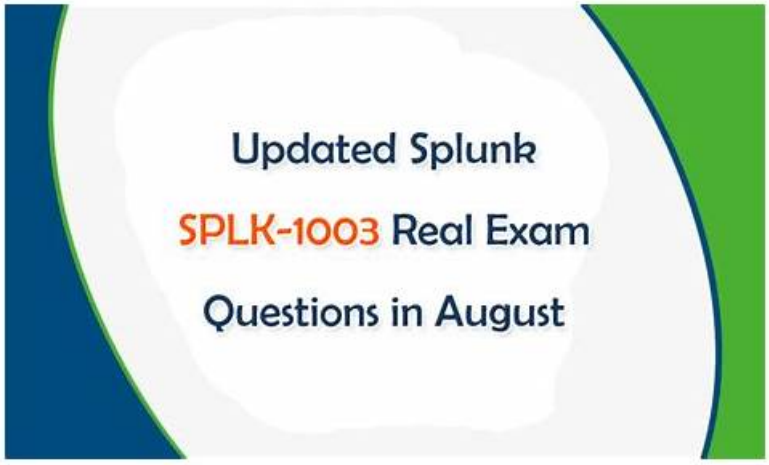
Valid Reliable SPLK-1003 Test Sims Help You to Get Acquainted with Real SPLK-1003 Exam Simulation



What's more, part of that ExamTorrent SPLK-1003 dumps now are free: https://drive.google.com/open?id=1ppkCtTGoZRBZlCC0oG-5oHFuaZlCCV_g

You can use this SPLK-1003 simulation software without an internet connection after installation. Tracking and reporting features of our Splunk SPLK-1003 practice exam software makes it easier for you to identify and overcome mistakes. Customization feature of this format allows you to change time limits and questions numbers of mock exams.

Splunk SPLK-1003 Exam Syllabus Topics:

Topic	Details
Topic 1	• Getting Data In: This domain addresses the responsibilities of Splunk Administrators in configuring data inputs, differentiating forwarder types, and using the command-line interface for setting up Universal Forwarders.
Topic 2	• Parsing Phase and Data: Security Operations Engineers are tested on their understanding of event parsing, timestamp recognition, and the use of data preview tools to verify data correctness prior to indexing.
Topic 3	• Manipulating Raw Data: Aimed at Splunk Administrators, this section covers using configuration files to mask, re-route, or suppress data at index time using props.conf, transforms.conf, and SEDCMD.
Topic 4	• Agentless Inputs: Designed for Security Operations Engineers, this section covers creating agentless inputs using WMI and HTTP Event Collector (HEC), particularly for integrating data from Windows and RESTful sources.
Topic 5	• Configuring Forwarders: Splunk Administrators are assessed on the deployment and configuration of forwarders, along with recognition of additional forwarder functionalities essential for scalable data ingestion.
Topic 6	• Splunk Admin Basics: This section evaluates the foundational knowledge required of a Splunk Administrator, focusing on identifying core components such as indexers, search heads, and forwarders within a Splunk deployment.
Topic 7	• Splunk Indexes: Relevant to Splunk Administrators, this section covers the structure and types of index buckets, data retention policies, integrity checks, and the role of the fishbucket in tracking file inputs.
Topic 8	• Forwarder Management: This section, intended for Splunk Administrators, tests the candidate's understanding of deployment servers, forwarder apps, client group management, and monitoring forwarder activities across distributed environments.

Topic 9	• Splunk Authentication Management: This domain is intended for Security Operations Engineers and involves integrating LDAP directories, implementing multi-factor authentication, and exploring other authentication mechanisms within Splunk.
Topic 10	• Fine Tuning Inputs: Splunk Administrators are evaluated on their ability to customise input processing, including sourcetype identification, character encoding, and other configurations for accurate data onboarding.
Topic 11	• Getting Data In – Staging: This section is relevant to Splunk Administrators and focuses on the three stages of data indexing—input, parsing, and indexing—and outlines data ingestion options and configurations.
Topic 12	• Splunk User Management: Aimed at Splunk Administrators, this area focuses on user account creation, role-based access controls, and custom role development to maintain a secure and organised user environment.
Topic 13	• License Management: Designed for Splunk Administrators, this domain addresses types of Splunk licenses, how to manage them effectively, and the implications of license violations on operational continuity.
Topic 14	• Network and Scripted Inputs: Security Operations Engineers are assessed on setting up and customising TCP and UDP network inputs, as well as implementing basic scripted inputs for dynamic data ingestion.
Topic 15	• Monitor Inputs: Targeted at Splunk Administrators, this domain involves creating and customising monitor inputs for files and directories, including the deployment of remote monitors.
Topic 16	• Distributed Search: Security Operations Engineers are assessed on their understanding of distributed search architecture, including search head and peer roles, and how to configure and manage search groups.

100% Pass Quiz 2026 SPLK-1003: Newest Reliable Splunk Enterprise Certified Admin Test Sims

Of course, when we review a qualifying exam, we can't be closed-door. We should pay attention to the new policies and information related to the test SPLK-1003 certification. For the convenience of the users, the SPLK-1003 test materials will be updated on the homepage and timely update the information related to the qualification examination. Annual qualification examination, although content broadly may be the same, but as the policy of each year, the corresponding examination pattern grading standards and hot spots will be changed, the SPLK-1003 Test Prep can help users to spend the least time to pass the exam.

Splunk Enterprise Certified Admin Sample Questions (Q12-Q17):

NEW QUESTION # 12
Which of the following authentication types requires scripting in Splunk?

- A. ADFS
- B. SAML
- C. LDAP
- D. RADIUS

Answer: D

Explanation:
https://answers.splunk.com/answers/131127/scripted-authentication.html
Scripted Authentication: An option for Splunk Enterprise authentication. You can use an authentication system that you have in place (such as PAM or RADIUS) by configuring authentication.conf to use a script instead of using LDAP or Splunk Enterprise default authentication.

NEW QUESTION # 13
The following stanza is active in indexes.conf:
[cat_facts]
maxHotSpanSecs = 3600
frozenTimePeriodInSecs = 2630000
maxTota1DataSizeMB = 650000
All other related indexes.conf settings are default values.
If the event timestamp was 3739283 seconds ago, will it be searchable?

- A. Yes, only if the index size is also below 650000 MB.
- B. No, because the event time is greater than the retention time.
- C. Yes, only if the bucket is still hot.
- D. No, because the index will have exceeded its maximum size.

Answer: B

Explanation:
The correct answer is D. No, because the event time is greater than the retention time.
According to the Splunk documentation1, the frozenTimePeriodInSecs setting in indexes.conf determines how long Splunk software retains indexed data before deleting it or archiving it to a remote storage. The default value is 188697600 seconds, which is equivalent to six years. The setting can be overridden on a per- index basis.
In this case, the cat_facts index has a frozenTimePeriodInSecs setting of 2630000 seconds, which is equivalent to about 30 days. This means that any event that is older than 30 days from the current time will be removed from the index and will not be searchable. The event timestamp was 3739283 seconds ago, which is equivalent to about 43 days. This means that the event is older than the retention time of the cat_facts index and will not be searchable.
The other settings in the stanza, such as maxHotSpanSecs and maxTota1DataSizeMB, do not affect the retention time of the events. They only affect the size and duration of the buckets that store the events.
References: 1: Set a retirement and archiving policy - Splunk Documentation

NEW QUESTION # 14
Which of the following lists the three phases of the Splunk Indexing process in order?

- A. Ingest phaseLicensing phaseParsing phase
- B. Sourcetype phaseIndex phaseWrite-to-disk phase
- C. Ingest phaseTransforming phaseIndexing phase
- D. Input phaseParsing phaseIndexing phase

Answer: D

Explanation:
The Splunk indexing process consists of three main phases: Input, Parsing, and Indexing. Understanding these phases is crucial for configuring data inputs and managing data flow within Splunk.
* Input Phase: Splunk receives data from various sources, such as files, network ports, or scripted inputs.
* Parsing Phase: Splunk breaks the data into individual events, applies transformations, and extracts timestamps.
* Indexing Phase: Splunk writes the parsed events to disk and creates indexes for efficient searching.
From the official Splunk documentation:
"The data pipeline consists of three main phases: input, parsing, and indexing."
- How the Splunk platform indexes data - Splunk Documentation
Therefore, the correct order of the indexing process is: Input phase # Parsing phase # Indexing phase.
Reference:
How the Splunk platform indexes data - Splunk Documentation

NEW QUESTION # 15
Where should apps be located on the deployment server that the clients pull from?

- A. $SPLUNK HCME/etc/deployment-apps
- B. $SPLUNK_HCME/etc/master-apps
- C. $SPLUNK_HCME/etc/sear:ch
- D. $SFLUNK_KOME/etc/apps

Answer: A

NEW QUESTION # 16
Where can scripts for scripted inputs reside on the host file system? (select all that apply)

- A. $SPLUNK_HOME/etc/system/bin
- B. $SPLUNK_HOME/etc/apps/bin
- C. $S?LUNK_HOME/etc/apps/<your_app>/bin_
- D. $SFLUNK_HOME/bin/scripts

Answer: A,C,D

NEW QUESTION # 17
.....

Our SPLK-1003 exam questions have been widely acclaimed among our customers, and the good reputation in industry prove that choosing our study materials would be the best way for you, and help you gain the SPLK-1003 certification successfully. With about ten years' research and development we still keep updating our SPLK-1003 Prep Guide, in order to grasp knowledge points in accordance with the exam, thus your study process would targeted and efficient.