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-1002 Practice Questions
SPLK-1002 Practice Test
SPLK-1002 Practice Exam
SPLK-1002 Exam Questions
SPLK-1002 Study Guide

killexams.com

Splunk

SPLK-1002

Splunk Core Certified Power User

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/SPLK-1002

Question: 168

Which of the following statements about event types is true? (select all that apply)
A . Event types can be tagged.
B . Event types must include a time range,
C . Event types categorize events based on a search.
D . Event types can be a useful method for capturing and sharing knowledge.

Answer: A,C,D

Explanation:

Reference: https://www.edureka.co/blog/splunk-events-event-types-and-tags/

Question: 169

To identify all of the contributing events within a transaction that contains at least one REJECT event, which syntax is correct?
A . Index-main | REJECT trans sessionid
B . Index-main | transaction sessionid | search REJECT
C . Index=main | transaction sessionid | whose transaction=reject
D . Index=main | transaction sessionid | where transaction=reject''

Answer: B

Question: 170

Which of the following statements describe data model acceleration? (select all that apply)
A . Root events cannot be accelerated.
B . Accelerated data models cannot be edited.
C . Private data models cannot be accelerated.
D . You must have administrative permissions or the accelerate_dacamodel capability to accelerate a data model.

Answer: C,D

Question: 171

Which of the following statements would help a user choose between the transaction and stars commands?
A . stats can only group events using IP addresses.
B . The transaction command is faster and more efficient.
C . There is a 1000 event limitation with the transaction command.
D . Use stats when the events need to be viewed as a single correlated event.

Answer: C

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/SearchReference/Transaction

Question: 172

Which one of the following statements about the search command is true?
A . It does not allow the use of wildcards.
B . It treats field values in a case-sensitive manner.
C . It can only be used at the beginning of the search pipeline.
D . It behaves exactly like search strings before the first pipe.

Answer: C

Explanation:

Reference: https://docs.splunk.com/Documentation/SplunkCloud/8.0.2003/Search/Usethesearchcommand

Question: 173

When using the Field Extractor (FX), which of the following delimiters will work? (Choose all that apply.)
A . Tabs
B . Pipes
C . Colons
D . Spaces

Answer: BD

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/FXSelectMethodstep

Question: 174

When can a pipe follow a macro?
A . A pipe may always follow a macro.
B . The current user must own the macro.
C . The macro must be defined in the current app.
D . Only when sharing is set to global for the macro.

Answer: A

Question: 175

Data models are composed of one or more of which of the following datasets? (Choose all that apply.)

A . Events datasets
B . Search datasets
C . Transaction datasets
D . Any child of event, transaction, and search datasets

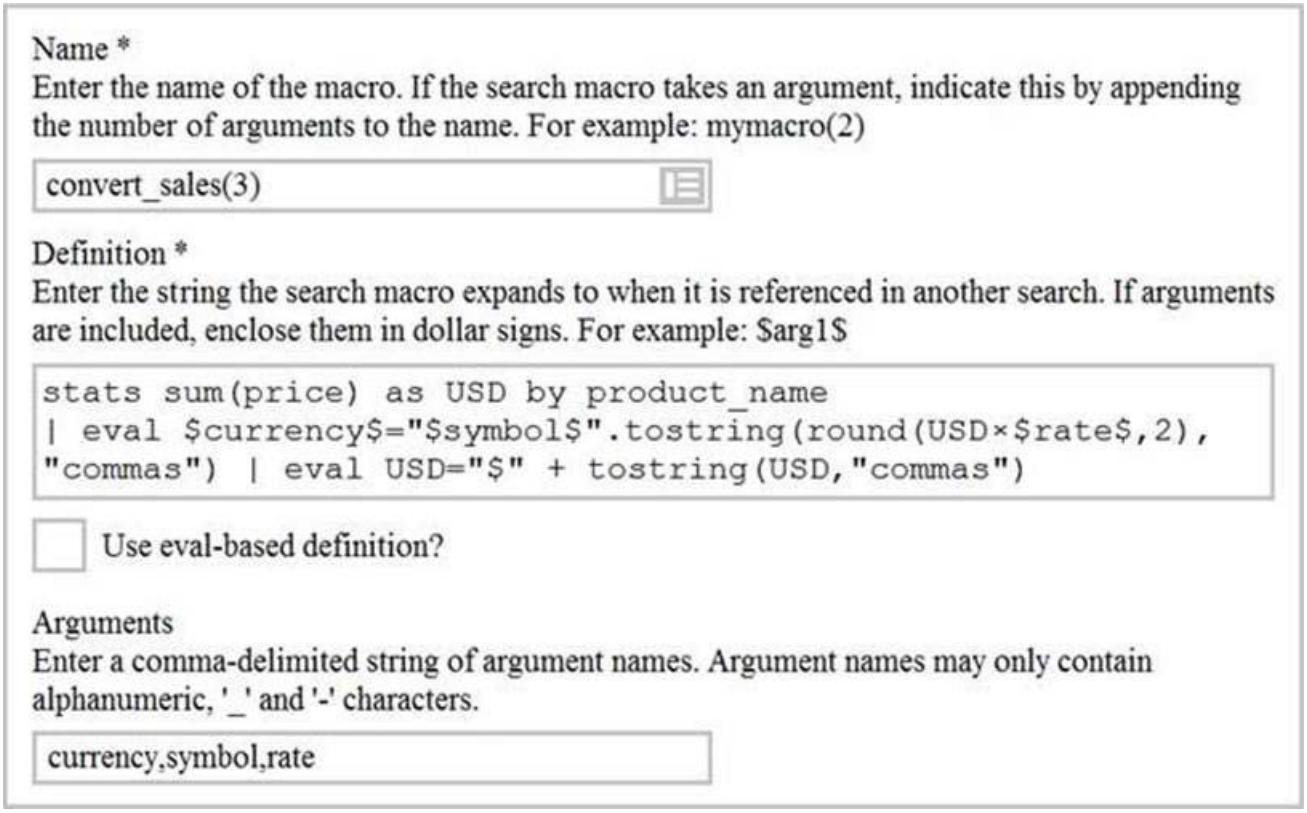
Answer: ABC

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Aboutdatamodels

Question: 176

Based on the macro definition shown below, what is the correct way to execute the macro in a search string?



A . "convert_sales(euro,,.79)"
B . ‘convert_sales(euro,,.79)’
C . "convert_sales($euro$,$$,$.79$)"
D . ‘convert_sales($euro$,$$,$.79$)’

Answer: D

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Usesearchmacros

Question: 177

Which of the following actions can the eval command perform?
A . Remove fields from results.
B . Create or replace an existing field.
C . Group transactions by one or more fields.
D . Save SPL commands to be reused in other searches.

Answer: A

Question: 178

Which group of users would most likely use pivots?
A . Users
B . Architects
C . Administrators
D . Knowledge Managers

Answer: D

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Pivot/IntroductiontoPivot

Question: 179

Which delimiters can the Field Extractor (FX) detect? (Choose all that apply.)
A . Tabs
B . Pipes
C . Spaces
D . Commas

Answer: BCD

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/FXSelectMethodstep

Question: 180

Which of the following statements describe the Common Information Model (CIM)? (Choose all that apply.)
A . CIM is a methodology for normalizing data.
B . CIM can correlate data from different sources.
C . The Knowledge Manager uses the CIM to create knowledge objects.
D . CIM is an app that can coexist with other apps on a single Splunk deployment.

Answer: AB

Explanation:

Reference: https://docs.splunk.com/Documentation/CIM/4.15.0/User/Overview

Question: 181

There are several ways to access the field extractor.

Which option automatically identifies the data type, source type, and sample event?
A . Event Actions > Extract Fields
B . Fields sidebar > Extract New Fields
C . Settings > Field Extractions > New Field Extraction
D . Settings > Field Extractions > Open Field Extractor

Answer: C

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.4/Knowledge/Managesearchtimefieldextractions

Question: 182

Which of the following knowledge objects represents the output of an eval expression?
A . Eval fields
B . Calculated fields
C . Field extractions
D . Calculated lookups

Answer: B

Explanation:

Reference: https://docs.splunk.com/Splexicon:Calculatedfield

Question: 183

By default, how is acceleration configured in the Splunk Common Information Model (CIM) add-on?
A . Turned off.
B . Turned on.
C . Determined automatically based on the source type.
D . Determined automatically based on the data source.

Answer: D

Question: 184

What do events in a transaction have in common?

A . All events in a transaction must have the same timestamp.
B . All events in a transaction must have the same source type.
C . All events in a transaction must have the exact same set of fields.
D . All events in a transaction must be related by one or more fields.

Answer: B

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Abouttransactions

Question: 185

When multiple event types with different color values are assigned to the same event, what determines the color displayed for the event?
A . Rank
B . Weight
C . Priority
D . Precedence

Answer: C

Explanation:

Reference: https://docs.splunk.com/Documentation/SplunkCloud/8.0.2003/Knowledge/Defineeventtypes

KILLEXAMS.COM

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 syllbus 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.