Splunk Fundamentals 1 Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. **Which command is used to visualize time series data in Splunk?**

   A. chart

   B. timechart

   C. top

   D. stats

2. **What is the purpose of alerts in Splunk?**

   A. To visualize data

   B. To send notifications based on conditions

   C. To parse logs

   D. To index data

3. **How many results are returned by default when using the top command?**

   A. 5

   B. 10

   C. 20

   D. 50

4. **What is the minimum number of search heads required for a search head cluster?**

   A. Two

   B. Three

   C. Four

   D. Five

5. **Adding child data model objects is similar to which operator in Splunk?**

   A. NOT

   B. AND

   C. OR

   D. XOR

6. What is the function of the 'by' clause in the stats command?

- **A. Defines the time range for the statistics.**
- **B. Selects the fields that will be counted.**
- **C. Groups results based on specified fields.**
- **D. Filters results before calculations.**

7. How would you modify the search to change the name of the count column to "Total Viewed"?

- **A. index=network sourcetype=cisco_wsa_squid | top user x_webcat_code_full limit=3 showperc=f**
- **B. index=network sourcetype=cisco_wsa_squid | top user x_webcat_code_full limit=3 *countfield="Total Viewed"* showperc=f**
- **C. index=network sourcetype=cisco_wsa_squid | top user x_webcat_code_full limit=3 count="Total Viewed"**
- **D. index=network sourcetype=cisco_wsa_squid | top user x_webcat_code_full limit=3 | rename count as "Total Viewed"**

8. What is the purpose of the CLI command 'splunk enable boot-start'?

- **A. To start Splunk service manually**
- **B. To enable Splunk to run on system boot**
- **C. To schedule data uploads**
- **D. To set up a remote indexer**

9. In the provided device log entries, what are the field names?

- **A. icmp_seq and ttl**
- **B. 0 and 64**
- **C. = and =**
- **D. icmp_seq and 0**

10. How does the process of indexing work in Splunk?

- **A. Converts data into raw format**
- **B. Aggregates data into a single file**
- **C. Breaks time-series data into events**
- **D. Compresses data for storage**

Answers

1. B
2. B
3. B
4. B
5. B
6. C
7. B
8. B
9. A
10. C

Explanations

1. Which command is used to visualize time series data in Splunk?

A. chart

B. timechart

C. top

D. stats

The command used to visualize time series data in Splunk is "timechart." This command is specifically designed to create visual representations of how a particular metric changes over time, making it ideal for trending analysis. When you use "timechart," Splunk automatically handles the time axis and aggregates the data in a way that allows for easy comparison across specified time intervals. For instance, if you're looking at the number of errors occurring in your logs over a series of days, "timechart" will display this data clearly in a line graph or bar chart format, enabling you to spot trends or anomalies visually. While other commands like "chart," "top," and "stats" can also provide useful summaries and metrics, they do not have the specific functionality to handle time series data in the same intuitive manner as "timechart." "Chart" is more general for grouping and visualizing data without an inherent time structure, "top" focuses on the most frequent values within a field, and "stats" aggregates data but does not inherently create time series visualizations. Thus, the "timechart" command stands out as the appropriate choice for visualizing data that varies over time.

2. What is the purpose of alerts in Splunk?

A. To visualize data

B. To send notifications based on conditions

C. To parse logs

D. To index data

The primary purpose of alerts in Splunk is to send notifications based on conditions that you define. Alerts monitor your data in real-time or on a scheduled basis, evaluating whether specific criteria are met. When these conditions are triggered, alerts can automatically notify users through various channels, such as email or webhook notifications. This functionality is crucial for maintaining situational awareness, allowing teams to respond quickly to vital events, anomalies, or security threats identified in their data. Visualizing data, parsing logs, and indexing data are all important functions within Splunk, but they serve different purposes. Visualization is focused on presenting data in graphical formats to aid analysis, parsing logs is about breaking down raw data into structured formats for effective searching, and indexing data refers to the process of storing data efficiently to enable fast searches. These functions do not directly relate to the goal of alerts, which is about notifying users based on specific events or conditions detected in the data.

3. How many results are returned by default when using the top command?

A. 5

B. 10

C. 20

D. 50

When using the top command in Splunk, the default number of results returned is 10. This command is used to identify the most frequently occurring values in a specific field, which can be useful for gaining insights into the most common data points within your dataset. It's important to note that while the command will return 10 results by default, users have the ability to specify a different number of results if needed by providing an additional argument in the command syntax. For example, if you want to see more results, you can modify the command to specify a greater number of top items to return. The other options reflect different values that are not the default outcome of the top command, further emphasizing the importance of knowing default settings for effectively utilizing Splunk commands.

4. What is the minimum number of search heads required for a search head cluster?

A. Two

B. Three

C. Four

D. Five

A search head cluster in Splunk is designed to provide high availability and load balancing for searches across multiple search heads. The minimum number of search heads required for a search head cluster is three. This configuration allows for a quorum to be established, which is crucial for maintaining cluster management and ensuring that the cluster continues to function correctly, even if one of the search heads goes offline. Having at least three search heads helps in achieving fault tolerance; with a majority (two out of three) still operational, the cluster can continue performing searches. This setup also improves performance by allowing searches to be distributed among the search heads, reducing the load on any single instance and leading to faster query responses. Options mentioning fewer search heads (like two) do not provide sufficient fault tolerance, as losing one of the two search heads would result in a situation where there's no majority to maintain the cluster. Therefore, a configuration of three search heads is considered the minimum requirement to ensure effective clustering and operational reliability.

5. Adding child data model objects is similar to which operator in Splunk?

A. NOT

B. AND

C. OR

D. XOR

The correct answer is that adding child data model objects is similar to the AND operator in Splunk. When you create a data model in Splunk, you can define parent and child objects, where the child objects inherit the characteristics and data attributes of the parent. This relationship simulates a logical AND operation, as the events must meet the criteria of both the parent and the specified child objects. This means that only events that satisfy both the parent object's criteria and the child object's criteria will be included in the results. The distinction is important in understanding how data models effectively aggregate and filter data. By utilizing the AND logic, Splunk ensures that the data returned is precise and meets the specific conditions outlined within multiple levels of the data model hierarchy.

6. What is the function of the 'by' clause in the stats command?

A. Defines the time range for the statistics.

B. Selects the fields that will be counted.

C. Groups results based on specified fields.

D. Filters results before calculations.

The 'by' clause in the stats command is used to group results based on specified fields. When you want to aggregate data and perform statistical operations, the 'by' clause allows you to segment the results into distinct categories based on the values of one or more fields. This functionality is essential when you are interested in calculating statistics like counts, averages, or sums within specific groups of your dataset. For example, if you want to find the total number of events per user, you would use the 'by' clause to group your data according to the user field. Consequently, you will get a clearer insight into the statistics as they relate to each unique user rather than a singular overall total, enhancing the analysis's effectiveness and granularity.

7. How would you modify the search to change the name of the count column to "Total Viewed"?

A. index=network sourcetype=cisco_wsa_squid | top user x_webcat_code_full limit=3 showperc=f

B. index=network sourcetype=cisco_wsa_squid | top user x_webcat_code_full limit=3 *countfield="Total Viewed"* showperc=f

C. index=network sourcetype=cisco_wsa_squid | top user x_webcat_code_full limit=3 count="Total Viewed"

D. index=network sourcetype=cisco_wsa_squid | top user x_webcat_code_full limit=3 | rename count as "Total Viewed"

The correct choice to modify the search to change the name of the count column to "Total Viewed" effectively uses the built-in functionality of the `top` command in Splunk. The command allows you to specify a new name for the count field directly in the search syntax. In this case, the syntax `*countfield="Total Viewed"*` is correct because it specifies the desired name for the count column while the `top` command processes its results. This means that as the data is aggregated, the output will reflect your new label for the count column, showing the total occurrences alongside the other specified fields. The significance of this ability enhances the clarity of your Splunk reports and visualizations by allowing them to be more descriptive and tailored to the audience's understanding. Properly renaming fields is a key practice in data analytics as it helps provide context and clarity. Other approaches, while useful for different purposes, do not achieve the same outcome. For example, manipulating the `rename` command after calculating counts is possible but adds an additional step. Therefore, integrating the renaming directly within the counting process simplifies the search and makes it more efficient.

8. What is the purpose of the CLI command 'splunk enable boot-start'?

A. To start Splunk service manually

B. To enable Splunk to run on system boot

C. To schedule data uploads

D. To set up a remote indexer

The command 'splunk enable boot-start' serves to configure the Splunk service so that it automatically starts when the operating system boots up. This functionality is crucial for ensuring that Splunk is always running and ready to process data without requiring manual intervention after a system restart. By enabling this boot start feature, it enhances the uptime and availability of the Splunk instance, allowing for continuous data collection and analysis. Additionally, the other options do not accurately reflect the purpose of this command. While starting the Splunk service manually or scheduling data uploads are important tasks, they are not achieved through this specific command. Setting up a remote indexer also does not relate to the boot-start configuration. Overall, enabling Splunk to run on system boot is the primary function associated with this command.

9. In the provided device log entries, what are the field names?

A. icmp_seq and ttl

B. 0 and 64

C. = and =

D. icmp_seq and 0

The field names in the context of log entries typically represent specific pieces of data that are extracted and recorded by log management systems like Splunk. In network-related logs, fields such as "icmp_seq" and "ttl" are common. "icmp_seq" stands for Internet Control Message Protocol sequence number, which is critical for tracking the sequence of packets being sent over the network. "ttl" stands for Time To Live, which is a field in the IP header that indicates the lifespan of the packet in the network. These fields are essential for analyzing network traffic and diagnosing issues, as they provide key insights about how data packets are flowing within the network. Focusing on these specific field names allows users to filter, search, and gather analytics on pertinent network activities efficiently. In contrast, the other options do not represent field names. "0" and "64" are values that could relate to these fields but do not serve as identifiers. "=" is a symbol used in various contexts but does not define a field name. Therefore, the identification of "icmp_seq" and "ttl" as field names is accurate and critical for effective data extraction and analysis in log management.

10. How does the process of indexing work in Splunk?

A. Converts data into raw format

B. Aggregates data into a single file

C. Breaks time-series data into events

D. Compresses data for storage

The process of indexing in Splunk primarily involves breaking time-series data into individual events. This is fundamental to how Splunk processes and manages data for effective searching and analysis. When data is ingested into Splunk, it identifies time-stamped records and separates them into discrete events based on specified configurations, such as line-breaking rules. Each event retains metadata, including timestamps and source information, which makes it easier to query and analyze the data later. By extracting meaningful events from continuous streams of data, Splunk ensures that users can perform more efficient searches and analyses, leveraging the time-based dimensions of the data. This event-based architecture allows for powerful capabilities in real-time data processing, which is especially crucial for machine data and log files, where continuous input is common. The other choices highlight aspects of data handling but do not capture the essence of the indexing function. Converting data into raw format is a step in data ingestion but doesn't define indexing. Aggregating data into a single file doesn’t align with how Splunk organizes and processes individual entries. While data compression can be part of the storage process for efficiency, it is not a primary function of indexing itself.