SPLK-1003$^{Q\&As}$

Splunk Enterprise Certified Admin

Pass Splunk SPLK-1003 Exam with 100% Guarantee

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

QUESTION 1

The CLI command splunk add forward-server indexer: will create stanza(s) in which configuration file?

A. inputs.conf

B. indexes.conf

C. outputs.conf

D. servers.conf

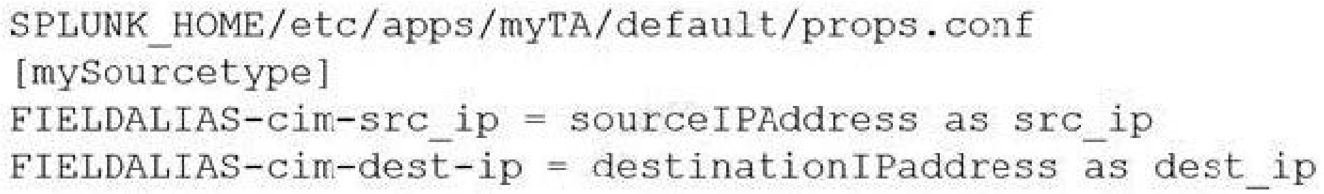
Correct Answer: C

The CLI command "Splunk add forward-server indexer:" is used to define the indexer and the listening port on forwards. The command creates this kind of entry "[tcpout-server://:]" in the outputs.conf file. https://docs.splunk.com/Documentation/Forwarder/8.2.2/Forwarder/Configureforwardingwit houtputs.conf

Reference: https://docs.splunk.com/Documentation/Forwarder/8.0.5/Forwarder/Enableareceiver

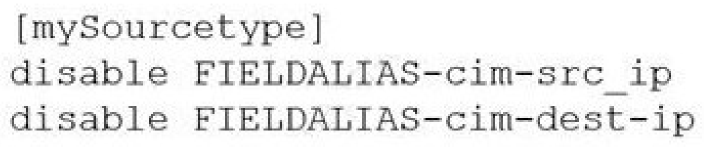
QUESTION 2

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?



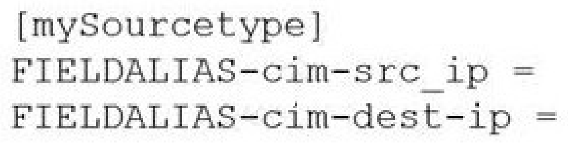
```
SPLUNK_HOME/etc/apps/myTA/default/props.conf
[mySourcetype]
FIELDALIAS-cim-src_ip = sourceIPAddress as src_ip
FIELDALIAS-cim-dest-ip = destinationIPaddress as dest_ip
```

A.



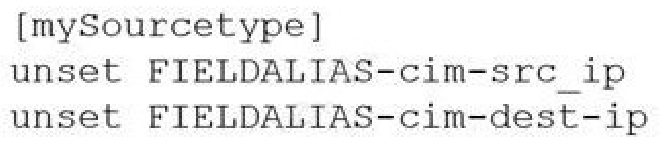
```
[mySourcetype]
disable FIELDALIAS-cim-src_ip
disable FIELDALIAS-cim-dest-ip
```

B.



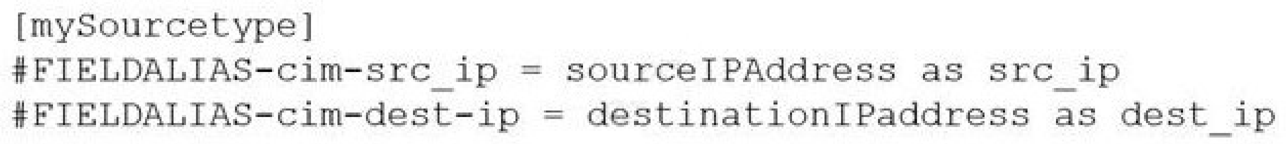
```
[mySourcetype]
FIELDALIAS-cim-src_ip =
FIELDALIAS-cim-dest-ip =
```

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 3

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

A. services/ collector

B. services/ inputs ? raw

C. services/ data/ collector

D. data/ collector

Correct Answer: C

The answer to your question is C. services/data/collector. This is the endpoint URI used to collect data in a customer managed Splunk Enterprise environment.According to the Splunk documentation1, "The HTTP Event Collector REST API

endpoint is /services/data/collector.You can use this endpoint to send events to HTTP Event Collector on a Splunk

Enterprise or Splunk Cloud Platform deployment." You can also use this endpoint to send events to a specific token or index1.

For example, you can use thefollowing curl command to send an event with the token 578254cc-05f5-46b5-957b-910d1400341a and the index main:

curl -k https://localhost:8088/services/data/collector -H\\'Authorization: Splunk 578254cc-05f5-46b5-957b-910d1400341a\\'-d\\'{"index":"main","event":"Hello, world!"}\\'

QUESTION 4

Which of the following applies only to Splunk index data integrity check?

A. Lookup table

B. Summary Index

C. Raw data in the index

D. Data model acceleration

Correct Answer: C

QUESTION 5

What is the command to reset the fishbucket for one source?

A. rm -r ~/splunkforwarder/var/lib/splunk/fishbucket

B. splunk clean eventdata -index _thefishbucket

C. splunk cmd btprobe -d SPLUNK_HOME/var/lib/splunk/fishbucket/splunk_private_db -- file --reset

D. splunk btool fishbucket reset

Correct Answer: C

Reference:https://community.splunk.com/t5/Getting-Data-In/How-can-I-trigger-the-re- indexing-of-a-single-file/m-p/108568

The fishbucket is a directory that stores information about the files that have been monitored and indexed by Splunk. The fishbucket helps Splunk avoid indexing duplicate data by keeping track of file signatures and offsets. To reset the fishbucket for one source, the command splunk cmd btprobe can be used with the -reset option and the name of the source file. Therefore, option C is the correct answer. References: Splunk Enterprise Certified Admin | Splunk, [Use btprobe to troubleshoot file monitoring - Splunk Documentation]