



Up-to-date Practice Test with Latest Questions and Answers covering latest syllabus and topics of the exam. Makes you ready to face actual exam.



SPLK-1001 Practice Questions
SPLK-1001 Practice Test
SPLK-1001 Practice Exam
SPLK-1001 Exam Questions
SPLK-1001 Study Guide



killexams.com

Splunk

SPLK-1001

Splunk Core Certified User

ORDER FULL VERSION

<https://killexams.com/pass4sure/exam-detail/SPLK-1001>



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](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 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

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](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

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including Exam Questions, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.



Practice Exam Questions Based on Current Exam Objectives

Killexams.com provides practice exam questions aligned with the latest official exam objectives and latest syllabus. Our content is reviewed and updated regularly to reflect recent changes announced by certification vendors. By studying these practice questions, candidates will cover the structure, difficulty level, and topics of the actual exam, helping them prepare more effectively and efficiently.

Comprehensive Practice Exams (PDF Format)

Killexams.com offers multiple-choice questions (MCQs) in easy-to-read PDF format, covering all major domains of the exam. Each PDF contains a structured collection of practice questions and verified answers designed to support focused study. These MCQs help candidates reinforce key concepts, identify knowledge gaps, and improve exam readiness through consistent practice.

Realistic Practice Tests (Online Test Engine & Desktop Test Engine)

To support hands-on preparation, Killexams.com provides practice tests through both an Online Test Engine and a Desktop Test Engine. These tools are designed to simulate a real exam environment, allowing candidates to practice under exam-like conditions, with latest syllabus and topics of the exam. Performance tracking, test history, and result analysis help users evaluate their progress and focus on areas that need improvement.

Risk-Free Purchase Policy

Killexams.com follows a transparent and customer-friendly purchase policy. If users are not satisfied with the study materials, they may request assistance or a refund in accordance with our published terms and conditions. This policy reflects our commitment to customer satisfaction, fairness, and confidence in our preparation resources.

Regularly Updated Content

Our practice question bank is reviewed and updated on an ongoing basis to stay aligned with the latest exam outlines and vendor updates. This ensures candidates are studying up-to-date, relevant material, and preparing with content that reflects current exam expectations, helping them stay confident and well-prepared.