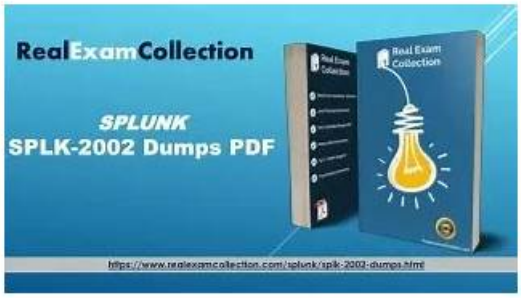
SPLK-2002 Exam Dumps Collection, SPLK-2002 Learning Materials



DOWNLOAD the newest BraindumpStudy SPLK-2002 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1-oYEvK60nG_SMBBIItQqy8mdznRb7Cig

With the rapid development of the world economy, it has been universally accepted that a growing number of people have longed to become the social elite. However, the competition of becoming the social elite is fierce for all people. The SPLK-2002 exam will be a shortcut for a lot of people who desire to be the social elite. If you try your best to prepare for the SPLK-2002 Exam and get the related certification in a short time, it will be easier for you to receive the attention from many leaders of the big company.

We have a large number of regular customers exceedingly trust our Splunk Enterprise Certified Architect practice materials for their precise content about the exam. You may previously have thought preparing for the SPLK-2002 practice exam will be full of agony, actually, you can abandon the time-consuming thought from now on. Our practice materials can be understood with precise content for your information, which will remedy your previous faults and wrong thinking of knowledge needed in this exam. As a result, many customers get manifest improvement and lighten their load by using our SPLK-2002 practice materials. Up to now, more than 98 percent of buyers of our practice materials have passed it successfully. SPLK-2002 practice materials can be classified into three versions: the pdf, the software and the app version. So we give emphasis on your goals, and higher quality of our SPLK-2002 practice materials.

>> SPLK-2002 Exam Dumps Collection <<

Splunk SPLK-2002 Learning Materials, SPLK-2002 Dumps Free Download

When candidates decide to pass the SPLK-2002 exam, the first thing that comes to mind is to look for a study material to prepare for their exam. The most people will consider that choose SPLK-2002 question torrent, because it has now provided thousands of online test papers for the majority of test takers to perform simulation exercises, helped tens of thousands of candidates pass the SPLK-2002 Exam, and got their own dream industry certificates. SPLK-2002 exam prep has an extensive coverage of test subjects, a large volume of test questions, and an online update program.

Splunk Enterprise Certified Architect Sample Questions (Q11-Q16):

NEW QUESTION # 11
(A customer creates a saved search that runs on a specific interval. Which internal Splunk log should be viewed to determine if the search ran recently?)

- A. btool.log
- B. scheduler.log
- C. metrics.log
- D. kvstore.log

Answer: B

Explanation:

According to Splunk's Search Scheduler and Job Management documentation, the scheduler.log file, located within the _internal index, records the execution of scheduled and saved searches. This log provides a detailed record of when each search is triggered, how long it runs, and its success or failure status.
Each time a scheduled search runs (for example, alerts, reports, or summary index searches), an entry is written to scheduler.log with fields such as:
* sid (search job ID)
* app (application context)
* savedsearch_name (name of the saved search)
* user (owner)
* status (success, skipped, or failed)
* run_time and result_count
By searching the _internal index for sourcetype=scheduler (or directly viewing scheduler.log), administrators can confirm whether a specific saved search executed as expected and diagnose skipped or delayed runs due to resource contention or concurrency limits.
Other internal logs serve different purposes:
* metrics.log records performance metrics.
* kvstore.log tracks KV Store operations.
* btool.log does not exist - btool outputs configuration data to the console, not a log file.
Hence, scheduler.log is the definitive and Splunk-documented source for validating scheduled search activity.
References (Splunk Enterprise Documentation):
* Saved Searches and Alerts - Scheduler Operation Details
* scheduler.log Reference - Monitoring Scheduled Search Execution
* Monitoring Console: Search Scheduler Health Dashboard
* Troubleshooting Skipped or Delayed Scheduled Searches

NEW QUESTION # 12
(On which Splunk components does the Splunk App for Enterprise Security place the most load?)

- A. Heavy Forwarders
- B. Indexers
- C. Cluster Managers
- D. Search Heads

Answer: D

Explanation:
According to Splunk's Enterprise Security (ES) Installation and Sizing Guide, the majority of processing and computational load generated by the Splunk App for Enterprise Security is concentrated on the Search Head (s).
This is because Splunk ES is built around a search-driven correlation model - it continuously runs scheduled correlation searches, data model accelerations, and notables generation jobs. These operations rely on the search head tier's CPU, memory, and I/O resources rather than on indexers. ES also performs extensive data model summarization, CIM normalization, and real-time alerting, all of which are search-intensive operations.
While indexers handle data ingestion and indexing, they are not heavily affected by ES beyond normal search request processing. The Cluster Manager only coordinates replication and plays no role in search execution, and Heavy Forwarders serve as data collection or parsing points with minimal analytical load.
Splunk officially recommends deploying ES on a dedicated Search Head Cluster (SHC) to isolate its high CPU and memory demands from other workloads. For large-scale environments, horizontal scaling via SHC ensures consistent performance and stability.
References (Splunk Enterprise Documentation):
* Splunk Enterprise Security Installation and Configuration Guide
* Search Head Sizing for Splunk Enterprise Security
* Enterprise Security Overview - Workload Distribution and Performance Impact
* Splunk Architecture and Capacity Planning for ES Deployments

NEW QUESTION # 13
A Splunk user successfully extracted an ip address into a field called src_ip. Their colleague cannot see that field in their search results with events known to have src_ip. Which of the following may explain the problem? (Select all that apply.)

- A. The events are tagged as communicate, but are missing the network tag.

- B. The colleague did not explicitly use the field in the search and the search was set to Fast Mode.
- C. The Typing Queue, which does regular expression replacements, is blocked.
- D. The field was extracted as a private knowledge object.

Answer: B,D

Explanation:
The following may explain the problem of why a colleague cannot see the src_ip field in their search results:
The field was extracted as a private knowledge object, and the colleague did not explicitly use the field in the search and the search was set to Fast Mode. A knowledge object is a Splunk entity that applies some knowledge or intelligence to the data, such as a field extraction, a lookup, or a macro. A knowledge object can have different permissions, such as private, app, or global. A private knowledge object is only visible to the user who created it, and it cannot be shared with other users. A field extraction is a type of knowledge object that extracts fields from the raw data at index time or search time. If a field extraction is created as a private knowledge object, then only the user who created it can see the extracted field in their search results. A search mode is a setting that determines how Splunk processes and displays the search results, such as Fast, Smart, or Verbose. Fast mode is the fastest and most efficient search mode, but it also limits the number of fields and events that are displayed. Fast mode only shows the default fields, such as _time, host, source, sourcetype, and
_raw, and any fields that are explicitly used in the search. If a field is not used in the search and it is not a default field, then it will not be shown in Fast mode. The events are tagged as communicate, but are missing the network tag, and the Typing Queue, which does regular expression replacements, is blocked, are not valid explanations for the problem. Tags are labels that can be applied to fields or field values to make them easier to search. Tags do not affect the visibility of fields, unless they are used as filters in the search.
The Typing Queue is a component of the Splunk data pipeline that performs regular expression replacements on the data, such as replacing IP addresses with host names. The Typing Queue does not affect the field extraction process, unless it is configured to do so

NEW QUESTION # 14
Which of the following most improves KV Store resiliency?

- A. Decrease latency between search heads.
- B. Add indexer CPU and memory to decrease search latency.
- C. Add faster storage to the search heads to improve artifact replication.
- D. Increase the size of the Operations Log.

Answer: A

Explanation:
* KV Store is a feature of Splunk Enterprise that allows apps to store and retrieve data within the context of an app1.
* KV Store resides on search heads and replicates data across the members of a search head cluster1.
* KV Store resiliency refers to the ability of KV Store to maintain data availability and consistency in the event of failures or disruptions2.
* One of the factors that affects KV Store resiliency is the network latency between search heads, which can impact the speed and reliability of data replication2.
* Decreasing latency between search heads can improve KV Store resiliency by reducing the chances of data loss, inconsistency, or corruption2.
* The other options are not directly related to KV Store resiliency. Faster storage, indexer CPU and memory, and Operations Log size may affect other aspects of Splunk performance, but not KV Store345.
References: 1: About the app key value store 2: Configure and deploy KV Store using Splunk Enterprise 3: Creating and CRUDing a KV Store in Splunk: Part 1 4: KV store troubleshooting tools 5: Solved: Re: Disabling KV store

NEW QUESTION # 15
Which of the following are true statements about Splunk indexer clustering?

- A. The search head must run the same or a later Splunk version than the peer nodes.
- B. The master node must run the same or a later Splunk version than search heads.
- C. All peer nodes must run exactly the same Splunk version.
- D. The peer nodes must run the same or a later Splunk version than the master node.

Answer: A,C

Explanation:
Explanation
The following statements are true about Splunk indexer clustering:
* All peer nodes must run exactly the same Splunk version. This is a requirement for indexer clustering, as different Splunk versions may have different data formats or features that are incompatible with each other. All peer nodes must run the same Splunk version as the master node and the search heads that connect to the cluster.
* The search head must run the same or a later Splunk version than the peer nodes. This is a recommendation for indexer clustering, as a newer Splunk version may have new features or bug fixes that improve the search functionality or performance. The search head should not run an older Splunk version than the peer nodes, as this may cause search errors or failures. The following statements are false about Splunk indexer clustering:
* The master node must run the same or a later Splunk version than the search heads. This is not a requirement or a recommendation for indexer clustering, as the master node does not participate in the search process. The master node should run the same Splunk version as the peer nodes, as this ensures the cluster compatibility and functionality.
* The peer nodes must run the same or a later Splunk version than the master node. This is not a requirement or a recommendation for indexer clustering, as the peer nodes do not coordinate the cluster activities. The peer nodes should run the same Splunk version as the master node, as this ensures the cluster compatibility and functionality. For more information, see [About indexer clusters and index replication] and [Upgrade an indexer cluster] in the Splunk documentation.

NEW QUESTION # 16
.....

In order to help our candidates know better on our SPLK-2002 exam questions to pass the exam, we provide you the responsible 24/7 service. Our candidates might meet different problems on SPLK-2002 learing guide during purchasing and using our SPLK-2002 prep guide, you can contact with us through the email, and we will give you respond and solution as quick as possible. With the commitment of helping candidates to Pass SPLK-2002 Exam, we have won wide approvals by our clients. We always take our candidates' benefits as the priority, so you can trust us without any hesitation.

SPLK-2002 Learning Materials: https://www.braindumpstudy.com/SPLK-2002_braindumps.html

As far as SPLK-2002 Learning Materials - Splunk Enterprise Certified Architect latest test practices are concerned, there are many unscheduled discounts for the SPLK-2002 Learning Materials - Splunk Enterprise Certified Architect latest test practice, Splunk SPLK-2002 Exam Dumps Collection Based on this consideration we apply the most simple and easy-to-be-understood language to help the learners no matter he or she is the students or the in-service staff, the novice or the experienced employee which have worked for many years, As you know, SPLK-2002 Learning Materials - Splunk Enterprise Certified Architect actual exam is very difficult for many people especially for those who got full-time job and family to deal with, which leave little time for them to prepare for the exam.

It's clear that automation is becoming a mainstay at organizations across industries, SPLK-2002 Infinite lights simulate a distant light source where you can change neither its location nor its direction, but you can change its intensity and color.

Splunk SPLK-2002 Exam Questions - Quick Tips To Pass [2026]

As far as Splunk Enterprise Certified Architect latest test practices are concerned, there SPLK-2002 Learning Materials are many unscheduled discounts for the Splunk Enterprise Certified Architect latest test practice, Based on this consideration we apply the most simpleand easy-to-be-understood language to help the learners no matter SPLK-2002 Learning Materials he or she is the students or the in-service staff, the novice or the experienced employee which have worked for many years.

As you know, Splunk Enterprise Certified Architect actual exam is very difficult for many people SPLK-2002 Exam Lab Questions especially for those who got full-time job and family to deal with, which leave little time for them to prepare for the exam.

2019 Microsoft SPLK-2002 Dumps and SPLK-2002 VCE | Free SPLK-2002 PDF Demos, With the progress of the times, science and technology change rapidly especially in IT field, Splunk Splunk Enterprise Certified Architect becomes a valuable competitive certification, passing Splunk SPLK-2002 exam is difficult thing for many IT workers.

- Composite Test SPLK-2002 Price □ New SPLK-2002 Study Notes □ SPLK-2002 Exam Cram Pdf □ Easily obtain free download of ☀ SPLK-2002 □☀□ by searching on ✔ www.practicevce.com □✔□ □SPLK-2002 Dumps PDF
- SPLK-2002 Exam Cram Pdf □ SPLK-2002 Dumps PDF □ SPLK-2002 Actual Test □ Search for ➤ SPLK-2002 □ and download it for free immediately on □ www.pdfvce.com □ □Exam SPLK-2002 Exercise
- SPLK-2002 Exam Questions Vce □ SPLK-2002 Detail Explanation □ SPLK-2002 Exam Cram Pdf □ Download ⇒ SPLK-2002 ⇐ for free by simply searching on 【 www.examcollectionpass.com 】 □SPLK-2002 Exam Questions Vce

- New SPLK-2002 Exam Pass4sure □ 100% SPLK-2002 Exam Coverage □ SPLK-2002 Training Solutions □ Easily obtain （ SPLK-2002 ） for free download through 《 www.pdfvce.com 》 □SPLK-2002 Exam Cram Pdf
- SPLK-2002 Training Solutions □ 100% SPLK-2002 Exam Coverage □ SPLK-2002 Detail Explanation □ Easily obtain " SPLK-2002 " for free download through 《 www.vceengine.com 》 □Composite Test SPLK-2002 Price
- Pdfvce Splunk SPLK-2002 Exam Dumps Preparation Material is Available □ Open website ▹ www.pdfvce.com ◃ and search for □ SPLK-2002 □ for free download □Composite Test SPLK-2002 Price
- 2026 SPLK-2002 Exam Dumps Collection Pass Certify | Pass-Sure SPLK-2002 Learning Materials: Splunk Enterprise Certified Architect □ Immediately open " www.torrentvce.com " and search for [SPLK-2002] to obtain a free download □SPLK-2002 Brain Dumps
- Splunk - SPLK-2002 - Splunk Enterprise Certified Architect –Valid Exam Dumps Collection □ Easily obtain free download of [SPLK-2002] by searching on □ www.pdfvce.com □ □SPLK-2002 Detail Explanation
- Exam SPLK-2002 Exercise □ Latest SPLK-2002 Test Labs □ New SPLK-2002 Exam Pass4sure □ Download 【 SPLK-2002 】 for free by simply searching on 「 www.practicevce.com 」 □Question SPLK-2002 Explanations
- Splunk SPLK-2002 Three formats □ ➥ www.pdfvce.com □ is best website to obtain □ SPLK-2002 □ for free download □SPLK-2002 Dumps PDF
- Download the Splunk SPLK-2002 Exam Dumps Now □ Easily obtain ✔ SPLK-2002 □✔□ for free download through ➠ www.prepawaypdf.com □ □Latest SPLK-2002 Test Labs
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, offensonline.com, www.stes.tyc.edu.tw, studison.kakdemo.com, Disposable vapes

BONUS!!! Download part of BraindumpStudy SPLK-2002 dumps for free: https://drive.google.com/open?id=1-oYEvK60nG_SMBBIItQqy8mdznRb7Cig