Study SPLK-1003 Tool | Free SPLK-1003 Practice Exams

What's more, part of that FreeCram SPLK-1003 dumps now are free: https://drive.google.com/open?id=1nyb5JQjrXwTijQCEOSXaJplPYV50GcIC

During the learning process on our SPLK-1003 study materials, you can contact us anytime if you encounter any problems. The staff of SPLK-1003 actual exam will be online 24 hours, hoping to solve the problem in time for you. You can contact our services via email or online, as long as you leave your message, our services will give you suggestions right away. And even you have problem when you already bought our SPLK-1003 learning guide, we will still help you solve it.

Splunk SPLK-1003 Exam Overview

The professionals aiming to gain and verify all the skills needed to manage Splunk Enterprise expertly should consider passing the Splunk Enterprise Certified Admin exam or SPLK-1003 by code and earning a corresponding certification. With it, one proves expertise in using Splunk software that gives a highly innovative end-to-end user experience which makes it more functional for business operations.

>> Study SPLK-1003 Tool <<

Free SPLK-1003 Practice Exams - Official SPLK-1003 Practice Test

People need to increase their level by getting the Splunk SPLK-1003 certification. If you take an example of the present scenario in this competitive world, you will find people struggling to meet their ends just because they are surviving on low-scale salaries. Even if they are thinking about changing their jobs, people who are ready with a better skill set or have prepared themselves with Splunk SPLK-1003 Certification grab the chance. This leaves them in the same place where they were.

To take the Splunk SPLK-1003 Exam, candidates must have a solid understanding of Splunk Enterprise and its various components. They must also have hands-on experience in managing and administering Splunk Enterprise. Candidates must be able to configure and manage data inputs, create and manage knowledge objects, and troubleshoot issues that may arise during the deployment and administration of Splunk Enterprise.

Splunk Enterprise Certified Admin Sample Questions (Q61-Q66):

NEW QUESTION # 61
What options are available when creating custom roles? (select all that apply)

- A. Allow or restrict indexes that can be searched.
- B. Limit the number of concurrent search jobs
- C. Whitelist search terms
- D. Restrict search terms

Answer: A,B,D

Explanation:

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."

NEW QUESTION # 62
A security team needs to ingest a static file for a specific incident. The log file has not been collected previously and future updates to the file must not be indexed.
Which command would meet these needs?

- A. splunk add one shot / opt/ incident [data .log -index incident
- B. splunk add monitor /opt/incident/data.log -index incident
- C. splunk edit oneshot [opt/ incident/data.* -index incident
- D. splunk edit monitor /opt/incident/data.* -index incident

Answer: A

Explanation:
The correct answer is A. splunk add one shot / opt/ incident [data . log -index incident According to the Splunk documentation1, the splunk add one shot command adds a single file or directory to the Splunk index and then stops monitoring it. This is useful for ingesting static files that do not change or update. The command takes the following syntax:
splunk add one shot <file> -index <index_name>
The file parameter specifies the path to the file or directory to be indexed. The index parameter specifies the name of the index where the data will be stored. If the index does not exist, Splunk will create it automatically.
Option B is incorrect because the splunk edit monitor command modifies an existing monitor input, which is used for ingesting files or directories that change or update over time. This command does not create a new monitor input, nor does it stop monitoring after indexing.
Option C is incorrect because the splunk add monitor command creates a new monitor input, which is also used for ingesting files or directories that change or update over time. This command does not stop monitoring after indexing.
Option D is incorrect because the splunk edit oneshot command does not exist. There is no such command in the Splunk CLI.
References: 1: Monitor files and directories with inputs.conf - Splunk Documentation

NEW QUESTION # 63
What conf file needs to be edited to set up distributed search groups?

- A. props.conf
- B. distsearch.conf
- C. distibutedsearch.conf
- D. search.conf

Answer: B

Explanation:
Explanation
"You can group your search peers to facilitate searching on a subset of them. Groups of search peers are known as "distributed search groups." You specify distributed search groups in the distsearch.conf file"

NEW QUESTION # 64
Using SEDCMD in props.conf allows raw data to be modified. With the given event below, which option will mask the first three digits of the AcctID field resulting output: [22/Oct/2018:15:50:21] VendorID=1234 Code=B AcctID=xxx5309 Event: [22/Oct/2018:15:50:21] VendorID=1234 Code=B AcctID=xxx5309

- A. SEDCMD-xxxAcct = s/AcctID=\d{3}(\d{4})/AcctID=xxx/g
- B. SEDCMD-1acct = s/AcctID=\d{3}(\d{4})/AcctID=\1xxx/g
- C. SEDCMD-1acct = s/AcctID=\d{3}(\d{4})/AcctID=xxx\1/g
- D. SEDCMD-1acct = s/VendorID=\d{3}(\d{4})/VendorID=xxx/g

Answer: B

NEW QUESTION # 65
When running a real-time search, search results are pulled from which Splunk component?

- A. Heavy forwarders
- B. Search peers
- C. Search heads
- D. Heavy forwarders and search peers

Answer: B

Explanation:
Using the Splunk reference URL https://docs.splunk.com/Splexicon:Searchpeer
"search peer is a splunk platform instance that responds to search requests from a search head. The term "search peer" is usally synonymous with the indexer role in a distributed search topology. However, other instance types also have access to indexed data, particularly internal diagnostic data, and thus function as search peers when they respond to search requests for that data."

NEW QUESTION # 66
.....