# Free Questions for SPLK-1002 by certscare

## Shared by Mills on 18-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

# Question 1

**Question Type:** **MultipleChoice**

Why would the following search produce multiple transactions instead of one?

Image not found or type unknown

## Options:

**A)** The maxspan option is not included.

**B)** The transaction command has a limit of 1000 events per transaction.

**C)** The transaction and commands cannot be used together.

**D)** The stats list () function is used.

## Answer:

B

## Explanation:

The correct answer is B. The transaction command has a limit of 1000 events per transaction.

The transaction command is used to group events that share some common values into a single record, called a transaction. A transaction can span multiple events and multiple sources, and can be useful for correlating events that are related but not contiguous1.

However, the transaction command has some limitations, one of which is that it can only group up to 1000 events per transaction. This means that if there are more than 1000 events that match the criteria for a transaction, they will be split into multiple transactions. This can result in incomplete or inaccurate transactions2.

To avoid this limitation, you can use the stats command instead of the transaction command. The stats command can also group events by common values, but it does not have a limit on the number of events per group. The stats command also performs faster and consumes less memory than the transaction command1.

In your search, you are using the stats list() function to group events by src_ip and dest_ip. This function returns a multivalue field that contains all the values of a given field for each group. However, this function does not create a single correlated event like the transaction command does. Instead, it creates a table of results with one row per group and one column per field3.

Therefore, your search will produce multiple transactions instead of one because you are using the transaction command with a limit of 1000 events per transaction, and you are using the stats list() function that does not create a single correlated event.

stats command overview

transaction command overview

Splunk Transaction Command: What It Is and How to Use It

Splunk Core Certified Power User SPLK-1002 Practice Exam Part 1

## Question 2

**Question Type:** **MultipleChoice**

Alert throttling is used to ________.

### Options:

**A)** verify each alert

**B)** stagger search request in a time sequenced order

**C)** stop spamming yourself with alerts

**D)** check severity

### Answer:

C

## Question 3

**Question Type:** **MultipleChoice**

A real-time alert is _______________.

### Options:

**A)** A scheduled alert

**B)** constantly running in the background

### Answer:

B

## Question 4

**Question Type:** **MultipleChoice**

This tab shows you the event patterns in the results of a specific search.

### Options:

**A)** statistics

**B)** visualization

**C)** patterns

### Answer:

C

# Question 5

**Question Type: MultipleChoice**

Which of the following are valid options with the chart command ?(select all that apply)

### Options:

**A)** usenull=f

**B)** useother=f

**C)** split=t

**D)** transcation=t

### Answer:

A, B

## Question 6

**Question Type:** **MultipleChoice**

This role is required to install the CIM Add-on.

Select your answer.

### Options:

**A)** ADMIN

**B)** POWER

**C)** USER

### Answer:

A

# Question 7

**Question Type: MultipleChoice**

When using a split series on a chart, the series MUST be displayed using the STACKED option.

## Options:

**A)** True

**B)** False

## Answer:

B

# Question 8

**Question Type: MultipleChoice**

The Splunk CIM Add-on includes data models in a __________ format.

Select your answer.

### Options:

**A)** MySQL

**B)** XML

**C)** JSON

### Answer:

C

## Question 9

**Question Type:** **MultipleChoice**

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

### Options:

**A)** tag=alert

**B)** host::tag::alert

**C)** tag==alert

**D)** tag::host=alert

### Answer:

D

# Question 10

**Question Type:** **MultipleChoice**

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

### Options:

**A)** Tag-<field?

**B)** Tag<filed(tagname.)

**C)** Tag=<filed>::<tagname>

**D)** Tag::<filed>=<tagname>

## Answer:

D