Vendor: Splunk

Exam Code: SPLK-1001

Exam Name: Splunk Core Certified User

Version: DEMO

QUESTION 1
When placed early in a search, which command is most effective at reducing search execution time?

A. dedup
B. rename
C. sort -
D. fields +

Answer: A

QUESTION 2
In the Splunk interface, the list of alerts can be filtered based on which characteristics?

A. App, Owner, Severity, and Type
B. App, Owner, Priority, and Status
C. App, Dashboard, Severity, and Type
D. App, Time Window, Type, and Severity

Answer: D

QUESTION 3
When displaying results of a search, which of the following is true about line charts?

A. Line charts are optimal for single and multiple series.
B. Line charts are optimal for single series when using Fast mode.
C. Line charts are optimal for multiple series with 3 or more columns.
D. Line charts are optimal for multiseries searches with at least 2 or more columns.

Answer: C

QUESTION 4
A collection of items containing things such as data inputs, UI elements, and knowledge objects is known as what?

A. An app
B. JSON
C. A role
D. An enhanced solution

Answer: A

QUESTION 5
Which of the following fields is stored with the events in the index?

A. user
B. source
C. location
D. sourcelp

Answer: B

QUESTION 6
Which of the following is the recommended way to create multiple dashboards displaying data from the same search?

A. Save the search as a report and use it in multiple dashboards as needed
B. Save the search as a dashboard panel for each dashboard that needs the data
C. Save the search as a scheduled alert and use it in multiple dashboards as needed
D. Export the results of the search to an XML file and use the file as the basis of the dashboards

Answer: A

QUESTION 7
What must be done in order to use a lookup table in Splunk?

A. The lookup must be configured to run automatically.
B. The contents of the lookup file must be copied and pasted into the search bar.
C. The lookup file must be uploaded to Splunk and a lookup definition must be created.
D. The lookup file must be uploaded to the etc/apps/lookups folder for automatic ingestion.

Answer: C

QUESTION 8
What is a suggested Splunk best practice for naming reports?

A. Reports are best named using many numbers so they can be more easily sorted.
B. Use a consistent naming convention so they are easily separated by characteristics such as group and object.
C. Name reports as uniquely as possible with no overlap to differentiate them from one another.
D. Any naming convention is fine as long as you keep an external spreadsheet to keep track.

Answer: B

QUESTION 9
Which of the following Splunk components typically resides on the machines where data originates?

A. Indexer
B. Forwarder
C. Search head
D. Deployment server

Answer: B

QUESTION 10
What does the following specified time range do?

```
earliest=-72h@h
latest=@d
```

A. Look back 3 days ago and prior
B. Look back 72 hours up to one day ago
C. Look back 72 hours, up to the end of today
D. Look back from 3 days ago up to the beginning of today

Answer: D

QUESTION 11
Which of the following is true about user account settings and preferences?

A. Search & Reporting is the only app that can be set as the default application.
B. Full names can only be changed by accounts with a Power User or Admin role.
C. Time zones are automatically updated based on the setting of the computer accessing Splunk.
D. Full name, time zone, and default app can be defined by clicking the login name in the Splunk bar.

Answer: D

QUESTION 12
Which of the following are common constraints of the top command?

A. limit, count
B. limit, showpercent
C. limits, countfield
D. showperc, countfield

Answer: B

QUESTION 13
What is the purpose of using a by clause with the stats command?

A. To group the results by one or more fields.
B. To compute numerical statistics on each field.
C. To specify how the values in a list are delimited.
D. To partition the input data based on the split-by fields.

Answer: A

QUESTION 14
Which events will be returned by the following search string? host=www3 status=503

A. All events that either have a host of www3 or a status of 50.
B. All events with a host of www3 that also have a status of 503
C. We need more information: we cannot tell without knowing the time range
D. We need more information a search cannot be run without specifying an index

Answer: B

QUESTION 15
Which of the following searches would return events with failure in index netfw or warn or critical in index netops?

A. (index=netfw failure) AND index=netops warn OR critical
B. (index=netfw failure) OR (index=netops (warn OR critical))
C. (index=netfw failure) AND (index=netops (warn OR critical))
D. (index=netfw failure) OR index=netops OR (warn OR critical)

Answer: B

QUESTION 16
At index time, in which field does Splunk store the timestamp value?

A. time
B. _time
C. EventTime
D. timestamp

Answer: B

QUESTION 17
Which statement is true about the top command?

A. It returns the top 10 results
B. It displays the output in table format
C. It returns the count and percent columns per row
D. All of the above

Answer: D

QUESTION 18
What determines the scope of data that appears in a scheduled report?

A. All data accessible to the User role will appear in the report.
B. All data accessible to the owner of the report will appear in the report.
C. All data accessible to all users will appear in the report until the next time the report is run.
D. The owner of the report can configure permissions so that the report uses either the User role or the owner's profile at run time.

Answer: D

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**