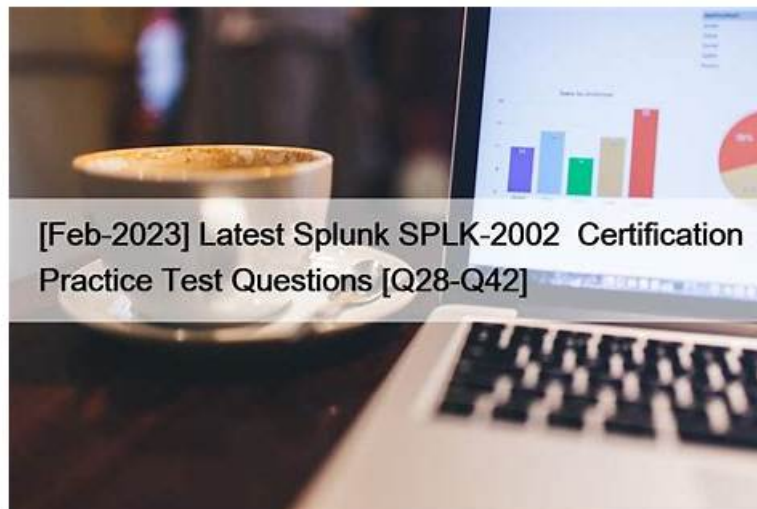


SPLK-2002 Latest Mock Test & New SPLK-2002 Exam Guide



BTW, DOWNLOAD part of Real4exams SPLK-2002 dumps from Cloud Storage: https://drive.google.com/open?id=1c2GuBNLcOhv6yo9VuV_-42CatJNV_G8n

The SPLK-2002 test materials are mainly through three learning modes, Pdf, Online and software respectively. The SPLK-2002 test materials have a biggest advantage that is different from some online learning platform which has using terminal number limitation, the SPLK-2002 quiz torrent can meet the client to log in to learn more, at the same time, the user can be conducted on multiple computers online learning, greatly reducing the time, and people can use the machine online of SPLK-2002 Test Prep more conveniently at the same time.

One of the key benefits of the SPLK-2002 certification is that it helps professionals stand out in a competitive job market. Employers are increasingly looking for certified Splunk architects who can help them make the most of their investment in the platform. By earning the SPLK-2002 certification, professionals can demonstrate their expertise and commitment to continuous learning and professional development.

The SPLK-2002 Exam consists of 70 multiple-choice questions and is administered through Pearson VUE, a leading provider of computer-based testing services. Candidates have 90 minutes to complete the exam and must achieve a passing score of 70% or higher to earn certification. SPLK-2002 exam is available in English and Japanese, and candidates can take it at any Pearson VUE testing center worldwide.

>> **SPLK-2002 Latest Mock Test** <<

Quiz Trustable Splunk - SPLK-2002 - Splunk Enterprise Certified Architect Latest Mock Test

Three versions for SPLK-2002 training materials are available, you can choose one you like according to your own needs. All three versions have free demo for you to have a try. SPLK-2002 PDF version is printable and you can learn them anytime and anyplace. SPLK-2002 Soft test engine can stimulate the real exam environment, so that you can know the procedures for the exam, and your confidence for SPLK-2002 Exam Materials will also be improved. SPLK-2002 Online test engine is convenient and easy to learn, it has testing history and performance review, and you can have a general review of what you have learned by this version.

Splunk Enterprise Certified Architect Sample Questions (Q137-Q142):

NEW QUESTION # 137

What log file would you search to verify if you suspect there is a problem interpreting a regular expression in a monitor stanza?

- A. splunkd.log
- B. btool.log

- C. **tailing_processor.log**
- D. metrics.log

Answer: C

Explanation:

Explanation

The `tailing_processor.log` file would be the best place to search if you suspect there is a problem interpreting a regular expression in a monitor stanza. This log file contains information about how Splunk monitors files and directories, including any errors or warnings related to parsing the monitor stanza. The `splunkd.log` file contains general information about the Splunk daemon, but it may not have the specific details about the monitor stanza. The `btool.log` file contains information about the configuration files, but it does not log the runtime behavior of the monitor stanza. The `metrics.log` file contains information about the performance metrics of Splunk, but it does not log the event breaking issues. For more information, see About Splunk Enterprise logging in the Splunk documentation.

NEW QUESTION # 138

Which of the following would be the least helpful in troubleshooting contents of Splunk configuration files?

- A. **crash logs**
- B. diagnostic logs
- C. search.log
- D. btool output

Answer: A

Explanation:

Splunk configuration files are files that contain settings that control various aspects of Splunk behavior, such as data inputs, outputs, indexing, searching, clustering, and so on¹. Troubleshooting Splunk configuration files involves identifying and resolving issues that affect the functionality or performance of Splunk due to incorrect or conflicting configuration settings. Some of the tools and methods that can help with troubleshooting Splunk configuration files are:

* `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 performance². This file can help troubleshoot issues related to search configuration, such as `props.conf`, `transforms.conf`, `macros.conf`, and so on³.

* `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 on⁴. This tool can help troubleshoot issues related to configuration precedence, inheritance, and merging, as well as identify the source of a configuration setting⁵.

* diagnostic logs: These are files that contain information about the Splunk system, such as the Splunk version, the operating system, the hardware, the license, the indexes, the apps, the users, the roles, the permissions, the configuration files, the log files, and the metrics⁶. These files can help troubleshoot issues related to Splunk installation, deployment, performance, and health⁷.

Option A is the correct answer because crash logs are the least helpful in troubleshooting Splunk configuration files. Crash logs are files that contain information about the Splunk process when it crashes, such as the stack trace, the memory dump, and the environment variables⁸. These files can help troubleshoot issues related to Splunk stability, reliability, and security, but not necessarily related to Splunk configuration⁹.

References:

1: About configuration files - Splunk Documentation 2: Use the search.log file - Splunk Documentation 3: Troubleshoot search-time field extraction - Splunk Documentation 4: Use btool to troubleshoot configurations - Splunk Documentation 5: Troubleshoot configuration issues - Splunk Documentation 6: About the diagnostic utility - Splunk Documentation 7: Use the diagnostic utility - Splunk Documentation 8: About crash logs - Splunk Documentation 9: [Troubleshoot Splunk Enterprise crashes - Splunk Documentation]

NEW QUESTION # 139

The master node distributes configuration bundles to peer nodes. Which directory peer nodes receive the bundles?

- A. **slave-apps**
- B. apps
- C. deployment-apps
- D. master-apps

Answer: A

Explanation:

The master node distributes configuration bundles to peer nodes in the slave-apps directory under \$SPLUNK_HOME/etc. The configuration bundle method is the only supported method for managing common configurations and app deployment across the set of peers. It ensures that all peers use the same versions of these files¹. Bundles typically contain a subset of files (configuration files and assets) from \$SPLUNK_HOME/etc/system, \$SPLUNK_HOME/etc/apps, and \$SPLUNK_HOME/etc/users². The process of distributing knowledge bundles means that peers by default receive nearly the entire contents of the search head's apps³.

NEW QUESTION # 140

A Splunk instance has the following settings in \$SPLUNK_HOME/etc/system/local/server.conf

[clustering]

mode = master

replication_factor = 2

pass4SymmKey = password123

Which of the following statements describe this Splunk instance? (Select all that apply.)

- A. This cluster's search factor is 2.
- B. This instance is missing the master_uri attribute.
- C. This is a multi-site cluster.
- D. This Splunk instance needs to be restarted.

Answer: B,D

NEW QUESTION # 141

In an existing Splunk environment, the new index buckets that are created each day are about half the size of the incoming data. Within each bucket, about 30% of the space is used for rawdata and about 70% for index files.

What additional information is needed to calculate the daily disk consumption, per indexer, if indexer clustering is implemented?

- A. Replication factor, search factor, number of accelerated searches, and total disk size across cluster.
- B. Total daily indexing volume, number of peer nodes, and number of accelerated searches.
- C. Total daily indexing volume, replication factor, search factor, and number of search heads.
- D. Total daily indexing volume, number of peer nodes, replication factor, and search factor.

Answer: D

Explanation:

The additional information that is needed to calculate the daily disk consumption, per indexer, if indexer clustering is implemented, is the total daily indexing volume, the number of peer nodes, the replication factor, and the search factor. These information are required to estimate how much data is ingested, how many copies of raw data and searchable data are maintained, and how many indexers are involved in the cluster. The number of accelerated searches, the number of search heads, and the total disk size across the cluster are not relevant for calculating the daily disk consumption, per indexer. For more information, see [Estimate your storage requirements] in the Splunk documentation.

NEW QUESTION # 142

.....

After you purchase our SPLK-2002 learning materials, we will still provide you with excellent service. Our customer service is 24 hours online, you can contact us any time you encounter any problems. Of course, you can also send us an email to contact with us on the SPLK-2002 Study Guide. We will reply you the first time. As you know, there are many users of SPLK-2002 exam preparation. But we work high-efficiently 24/7 to give you guidance.

New SPLK-2002 Exam Guide: https://www.real4exams.com/SPLK-2002_braindumps.html

- SPLK-2002 Latest Torrent ☐ SPLK-2002 Exams Dumps ☐ Training SPLK-2002 Solutions ☐ Enter ☐ www.vce4dumps.com ☐ and search for ➡ SPLK-2002 ☐ to download for free ☐ SPLK-2002 Exams Dumps
- Free PDF Quiz Splunk SPLK-2002 - First-grade Splunk Enterprise Certified Architect Latest Mock Test ☐ Search for ☐ SPLK-2002 ☐ and download it for free on ✓ www.pdfvce.com ☐ ✓ ☐ website ☐ SPLK-2002 Testing Center
- Buy www.prepaywaypdf.com Splunk SPLK-2002 Exam Dumps Today and Get Free Updates for 1 year ☐ Simply search for ➡ SPLK-2002 ☐ ☐ ☐ for free download on ☐ www.prepaywaypdf.com ☐ ☐ SPLK-2002 Testing Center

- Free Valid Splunk SPLK-2002 Questions Updates and Free Demos □ Open 《 www.pdfvce.com 》 and search for □ SPLK-2002 □ to download exam materials for free □ Valid SPLK-2002 Exam Labs
- Buy www.pdf.dumps.com Splunk SPLK-2002 Exam Dumps Today and Get Free Updates for 1 year □ Copy URL ► www.pdf.dumps.com ◀ open and search for □ SPLK-2002 □ to download for free □ Reliable SPLK-2002 Test Tips
- Free Valid Splunk SPLK-2002 Questions Updates and Free Demos □ Immediately open ⇒ www.pdfvce.com ⇐ and search for 【 SPLK-2002 】 to obtain a free download □ Valid SPLK-2002 Practice Questions
- Reliable SPLK-2002 Test Tips □ Valid SPLK-2002 Exam Labs □ Testking SPLK-2002 Learning Materials □ Search for ➡ SPLK-2002 □ and obtain a free download on 「 www.practicevce.com 」 □ Training SPLK-2002 Solutions
- Free PDF Quiz Splunk SPLK-2002 - First-grade Splunk Enterprise Certified Architect Latest Mock Test □ Search on □ www.pdfvce.com □ for ➡ SPLK-2002 □ to obtain exam materials for free download □ SPLK-2002 Latest Torrent
- Pass Guaranteed Quiz Splunk - SPLK-2002 Newest Latest Mock Test □ Search on 《 www.vceengine.com 》 for “ SPLK-2002 ” to obtain exam materials for free download □ SPLK-2002 PDF Question
- Free PDF Quiz Splunk SPLK-2002 - First-grade Splunk Enterprise Certified Architect Latest Mock Test ☼ Search for { SPLK-2002 } and easily obtain a free download on □ www.pdfvce.com □ □ SPLK-2002 Testing Center
- Test SPLK-2002 Dumps Free □ Valid SPLK-2002 Exam Format □ SPLK-2002 Valid Braindumps Ebook □ Search for ➡ SPLK-2002 □ and download it for free immediately on “ www.vce4dumps.com ” □ Valid SPLK-2002 Practice Questions
- bbs.t-firefly.com, renasnook.com, bbs.t-firefly.com, www.kelkeyglobalacademy.com, www.sxr.edu.cn, bbs.t-firefly.com, lb.abcbbk.com, gravitycp.academy, bbs.t-firefly.com, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New SPLK-2002 dumps are available on Google Drive shared by Real4exams: https://drive.google.com/open?id=1c2GuBNLcOhv6yo9VuV_-42CatJNV_G8n