TOPEXAM

一番権威的な IT 認定試験ウェブサイト

http://www.topexam.jp

最も新たな国際 IT 認定試験問題集

Exam : **SPLK-1001**

Title : Splunk Core Certified User

Vendor : Splunk

Version : DEMO

NO.1 Which statement describes field discovery at search time?
A. Splunk automatically discovers only alphanumeric fields
B. Splunk automatically discovers only fields directly related to the search results
C. Splunk automatically discovers only manually configured fields
D. Splunk automatically discovers only numeric fields
Answer: B

NO.2 You can also specify a time range in the search bar. You can use the following for beginning and ending for a time range (Choose two.):
A. earliest=
B. latest=
C. start=
D. Not possible to specify time manually in Search query
E. end=
Answer: A,B

NO.3 Which of the following is the best way to create a report that shows the last 24 hours of events?
A. Use the time range picket to select "Yesterday"
B. Use earliest=-1d@d latest=@d
C. Set a real-time search over a 24-hour window
D. Use the time range picker to select "Last 24 hours"
Answer: D

NO.4 A collection of items containing things such as data inputs, UI elements, and knowledge objects is known as what?
A. A role
B. An app
C. JSON
D. An enhanced solution
Answer: B

NO.5 Splunk shows data in _____.
A. Reverse chronological order.
B. Alphanumeric order.
C. Chronological order.
D. ASCII Character order.
Answer: A

NO.6 What are the steps to schedule a report?
A. After saving the report, click Event Type.
B. After saving the report, click Schedule.
C. After saving the report, click Scheduling.

D. After saving the report, click Dashboard Panel.
Answer: B

NO.7 What options do you get after selecting timeline? (Choose four.)
A. Zoom Out
B. Zoom to selection
C. Format Timeline
D. Deselect
E. Delete
Answer: A,B,C,D

NO.8 What is Search Assistant in Splunk?
A. Shows options to complete the search string
B. It is only available to Admins.
C. Such feature does not exist in Splunk.
Answer: A

NO.9 By default, all users have DELETE permission to ALL knowledge objects.
A. True
B. False
Answer: B

NO.10 Query - status != 100:
A. Will get different results depending on data
B. Will return event where status field exist but value of that field is not 100.
C. Will return event where status field exist but value of that field is not 100 and all events where status field doesn't exist.
Answer: B

NO.11 The command shown here does witch of the following: Command: |outputlookup products.csv
A. Writes search results to a file named products.csv
B. Returns the contents of a file named products.csv
Answer: A

NO.12 When running searches command modifiers in the search string are displayed in what color?
A. Blue
B. Orange
C. Red
D. Highlighted
Answer: A

NO.13 Following are the time selection option while making search:

(Choose all that apply.)
A. Presets
B. Advanced
C. Date Range
D. Relative
E. Date & Time Range
Answer: B

NO.14 We should use heavy forwarder for sending event-based data to Indexers.
A. True
B. False
Answer: A

NO.15 _____ is the default web port used by Splunk.
A. 8089
B. 443
C. 8080
D. 8000
Answer: D

NO.16 Which command is used to validate a lookup file?
A. inputlookup products.csv
B. | lookup definition products.csv
C. I inputlookup products.csv
D. | lookup products.csv
Answer: C

NO.17 When a search returns _____, you can view the results as a list.
A. a list of events
B. statistical values
C. transactions
Answer: B

NO.18 Prefix wildcards might cause performance issues.
A. False
B. True
Answer: B

NO.19 How to make Interesting field into a selected field?
A. Not possible.
B. Only CLI changes will enable it.
C. Click field in field sidebar -> click YES on the pop-up dialog on upper right side -> check now field should be visible in the list of selected fields.

D. Click Settings -> Find field option -> Drop down select field -> enable selected field -> check now field should be visible in the list of selected fields.
Answer: C

NO.20 Which of the following constraints can be used with the top command?
A. useperc
B. limit
C. addtotals
D. fieldcount
Answer: B