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

What is the valid option for a [monitor] stanza in inputs.conf?

A. enabled

B. datasource

C. server_name

D. ignoreOlderThan

Correct Answer: D

Setting: ignoreOlderThan = Description: "Causes the input to stop checking files for updates if the file modification time has passed the threshold." Default: 0 (disabled)

QUESTION 2

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]

QUESTION 3

What happens when there are conflicting settings within two or more configuration files?

A. The setting is ignored until conflict is resolved.

B. The setting for both values will be used together.

C. The setting with the lowest precedence is used.

D. The setting with the highest precedence is used.

Correct Answer: D

When there are conflicting settings within two or more configuration files, the setting with the highest precedence is used. The precedence of configuration files is determined by a combination of the file type, the directory location, and the alphabetical order of the file names.

QUESTION 4

All search-time field extractions should be specified on which Splunk component?

A. Deployment server

B. Universal forwarder

C. Indexer

D. Search head

Correct Answer: D

Search-time field extractions are the process of extracting fields from events after they are indexed. Search-time field extractions are specified on the search head, which is the Splunk component that handles searching and reporting. Search-time field extractions are configured in props.conf and transforms.conf files, which are located in the etc/system/local directory on the search head. Therefore, option D is the correct answer. References: Splunk Enterprise Certified Admin | Splunk, [About fields - Splunk Documentation]

QUESTION 5

Which of the following statements describe deployment management? (select all that apply)

A. Requires an Enterprise license

B. Is responsible for sending apps to forwarders.

C. Once used, is the only way to manage forwarders

D. Can automatically restart the host OS running the forwarder.

Correct Answer: AB

https://docs.splunk.com/Documentation/Splunk/8.2.2/Admin/Distdeploylicenses#:~:text=License%20requirements,do%20not%20index%20external%20data.

"All Splunk Enterprise instances functioning as management components needs access to an Enterprise license. Management components include the deployment server, the indexer cluster manager node, the search head cluster deployer, and the monitoring console."

https://docs.splunk.com/Documentation/Splunk/8.2.2/Updating/Aboutdeploymentserver

"The deployment server is the tool for distributing configurations, apps, and content updates to groups of Splunk Enterprise instances."