table of the total count of users and split by corndogs.
B. Creates a table of the total count of mysterymeat corndogs split by user.
C. Creates a table with the count of all types of corndogs eaten split by user.
D. Creates a table that groups the total number of users by vegetarian corndogs.

Answer: B
Explanation:
The search string below creates a table of the total count of mysterymeat corndogs split by user.
| stats count by user | where corndog=mysterymeat

The search string does the following:
It uses the stats command to calculate the count of events for each value of the user field.
The stats command creates a table with two columns: user and count. It uses the where command to filter the results by the value of the corndog field. The where command only keeps the rows where corndog equals mysterymeat.
Therefore, the search string creates a table of the total count of mysterymeat corndogs split by user.

QUESTION 9
Which of the following statements describes Search workflow actions?

A. By default. Search workflow actions will run as a real-time search.

B. Search workflow actions can be configured as scheduled searches,
C. The user can define the time range of the search when created the workflow action.
D. Search workflow actions cannot be configured with a search string that includes the transaction command

Answer: C
Explanation:
Search workflow actions are custom actions that run a search when you click on a field value in your search results. Search workflow actions can be configured with various options, such as label name, search string, time range, app context, etc. One of the options is to define the time range of the search when creating the workflow action. You can choose from predefined time ranges, such as Last 24 hours, Last 7 days, etc., or specify a custom time range using relative or absolute time modifiers. Search workflow actions do not run as real-time searches by default, but rather use the same time range as the original search unless specified otherwise. Search workflow actions cannot be configured as scheduled searches, as they are only triggered by user interaction. Search workflow actions can be configured with any valid search string that includes any search command, such as transaction.

QUESTION 10
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.

Answer: D
Explanation:
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 11
Which of the following statements describe GET workflow actions?

A. GET workflow actions must be configured with POST arguments.
B. Configuration of GET workflow actions includes choosing a sourcetype.
C. Label names for GET workflow actions must include a field name surrounded by dollar signs.
D. GET workflow actions can be configured to open the URT link in the current window or in a new window

Answer: D
Explanation:
GET workflow actions are custom actions that open a URL link when you click on a field value in your search results. GET workflow actions can be configured with various options, such as label name, base URL, URI parameters, app context, etc. One of the options is to choose whether to open the URL link in the current window or in a new window. GET workflow actions do not have to be configured with POST arguments, as they use GET method to send requests to web

servers. Configuration of GET workflow actions does not include choosing a sourcetype, as they do not generate any data in Splunk. Label names for GET workflow actions must include a field name surrounded by dollar signs, as this indicates the field value that will be used to replace the variable in the URL link.

QUESTION 12
Data model are composed of one or more of which of the following datasets? (select all that apply.)

A. Events datasets
B. Search datasets
C. Transaction datasets
D. Any child of event, transaction, and search datasets

Answer: ABC
Explanation:
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. Data models can be composed of one or more of the following datasets:
Events datasets: These are the base datasets that represent raw events in Splunk. Events datasets can be filtered by constraints, such as search terms, sourcetypes, indexes, etc.
Search datasets: These are derived datasets that represent the results of a search on events or other datasets. Search datasets can use any search command, such as stats, eval, rex, etc., to transform the data.
Transaction datasets: These are derived datasets that represent groups of events that are related by fields, time, or both. Transaction datasets can use the transaction command or event types with transactiontype=true to create transactions.

QUESTION 13
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

Answer: B
Explanation:
Knowledge objects are entities that you create to add knowledge to your data and make it easier to search and analyze. Some examples of knowledge objects are field extractions, field aliases and lookups. Field extractions are methods that extract fields from your raw data using various techniques such as regular expressions, delimiters or key-value pairs. Field aliases are ways to assign alternative names to existing fields without changing the original field names or values. Lookups are ways to enrich your data with additional information from external sources such as CSV files or databases. The order in which these knowledge objects/configurations are applied is as follows: field extractions, field aliases and then lookups. 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 fields. Therefore, option B is correct, while options A, C and D are incorrect.

QUESTION 14
Which of the following knowledge objects represents the output of an eval expression?

A. Eval fields
B. Calculated fields
C. Field extractions
D. Calculated lookups

Answer: B
Explanation:
The eval command is used to create new fields or modify existing fields based on an expression. The output of an eval expression is a calculated field, which is a field that you create based on the value of another field or fields. You can use calculated fields to enrich your data with additional information or to transform your data into a more useful format. Therefore, option B is correct, while options A, C and D are incorrect because they are not names of knowledge objects that represent the output of an eval expression.

QUESTION 15
A calculated field maybe based on which of the following?

A. Lookup tables
B. Extracted fields
C. Regular expressions
D. Fields generated within a search string

Answer: B
Explanation:
As mentioned before, a calculated field is a field that you create based on the value of another field or fields. A calculated field 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 pairs. Therefore, option B is correct, while options A, C and D are incorrect because they are not types of fields that a calculated field can be based on.

QUESTION 16
Which of the following eval command function is valid?

A. Int ()
B. Count ( )
C. Print ()
D. Tostring ()

Answer: D
Explanation:
The eval command supports a number of functions that you can use in your expressions to perform calculations, conversions, string manipulations and more. One of the eval command functions is tostring(), which converts a numeric value to a string value. Therefore, option D is correct, while options A, B and C are incorrect because they are not valid eval command functions.

QUESTION 17
Which one of the following statements about the search command is true?

A. It does not allow the use of wildcards.

B. It treats field values in a case-sensitive manner.
C. It can only be used at the beginning of the search pipeline.
D. It behaves exactly like search strings before the first pipe.

Answer: D
Explanation:
The search command is used to filter or refine your search results based on a search string that matches the events. The search command behaves exactly like search strings before the first pipe, which means that you can use the same syntax and operators as you would use in the initial part of your search. Therefore, option D is correct, while options A, B and C are incorrect because they are not true statements about the search command.

QUESTION 18
What does the Splunk Common Information Model (CIM) add-on include? (select all that apply)

A. Custom visualizations
B. Pre-configured data models
C. Fields and event category tags
D. Automatic data model acceleration

Answer: BC
Explanation:
The Splunk Common Information Model (CIM) add-on is a collection of pre-built data models and knowledge objects that help you normalize your data from different sources and make it easier to analyze and report on it. The CIM add-on includes pre-configured data models that cover various domains such as Alerts, Email, Database, Network Traffic, Web and more. Therefore, option B is correct. The CIM add-on also includes fields and event category tags that define the common attributes and labels for the data models. Therefore, option C is correct. The CIM add-on does not include custom visualizations or automatic data model acceleration. Therefore, options A and D are incorrect.

QUESTION 19
Which of the following file formats can be extracted using a delimiter field extraction?

A. CSV
B. PDF
C. XML
D. JSON

Answer: A
Explanation:
A delimiter field extraction is a method of extracting fields from data that uses a character or a string to separate fields in each event. A delimiter field extraction can be performed by using the Field Extractor (FX) tool or by editing the props.conf file. A delimiter field extraction can be applied to any file format that uses a delimiter to separate fields, such as CSV, TSV, PSV, etc. A CSV file is a comma- separated values file that uses commas as delimiters. Therefore, a CSV file can be extracted using a delimiter field extraction.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**