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.geekcert.com/splk-1003.html

100% Passing Guarantee
100% Money Back Assurance

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

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

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 3

Which configuration file would be used to forward the Splunk internal logs from a search head to the indexer?

A. props.conf

B. inputs.conf

C. outputs.conf

D. collections.conf

Correct Answer: C

https://docs.splunk.com/Documentation/Splunk/8.1.1/DistSearch/Forwardsearchheaddata Per the provided Splunk reference URL by @hwangho, scroll to section Forward search head data, subsection titled, 2. Configure the search head as a forwarder. "Create an outputs.conf file on the search head that configures the search head for load-balanced forwarding across the set of search peers (indexers)."

Reference: https://community.splunk.com/t5/Getting-Data-In/How-to-configure-search-head-to-forwardinternal-data-to-the/td-p/111658

QUESTION 4

In a distributed environment, which Splunk component is used to distribute apps and configurations to the other Splunk instances?

A. Indexer

B. Deployer

C. Forwarder

D. Deployment server

Correct Answer: D

The deployer is a Splunk Enterprise instance that you use to distribute apps and certain other configuration updates to search head cluster members. The set of updates that the deployer distributes is called the configuration bundle.

QUESTION 5

Which of the following indexes come pre-configured with Splunk Enterprise? (select all that apply)

A. _license

B. _Internal

C. _external

D. _thefishbucket

Correct Answer: BD

https://docs.splunk.com/Documentation/Splunk/8.0.5/Indexer/Howindexingworks