SPLK-1003 Q&As

Splunk Enterprise Certified Admin

Pass Splunk SPLK-1003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/splk-1003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Running this search in a distributed environment:

```
index=aws source=*/AWSLogs/314575187704/elasticloadbalancing/*
| lookup responsible_teams elb OUTPUT team
| eval team=coalesce(team,elb)
| stats sum(received_bytes) sum(sent_bytes) by team
| outputlookup current_prod_account_data
```

On what Splunk component does the eval command get executed?

A. Heavy Forwarders

B. Universal Forwarders

C. Search peers

D. Search heads

Correct Answer: C

The eval command is a distributable streaming command, which means that it can run on the search peers in a distributed environment1. The search peers are the indexers that store the data and perform the initial steps of the search processing2. The eval command calculates an expression and puts the resulting value into a search results field1. In your search, you are using the eval command to create a new field called "responsible_team" based on the values in the "account" field.

QUESTION 2

When are knowledge bundles distributed to search peers?

A. After a user logs in.

B. When Splunk is restarted.

C. When adding a new search peer.

D. When a distributed search is initiated.

Correct Answer: D

"The search head replicates the knowledge bundle periodically in the background or when initiating a search. " "As part of the distributed search process, the search head replicates and distributes its knowledge objects to its search peers, or indexers. Knowledge objects include saved searches, event types, and other entities used in searching accorss indexes. The search head needs to distribute this material to its search peers so that they can properly execute queries on its behalf."

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/DistSearch/Whatsearchheadssend

QUESTION 3

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
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: B

https://docs.splunk.com/Documentation/Splunk/latest/Admin/Howtoeditaconfigurationfile#Clear%20a%20setting

QUESTION 4

Which of the following accurately describes HTTP Event Collector indexer acknowledgement?

A. It requires a separate channel provided by the client.

B. It is configured the same as indexer acknowledgement used to protect in-flight data.

C. It can be enabled at the global setting level.

D. It stores status information on the Splunk server.

Correct Answer: A

https://docs.splunk.com/Documentation/Splunk/8.2.2/Data/AboutHECIDXAck

-Section: About channels and sending data

Sending events to HEC with indexer acknowledgment active is similar to sending them with the setting off. There is one crucial difference: when you have indexer acknowledgment turned on, you must specify a channel when you send

events. The concept of a channel was introduced in HEC primarily to prevent a fast client from impeding the performance of a slow client. When you assign one channel per client, because channels are treated equally on Splunk Enterprise,

one client can\\'t affect another. You must include a matching channel identifier both when sending data to HEC in an HTTP request and when requesting acknowledgment that events contained in the request have been indexed. If you don\\'t,

you will receive the error message, "Data channel is missing." Each request that includes a token for which indexer acknowledgment has been enabled must include a channel identifier, as shown in the following example cURL statement,

where represents the event data portion of the request

QUESTION 5

When configuring monitor inputs with whitelists or blacklists, what is the supported method of filtering the lists?

A. Slash notation

B. Regular expression

C. Irregular expression

D. Wildcard-only expression

Correct Answer: B

https://docs.splunk.com/Documentation/Splunk/latest/Data/Whitelistorblacklistspecificincom
ingdata#Include_or_exclude_specific_incoming_data