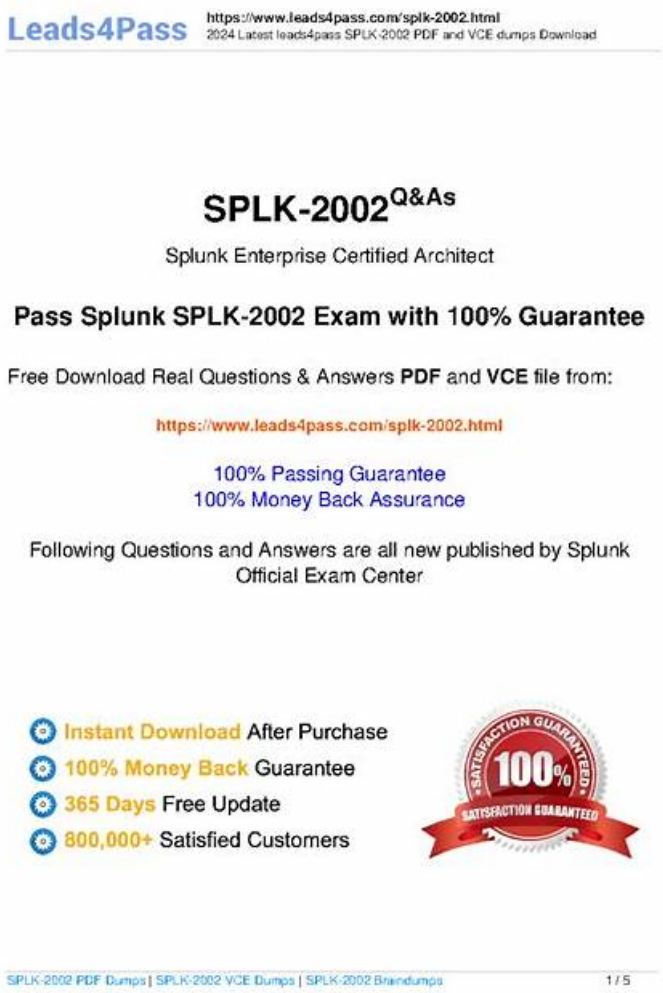
Latest SPLK-2002 Exam Pattern & SPLK-2002 Exam Review



P.S. Free 2026 Splunk SPLK-2002 dumps are available on Google Drive shared by Actual4dump: https://drive.google.com/open?id=1Ndfl2tjs-h9My-PWvayRBW2qFb5cslkN

You may be busy in your jobs, learning or family lives and can't get around to preparing and takes the certificate exams but on the other side you urgently need some useful SPLK-2002 certificates to improve your abilities in some areas. If you choose the test SPLK-2002 certification and then buy our SPLK-2002 prep material you will get the panacea to both get the useful SPLK-2002 certificate and spend little time. Passing the SPLK-2002 test certification can help you stand out in your colleagues and have a bright future in your career.

Splunk Enterprise Certified Architect (SPLK-2002) certification exam is an important credential for experienced Splunk professionals who want to demonstrate their mastery of the platform's architecture and deployment. SPLK-2002 exam covers a broad range of topics and requires significant preparation to pass. However, the rewards of earning the certification include increased job opportunities, higher salaries, and recognition as a leader in the field of Splunk architecture and deployment.

Splunk SPLK-2002 Certification Exam is a valuable certification for experienced Splunk professionals who want to demonstrate their skills in designing and deploying Splunk Enterprise environments. Splunk Enterprise Certified Architect certification is highly regarded in the technology industry and is recognized globally. Candidates can prepare for the exam by taking official training courses, practice exams, and study guides available online.

>> Latest SPLK-2002 Exam Pattern <<

SPLK-2002 Exam Review - SPLK-2002 Practice Test Fee

Our SPLK-2002 exam guide has high quality of service. We provide 24-hour online service on the SPLK-2002 training engine. If you have any questions in the course of using the bank, you can contact us by email. We will provide you with excellent after-sales service with the utmost patience and attitude. And we will give you detailed solutions to any problems that arise during the course of using the SPLK-2002 learning braindumps. And our SPLK-2002 study materials welcome your supervision and criticism.

Splunk SPLK-2002 (Splunk Enterprise Certified Architect) Certification Exam is a professional certification that is designed to validate an individual's knowledge and skills in the area of Splunk Enterprise architecture. SPLK-2002 exam is intended for experienced Splunk professionals who are responsible for designing and deploying Splunk Enterprise solutions in complex environments. Splunk Enterprise Certified Architect certification is highly regarded and recognized by the industry, and it is an excellent way for professionals to showcase their Splunk expertise and advance their careers.

Splunk Enterprise Certified Architect Sample Questions (Q21-Q26):

NEW QUESTION # 21
In a distributed environment, knowledge object bundles are replicated from the search head to which location on the search peer(s)?

- A. SPLUNK_HOME/var/run/searchpeers
- B. SPLUNK_HOME/var/lib/searchpeers
- C. SPLUNK_HOME/var/log/searchpeers
- D. SPLUNK_HOME/var/spool/searchpeers

Answer: A

NEW QUESTION # 22
How can internal logging levels in a Splunk environment be changed to troubleshoot an issue? (select all that apply)

- A. Use Splunk command line.
- B. Edit log-local. cfg.
- C. Use Splunk Web.
- D. Use the Monitoring Console (MC).

Answer: A,B,C,D

Explanation:
Splunk provides various methods to change the internal logging levels in a Splunk environment to troubleshoot an issue. All of the options are valid ways to do so. Option A is correct because the Monitoring Console (MC) allows the administrator to view and modify the logging levels of various Splunk components through a graphical interface. Option B is correct because the Splunk command line provides the splunk set log-level command to change the logging levels of specific components or categories. Option C is correct because the Splunk Web provides the Settings > Server settings > Server logging page to change the logging levels of various components through a web interface. Option D is correct because the log-local.cfg file allows the administrator to manually edit the logging levels of various components by overriding the default settings in the log.cfg file123
1: https://docs.splunk.com/Documentation/Splunk/9.1.2/Troubleshooting/Enabledebuglogging 2: https://docs.splunk.com/Documentation/Splunk/9.1.2/Admin/Serverlogging 3: https://docs.splunk.com/Documentation/Splunk/9.1.2/Admin/Loglocalcfg

NEW QUESTION # 23
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 field was extracted as a private knowledge object.
- B. The Typing Queue, which does regular expression replacements, is blocked.
- C. The colleague did not explicitly use the field in the search and the search was set to Fast Mode.
- D. The events are tagged as communicate, but are missing the network tag.

Answer: A,C

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 # 24
Several critical searches that were functioning correctly yesterday are not finding a lookup table today. Which log file would be the best place to start troubleshooting?

- A. health.log
- B. web_access.log
- C. configuration_change.log
- D. btool.log

Answer: B

Explanation:
A lookup table is a file that contains a list of values that can be used to enrich or modify the data during search time1. Lookup tables can be stored in CSV files or in the KV Store1. Troubleshooting lookup tables involves identifying and resolving issues that prevent the lookup tables from being accessed, updated, or applied correctly by the Splunk searches. Some of the tools and methods that can help with troubleshooting lookup tables are:
* web_access.log: This is a file that contains information about the HTTP requests and responses that occur between the Splunk web server and the clients2. This file can help troubleshoot issues related to lookup table permissions, availability, and errors, such as 404 Not Found, 403 Forbidden, or 500 Internal Server Error34.
* btool output: This is a command-line tool that displays the effective configuration settings for a given Splunk component, such as inputs, outputs, indexes, props, and so on5. This tool can help troubleshoot issues related to lookup table definitions, locations, and precedence, as well as identify the source of a configuration setting6.
* search.log: This is a file that contains detailed information about the execution of a search, such as the search pipeline, the search commands, the search results, the search errors, and the search performance.
This file can help troubleshoot issues related to lookup table commands, arguments, fields, and outputs,
* such as lookup, inputlookup, outputlookup, lookup_editor, and so on .
Option B is the correct answer because web_access.log is the best place to start troubleshooting lookup table issues, as it can provide the most relevant and immediate information about the lookup table access and status.
Option A is incorrect because btool output is not a log file, but a command-line tool. Option C is incorrect because health.log is a file that contains information about the health of the Splunk components, such as the indexer cluster, the search head cluster, the license master, and the deployment server. This file can help troubleshoot issues related to Splunk deployment health, but not necessarily related to lookup tables. Option D is incorrect because configuration_change.log is a file that contains information about the changes made to the Splunk configuration files, such as the user, the time, the file, and the action. This file can help troubleshoot issues related to Splunk configuration changes, but not necessarily related to lookup tables.
References:
1: About lookups - Splunk Documentation 2: web_access.log - Splunk Documentation 3: Troubleshoot lookups to the Splunk Enterprise KV Store 4: Troubleshoot lookups in Splunk Enterprise Security - Splunk Documentation 5: Use btool to troubleshoot configurations - Splunk Documentation 6: Troubleshoot configuration issues - Splunk Documentation : Use the search.log file - Splunk Documentation : Troubleshoot search-time field extraction - Splunk Documentation : [Troubleshoot lookups - Splunk Documentation] :
[health.log - Splunk Documentation] : [configuration_change.log - Splunk Documentation]

NEW QUESTION # 25
Which of the following commands is used to clear the KV store?

- A. splunk clear kvstore
- B. splunk delete kvstore
- C. splunk clean kvstore
- D. splunk reinitialize kvstore

Answer: C

Explanation:
Explanation
The splunk clean kvstore command is used to clear the KV store. This command will delete all the collections and documents in the KV store and reset it to an empty state. This command can be useful for troubleshooting KV store issues or resetting the KV store data. The splunk clear kvstore, splunk delete kvstore, and splunk reinitialize kvstore commands are not valid Splunk commands. For more information, see Use the CLI to manage the KV store in the Splunk documentation.

NEW QUESTION # 26
.....