Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

SPLK-1001 Dumps
SPLK-1001 Braindumps
SPLK-1001 Real Questions
SPLK-1001 Practice Test
SPLK-1001 Actual Questions

PASS

Splunk

SPLK-1001

Splunk Core Certified User

Question: 238

When editing a dashboard, which of the following are possible options? (select all that apply)
A . Add an output.
B . Export a dashboard panel.
C . Modify the chart type displayed in a dashboard panel.
D . Drag a dashboard panel to a different location on the dashboard.

Answer: C

Question: 239

Which of the following constraints can be used with the top command?
A . limit
B . useperc
C . addtotals
D . fieldcount

Answer: A

Question: 240

Which of the following constraints can be used with the top command?
A . limit
B . useperc
C . addtotals
D . fieldcount

Answer: A

Explanation:

Reference: https://answers.splunk.com/answers/339141/how-to-use-top-command-or-stats-with-sortresults.html

Question: 241

How are events displayed after a search is executed?
A . In chronological order.
B . Randomly by default.
C . In reverse chronological order.
D . Alphabetically according to field name.

Answer: A

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/SearchReference/Eventorderfunctions

Question: 242

Which of the following represents the Splunk recommended naming convention for dashboards?
A . Description_Group_Object
B . Group_Description_Object
C . Group_Object_Description
D . Object_Group_Description

Answer: C

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Knowledge/ Developnamingconventionsforknowledgeobjecttitles

Question: 243

What is a primary function of a scheduled report?
A . Auto-detect changes in performance.
B . Auto-generated PDF reports of overall data trends.
C . Regularly scheduled archiving to keep disk space use low.
D . Triggering an alert in your Splunk instance when certain conditions are met.

Answer: D

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Report/Schedulereports

Question: 244

When sorting on multiple fields with the sort command, what delimiter can be used between the field names in the search?
A . |
B . $
C . !
D . ,

Answer: D

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/SearchReference/Sort

Question: 245

Which of the following are common constraints of the top command?
A . limit, count
B . limit, showpercent
C . limits, countfield
D . showperc, countfield

Answer: A

Question: 246

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: 247

How can search results be kept longer than 7 days?
A . By scheduling a report.
B . By creating a link to the job.
C . By changing the job settings.

D . By changing the time range picker to more than 7 days.

Answer: C

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Extendjoblifetimes

Question: 248

Select the answer that displays the accurate placing of the pipe in the following search string:

index=security sourcetype=access_* status=200 stats count by price
A . index=security sourcetype=access_* status=200 stats | count by price
B . index=security sourcetype=access_* status=200 | stats count by price
C . index=security sourcetype=access_* status=200 | stats count | by price
D . index=security sourcetype=access_* | status=200 | stats count by price

Answer: A

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Aboutsubsearches

Question: 249

Which command is used to review the contents of a specified static lookup file?
A . lookup
B . csvlookup
C . inputlookup
D . outputlookup

Answer: C

Question: 250

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: C

Question: 251

Which of the following is a Splunk search best practice?
A . Filter as early as possible.
B . Never specify more than one index.
C . Include as few search terms as possible.
D . Use wildcards to return more search results.

Answer: A

Question: 252

When writing searches in Splunk, which of the following is true about Booleans?
A . They must be lowercase.
B . They must be uppercase.

C . They must be in quotations.
D . They must be in parentheses.

Answer: D

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Booleanexpressions

Question: 253

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

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Viz/LineAreaCharts

Question: 254

Which of the following searches would return events with failure in index netfw or warn or criticalin 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

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Search/Aboutsubsearches

Question: 255

When looking at a dashboard panel that is based on a report, which of the following is true?
A . You can modify the search string in the panel, and you can change and configure the visualization.
B . You can modify the search string in the panel, but you cannot change and configure the visualization.
C . You cannot modify the search string in the panel, but you can change and configure the visualization.
D . You cannot modify the search string in the panel, and you cannot change and configure the visualization.

Answer: C

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Viz/WorkingWithDashboardPanels

Question: 256

What must be done before an automatic lookup can be created? (select all that apply)
A . The lookup command must be used.
B . The lookup definition must be created.
C . The lookup file must be uploaded to Splunk.
D . The lookup file must be verified using the inputlookup command.

Answer: B

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Knowledge/ DefineanautomaticlookupinSplunkWeb

Question: 257

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

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/7.2.6/Report/Managereportpermissions

Question: 258

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: B

SAMPLE QUESTIONS

These questions are for demo purpose only. ***Full version*** *is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

Actual Exam Questions*: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

Exam Dumps*: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

Practice Tests*: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

Guaranteed Success*: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

Updated Content: *Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

Technical Support*: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*