Vendor: Splunk

Exam Code: SPLK-1004

Exam Name: Splunk Core Certified Advanced Power User

Version: DEMO

QUESTION 1
Where can wildcards be used in the tstats command?

A. No wildcards can be used with
B. In the where to clause.
C. In the from clause.
D. In the by clause.

Answer: C
Explanation:
Wildcards can be used in the from clause of the tstats command in Splunk (Option C). The from clause specifies the data model or dataset from which to retrieve the statistics, and using wildcards here allows users to query across multiple data models or datasets that share a common naming pattern, making the search more flexible and encompassing.

QUESTION 2
what is the result of the xyseries command?

A. To transform single series output into a multi-series output
B. To transform a stats-like output into chart-like output.
C. To transform a multi-series output into single series output.
D. To transform a chart-like output into a stats-like output.

Answer: B
Explanation:
The result of the xyseries command in Splunk is to transform a stats-like output into chart-like output (Option B). The xyseries command restructures the search results so that each row represents a unique combination of x and y values, suitable for plotting in a chart, making it easier to visualize complex relationships between multiple data points.

QUESTION 3
What XML element is used to pass multiple fields into another dashboard using a dynamic drilldown?

A. <drilldown field_"sources_Field_name">
B. <condition field_"sources_Field_name">
C. <pas_token field_"sources_field_name">
D. <link field_"sources_field_name">

Answer: D
Explanation:
In Splunk Simple XML for dashboards, dynamic drilldowns are configured within the <drilldown> element, not <link>, <condition>, or <pass_token>. To pass multiple fields to another dashboard, you would use a combination of <set> tokens within the <drilldown> element. Each <set> token specifies a field or value to be passed. The correct configuration might look something like this within the <drilldown> element:
<drilldown>
<set token="token1">$row.field1$</set>
<set token="token2">$row.field2$</set>
<link target="_blank">/app/search/new_dashboard</link> </drilldown>
In this configuration, $row.field1$ and $row.field2$ are placeholders for the field values from the clicked event, which are assigned to tokens token1 and token2. These tokens can then be used

in the target dashboard to receive the values. The <link> element specifies the target dashboard. Note that the exact syntax can vary based on the specific requirements of the drilldown and the dashboard configuration.

QUESTION 4
which function of the stats command creates a multivalue entry?

A. mvcombine
B. eval
C. makemv
D. list

Answer: D

QUESTION 5
What is the recommended way to create a field extraction that is both persistent and precise?

A. Use the rex command.
B. Use the Field Extractor and manually edit the generated regular expression.
C. Use the Field Extractor and let it automatically generate a regular expression.
D. Use the erex command.

Answer: B

QUESTION 6
What is the value of base lispy in the Search Job Inspector for the search index-sales clientip-170.192.178.10?

A. [index::sales 192 AND 10 AMD 178 AND 170]
B. [index::sales AND 469 10 702 390]
C. [192 AND 10 AND 178 AND 170 Index::sales]
D. [AND 10 170 178 192 Index::sales]

Answer: A

QUESTION 7
What is an example of the simple XML syntax for a base search and its post-srooess search?

A. <search id="myBaseSearch">, <search base="myBaseSearch">
B. <search globalsearch="myBaseSearch">, <search globalsearch>
C. <panel id="myBaseSearch">, <panel base="myBaseSearch">
D. <search id="myGlobalSearch">, <search base="myBaseSearch">

Answer: A

QUESTION 8
What arguments are required when using the spath command?

A. input, output, index
B. input, output path
C. No arguments are required.
D. field, host, source

Answer: B

QUESTION 9
When possible, what is the best choice for summarizing data to improve search performance?

A. Us the fieldsummary command.
B. Data model acceleration
C. Report acceleration
D. Summary indexing

Answer: D

QUESTION 10
Which syntax is used when referencing multiple CSS files in a view?

A. <dashboard stylesheet="custom.css, userapps.css">
B. <dashboard style="custom.css, userapps.css">
C. <dashboard stylesheet=custom.css stylesheet=userapps.css>
D. <dashboard stylesheet="custom.css | userapps.css">

Answer: C
Explanation:
When referencing multiple CSS files in a Splunk dashboard view (within Simple XML), the correct approach is to include separate stylesheet attributes for each CSS file. The syntax for this would be similar to <dashboard stylesheet="custom.css" stylesheet="userapps.css"> (Option C). This method allows the dashboard to load and apply the styles from both CSS files, enhancing the dashboard's visual appearance and user interface design.

QUESTION 11
How can a lookup be referenced in an alert?

A. Use the lookup dropdown in the alert configuration window.
B. Follow a lookup with an alert command in the search bar.
C. Run a search that uses a lookup and save as an alert.
D. Upload a lookup file directly to the alert.

Answer: C
Explanation:
To reference a lookup in an alert in Splunk, you would run a search that uses a lookup and then save that search as an alert (Option C). This method integrates the lookup within the search logic, and when the search conditions meet the alert's trigger conditions, the alert is activated. This approach allows the alert to leverage the enriched data provided by the lookup for more accurate and informative alerting.

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**