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

KILL EXAMS

SPLK-1002 Dumps
SPLK-1002 Braindumps
SPLK-1002 Real Questions
SPLK-1002 Practice Test
SPLK-1002 Actual Questions

PASS

Splunk

SPLK-1002

Splunk Core Certified Power User

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

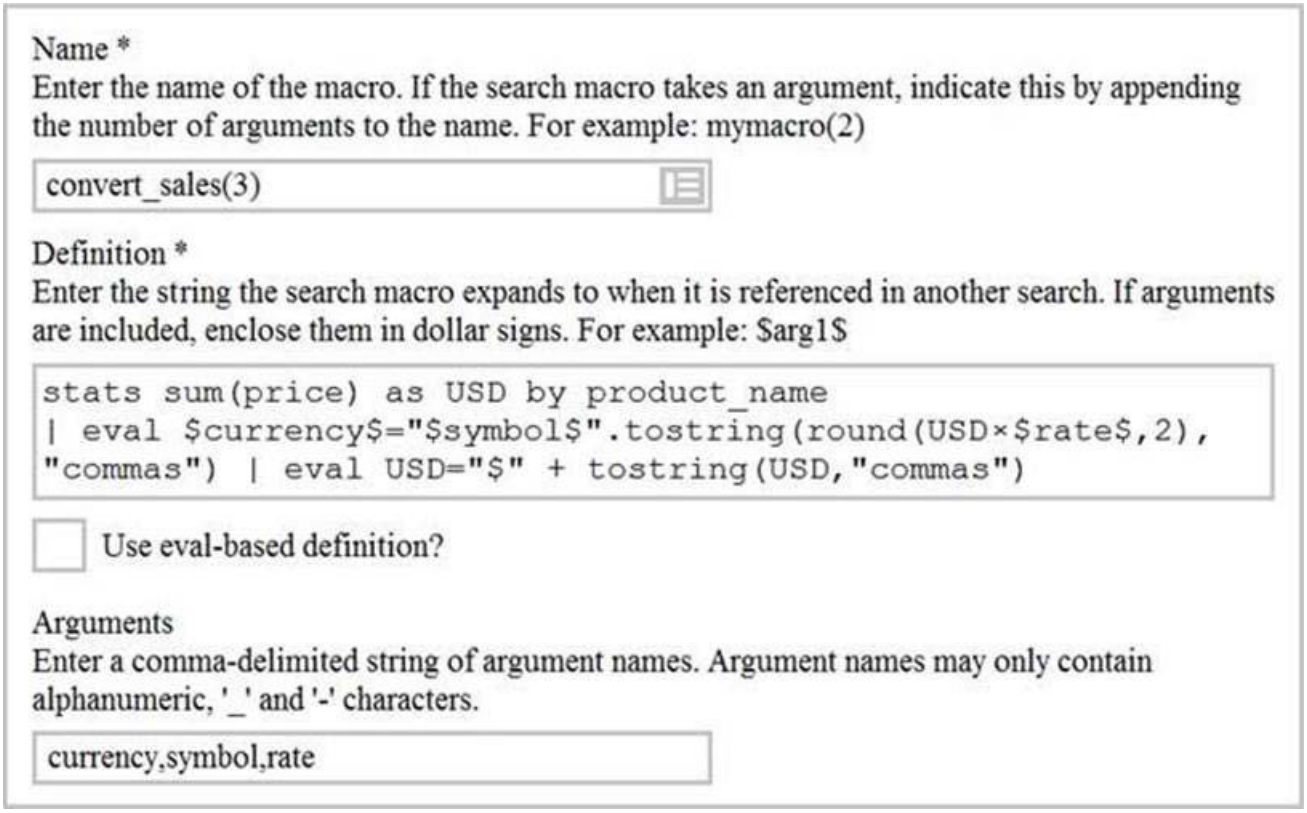
Answer: ABC

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

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.*