Splunk SPLK-1003 Mock Exam

Shared by Frazier on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An add-on has configured field aliases for source IP address and destination IP address fields. A specific user prefers not to have those fields present in their user context. Based on the defaultprops.confbelow, whichSPLUNK_HOME/etc/users/buttercup/myTA/local/props.confstanza can be added to the user's local context to disable the field aliases?

```
SPLUNK_HOME/etc/apps/myTA/default/props.conf
[mySourcetype]
FIELDALIAS-cim-src_ip = sourceIPAddress as src_ip
FIELDALIAS-cim-dest-ip = destinationIPaddress as dest_ip
```

A.
```
[mySourcetype]
disable FIELDALIAS-cim-src_ip
disable FIELDALIAS-cim-dest-ip
```

B.
```
[mySourcetype]
FIELDALIAS-cim-src_ip =
FIELDALIAS-cim-dest-ip =
```

C.
```
[mySourcetype]
unset FIELDALIAS-cim-src_ip
unset FIELDALIAS-cim-dest-ip
```

D.
```
[mySourcetype]
#FIELDALIAS-cim-src_ip = sourceIPAddress as src_ip
#FIELDALIAS-cim-dest-ip = destinationIPaddress as dest_ip
```

Options:

A- Option A
B- Option B
C- Option C
D- Option D

Answer:

B

Question 2

Question Type: MultipleChoice

In a customer managed Splunk Enterprise environment, what is the endpoint URI used to collect data?

Options:

A- services/ collector
B- services/ inputs ? raw
C- services/ data/ collector
D- data/ collector

Answer:

C

Question 3

Question Type: MultipleChoice

The Splunk administrator wants to ensure data is distributed evenly amongst the indexers. To do this, he runs

the following search over the last 24 hours:

index=*

What field can the administrator check to see the data distribution?

Options:

A- host
B- index
C- linecount
D- splunk_server

Answer:

D

Question 4

Question Type: MultipleChoice

What are the values forhostandindexfor[stanza1]used by Splunk during index time, given the following configuration files?

```
SPLUNK_HOME/etc/system/local/inputs.conf:
 [stanza1]
host=server1

SPLUNK_HOME/etc/apps/search/local/inputs.conf:
 [stanza1]
host=searchsvr1
index=searchinfo

SPLUNK_HOME/etc/apps/search/local/inputs.conf:
 [stanza1]
host=unixsvr1
index=unixinfo
```

Options:

A- host=server1index=unixinfo
B- host=server1index=searchinfo
C- host=searchsvr1index=searchinfo
D- host=unixsvr1index=unixinfo

Answer:

A

Question 5

Question Type: MultipleChoice

Which of the following statements describes how distributed search works?

Options:

A- Forwarders pull data from the search peers.
B- Search heads store a portion of the searchable data.

C- The search head dispatches searches to the search peers.
D- Search results are replicated within the indexer cluster.

Answer:

C

Question 6

Question Type: MultipleChoice

A user is assigned two roles with the following search filters. What is the user's applied search filter?

```
[role_A]
srchFilterSelecting = true
srchFilter = sourcetype!=json AND index=main

[role_B]
srchFilterSelecting = true
srchFilter = sourcetype=csv
```

Options:

A- Option A
B- Option B
C- Option C
D- Option D

Answer:

A

Question 7

Question Type: MultipleChoice

What is the correct example to redact a plain-text password from raw events?

Options:

A- in props.conf:[identity]REGEX-redact_pw = s/password=([^,|/s]+)/ ####REACTED####/g
B- in props.conf:[identity]SEDCMD-redact_pw = s/password=([^,|/s]+)/ ####REACTED####/g
C- in transforms.conf:[identity]SEDCMD-redact_pw = s/password=([^,|/s]+)/ ####REACTED####/g
D- in transforms.conf:[identity]REGEX-redact_pw = s/password=([^,|/s]+)/ ####REACTED####/g

Answer:

B

Question 8

Question Type: MultipleChoice

In this source definition the MAX_TIMESTAMP_LOOKHEAD is missing. Which value would fit best?

```
[sshd_syslog]
TIME_PREFIX = ^
TIME_FORMAT = %Y-%m-%d %H:%M:%S.%3N %z
LINE_BREAKER = ([\r\n]+)\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2}
SHOULD_LINEMERGE = false
TRUNCATE = 0
```

Event example:

```
2018-04-13 13:42:41.214 -0500 server sshd[26219]: Connection from 172.0.2.60 port 47366
```

Options:

A- MAX_TIMESTAMP_L0CKAHEAD = 5
B- MAX_TIMESTAMP_LOOKAHEAD - 10
C- MAX_TIMESTAMF_LOOKHEAD = 20
D- MAX TIMESTAMP LOOKAHEAD - 30

Answer:

D

Question 9

Question Type: MultipleChoice

Which feature of Splunk's role configuration can be used to aggregate multiple roles intended for groups of

users?

Options:

A- Linked roles
B- Grantable roles
C- Role federation
D- Role inheritance

Answer:

D

Question 10

Question Type: MultipleChoice

What options are available when creating custom roles? (select all that apply)

Options:

A- Restrict search terms
B- Whitelist search terms
C- Limit the number of concurrent search jobs
D- Allow or restrict indexes that can be searched.

Answer:

A, C, D