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

What options are available when creating custom roles? (select all that apply)

A. Restrict search terms

B. Whitelist search terms

C. Limit the number of concurrent search jobs

D. Allow or restrict indexes that can be searched.

Correct Answer: ACD

https://docs.splunk.com/Documentation/SplunkCloud/8.2.2106/Admin/ConcurrentLimits "Set limits for concurrent scheduled searches. You must have the edit_search_concurrency_all and edit_search_concurrency_scheduled capabilities to configure these settings."

QUESTION 2

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

QUESTION 3

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 4

After configuring a universal forwarder to communicate with an indexer, which index can be checked via the Splunk Web UI for a successful connection?

A. index=main

B. index=test

C. index=summary

D. index=_internal

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Security/Validateyourconfiguration

---

QUESTION 5

Which setting allows the configuration of Splunk to allow events to span over more than one line?

A. SHOULD_LINEMERGE = true

B. BREAK_ONLY_BEFORE_DATE = true

C. BREAK_ONLY_BEFORE =

D. SHOULD_LINEMERGE = false

Correct Answer: A

The setting that allows the configuration of Splunk to allow events to span over more than one line is SHOULD_LINEMERGE. This setting determines whether consecutive lines from a single source should be concatenated into a single event. If SHOULD_LINEMERGE is set to true, Splunk will attempt to merge multiple lines into one event based on certain criteria, such as timestamps or regular expressions. Therefore, option A is the correct answer. References: Splunk Enterprise Certified Admin | Splunk, [Configure event line merging - Splunk Documentation]