DUMPSARENA

Splunk Core Certified User

Splunk SPLK-1001

Version Demo

Total Demo Questions: 15

Total Premium Questions: 243

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Three basic components of Splunk are (Choose three.):

A. Forwarders

B. Deployment Server

C. Indexer

D. Knowledge Objects

E. Index

F. Search Head

ANSWER: A C F

QUESTION NO: 2

Which Field/Value pair will return only events found in the index named security?

A. Index=Security

B. index=Security

C. Index=security

D. index!=Security

ANSWER: B

Explanation:

Reference: https://answers.splunk.com/answers/712164/why-are-the-wineventlogssecurity-indexing-in-diffe.html

QUESTION NO: 3

Which Field/Value pair will return only events found in the index named security?

A. index!=Security

B. Index-security

C. Index=Security

D. index=Security

ANSWER: D

Explanation:

The Kusto Query Language (KQL) is the language you use to query data in Azure Data Explorer [1]. To query for events that are found in the index named security, you would use the following KQL query:

index=Security

This query will return all events that are found in the security index. It is important to note that the "=" operator must be used in order to match the exact index name.

QUESTION NO: 4

Which component of Splunk is primarily responsible for saving data?

A. Search Head

B. Heavy Forwarder

C. Indexer

D. Universal Forwarder

ANSWER: C

QUESTION NO: 5

What options do you get after selecting timeline? (Choose four.)

A. Zoom to selection

B. Format Timeline

C. Deselect

D. Delete

E. Zoom Out

ANSWER: A B C E

QUESTION NO: 6

Which of the statements are correct about HF? (Choose three.)

A. Parsing

B. Masking

C. Searching

D. Forwarding

ANSWER: A B D

QUESTION NO: 7

By default, how long does Splunk retain a search job?

A. 10 Minutes

B. 15 Minutes

C. 1 Day

D. 7 Days

ANSWER: A

Explanation:

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

QUESTION NO: 8

Assuming a user has the capability to edit reports, which of the following are editable?

A. Acceleration, schedule, permissions

B. The report's name, schedule, permissions

C. The report's name, acceleration, schedule

D. The report's name, acceleration, permissions

ANSWER: B

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Report/Createandeditreports

QUESTION NO: 9

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. Not possible to specify time manually in Search query

B. end=

C. start=

D. earliest=

E. latest=

ANSWER: D E

QUESTION NO: 10

Which of the following statements about case sensitivity is true?

A. Both field names and field values ARE case sensitive.

B. Field names ARE case sensitive; field values are NOT.

C. Field values ARE case sensitive; field names ARE NOT.

D. Both field names and field values ARE NOT case sensitive.

ANSWER: B

Explanation:

Reference: https://answers.splunk.com/answers/65/are-field-values-case-sensitive.html

QUESTION NO: 11

Select the best options for "search best practices" in Splunk:

(Choose five.)

A. Select the time range always.

B. Try to specify index values.

C. Include as many search terms as possible.

D. Never select time range.

E. Try to use * with every search term.

F. Inclusion is generally better than exclusion.

G. Try to keep specific search terms.

ANSWER: A B C F G

QUESTION NO: 12

Data summary button just below the search bar gives you the following (Choose three.):

A. Hosts

B. Sourcetypes

C. Sources

D. Indexes

ANSWER: A B C

QUESTION NO: 13

Which symbol is used to snap the time?

A. @

B. &

C. *

D. #

ANSWER: A

QUESTION NO: 14

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. Not possible to specify time manually in Search query

B. end=

C. start=

D. earliest=

E. latest=

ANSWER: D E

QUESTION NO: 15

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