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.pass4itsure.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

Social Security Numbers (PII) data is found in log events, which is against company policy. SSN format is as follows: 123-44-5678.

Which configuration file and stanza pair will mask possible SSNs in the log events?

A. props.conf [mask-SSN] REX = (?ms)^(.)\\d{3}-?\d{2}-?(\d{4}.*)$" FORMAT = $1###-##-$2 KEY = _raw

B. props.conf [mask-SSN] REGEX = (?ms)^(.)\\d{3}-?\d{2}-?(\d{4}.*)$" FORMAT = $1###-##-$2 DEST_KEY = _raw

C. transforms.conf [mask-SSN] REX = (?ms)^(.)\\d{3}-?\d{2}-?(\d{4}.*)$" FORMAT = $1###-##-$2 DEST_KEY = _raw

D. transforms.conf [mask-SSN] REGEX = (?ms)^(.)\\d{3}-?\d{2}-?(\d{4}.*)$" FORMAT = $1###-##-$2 DEST_KEY = _raw

Correct Answer: D

because transforms.conf is the right configuration file to state the regex expression.https://docs.splunk.com/Documentation/Splunk/8.1.0/Admin/Transformsconf

Reference: https://community.splunk.com/t5/Archive/How-to-mask-SSN-into-our-logs- going-into-Splunk/tdp/433035

QUESTION 2

An admin is running the latest version of Splunk with a 500 GB license. The current daily volume of new data

is 300 GB per day. To minimize license issues, what is the best way to add 10 TB of historical data to the

index?

A. Buy a bigger Splunk license.

B. Add 2.5 TB each day for the next 5 days.

C. Add all 10 TB in a single 24 hour period.

D. Add 200 GB of historical data each day for 50 days.

Correct Answer: C

https://docs.splunk.com/Documentation/Splunk/8.1.2/Admin/Aboutlicenseviolations "An Enterprise license stack with a license volume of 100 GB of data per day or more does not currently violate."

QUESTION 3

Which Splunk component consolidates the individual results and prepares reports in a distributed environment?

A. Indexers

B. Forwarder

C. Search head

D. Search peers

Correct Answer: C

https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/Howuserscancontroldistributedsearches "From the user standpoint, specifying and running a distributed search is essentially the same as running any other search. Behind the scenes, the search head distributes the query to its search peers, and consolidates the results when presenting them to the user."

QUESTION 4

Which of the following statements describes how distributed search works?

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.

Correct Answer: C

"To activate distributed search, you add search peers, or indexers, to a Splunk Enterprise instance that you desingate as a search head. You do this by specifying each search peer manually."

QUESTION 5

Which configuration files are used to transform raw data ingested by Splunk? (Choose all that apply.)

A. props.conf

B. inputs.conf

C. rawdata.conf

D. transforms.conf

Correct Answer: AD

https://docs.splunk.com/Documentation/Splunk/8.1.1/Knowledge/Configureadvancedextrac tionswithfieldtransforms use transformations with props.conf and transforms.conf to: Mask or delete raw data as it is being indexed verride sourcetype or host based upon event values Route events to specific indexes based on event content ?Prevent unwanted events from being indexed

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Data/Configuretimestamprecognition