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

What event-processing pipelines are used to process data for indexing? (select all that apply)

A. fifo pipeline

B. Indexing pipeline

C. Parsing pipeline

D. Typing pipeline

Correct Answer: BC

The indexing pipeline and the parsing pipeline are the two pipelines that are responsible for transforming the raw data into events and preparing them for indexing. The indexing pipeline applies index-time settings, such as timestamp extraction, line breaking, host extraction, and source type recognition. The parsing pipeline applies parsing settings, such as field extraction, event segmentation, and event annotation.

QUESTION 3

Which of the following describes a Splunk deployment server?

A. A Splunk Forwarder that deploys data to multiple indexers.

B. A Splunk app installed on a Splunk Enterprise server.

C. A Splunk Enterprise server that distributes apps.

D. A server that automates the deployment of Splunk Enterprise to remote servers.

Correct Answer: C

A Splunk deployment server is a system that distributes apps, configurations, and other assets to groups of Splunk Enterprise instances. You can use it to distribute updates to most types of Splunk Enterprise components: forwarders, non-

clustered indexers, and search heads.

A Splunk deployment server is available on every full Splunk Enterprise instance. To use it, you must activate it by placing at least one app into %SPLUNK_HOME%\etc\deployment-apps on the host you want to act as deployment server. A

Splunk deployment server maintains the list of server classes and uses those server classes to determine what content to distribute to each client. A server class is a group of deployment clients that share one or more defined characteristics.

A Splunk deployment client is a Splunk instance remotely configured by a deployment server. Deployment clients can be universal forwarders, heavy forwarders, indexers, or search heads. Each deployment client belongs to one or more

server classes.

A Splunk deployment app is a set of content (including configuration files) maintained on the deployment server and deployed as a unit to clients of a server class. A deployment app can be an existing Splunk Enterprise app or one developed

solely to group some content for deployment purposes. Therefore, option C is correct, and the other options are incorrect.

QUESTION 4

What is the default character encoding used by Splunk during the input phase?

A. UTF-8

B. UTF-16

C. EBCDIC

D. ISO 8859

Correct Answer: A

https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/Configurecharactersetencoding

"Configure character set encoding. Splunk software attempts to apply UTF-8 encoding to your scources by default. If a source foesn\\'t use UTF-8 encoding or is a non-ASCII file, Splunk software tries to convert data from the source to UTF-8 encoding unless you specify a character set to use by setting the CHARSET key in the props.conf file."

QUESTION 5

When indexing a data source, which fields are considered metadata?

A. source, host, time

B. time, sourcetype, source

C. host, raw, sourcetype

D. sourcetype, source, host

Correct Answer: D