

100% Pass Quiz 2026 Splunk SPLK-2002 Authoritative Valid Test Cost



What's more, part of that DumpsQuestion SPLK-2002 dumps now are free: https://drive.google.com/open?id=1F9fauV86W-6cK1Vb0owuX-O_WMu4akqg

The pass rate of SPLK-2002 study materials are 98.95%, if you buy SPLK-2002 study material from us, we can ensure you pass the exam successfully. Besides you can get SPLK-2002 exam dumps in ten minutes after your payment. You can use the SPLK-2002 exam dumps freely, if you have any questions in the process of your learning, you can consult the service stuff, and they have the professional knowledge about SPLK-2002 Learning Materials, so don't hesitate to ask for help from them.

Splunk SPLK-2002: Splunk Enterprise Certified Architect Exam

A Splunk Enterprise Certified Architect has a thorough understanding of Splunk Deployment Methodology and best practices for planning, data collection, and sizing for a distributed deployment and can manage and troubleshoot a standard distributed deployment with indexer and search head clustering. This certification demonstrates an individual's ability to deploy, manage, and troubleshoot complex Splunk Enterprise environments. The best way to start the preparation is to start preparing **splk-2002 exam dumps** and then practice **splk-2002 practice exams**.

>> Valid SPLK-2002 Test Cost <<

Quick Tips to Pass your Exam with Splunk SPLK-2002 Questions

After decades of hard work, our products are currently in a leading position in the same kind of education market, our SPLK-2002 learning materials, with their excellent quality and constantly improved operating system, In many areas won the unanimous endorsement of many international customers. Advanced operating systems enable users to quickly log in and use, in constant practice and theoretical research, our SPLK-2002 learning materials have come up with more efficient operating system to meet user needs, so we can assure users here , after user payment , users can perform a review of the SPLK-2002 Exam in real time , because our advanced operating system will immediately send users SPLK-2002 learning material to the email address where they are paying , this greatly facilitates the user, lets the user be able to save more study time.

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 (Q144-Q149):

NEW QUESTION # 144

Which of the following is a problem that could be investigated using the Search Job Inspector?

- A. Different users are seeing different extracted fields from the same search.
- **B. Error messages are appearing underneath the search bar in Splunk Web.**
- C. Events are not being sorted in reverse chronological order.
- D. Dashboard panels are showing "Waiting for queued job to start" on page load.

Answer: B

Explanation:

According to the Splunk documentation¹, the Search Job Inspector is a tool that you can use to troubleshoot search performance and understand the behavior of knowledge objects, such as event types, tags, lookups, and so on, within the search. You can inspect search jobs that are currently running or that have finished recently.

The Search Job Inspector can help you investigate error messages that appear underneath the search bar in Splunk Web, as it can show you the details of the search job, such as the search string, the search mode, the search timeline, the search log, the search profile, and the search properties. You can use this information to identify the cause of the error and fix it². The other options are false because:

* Dashboard panels showing "Waiting for queued job to start" on page load is not a problem that can be investigated using the Search Job Inspector, as it indicates that the search job has not started yet. This could be due to the search scheduler being busy or the search priority being low. You can use the Jobs page or the Monitoring Console to monitor the status of the search jobs and adjust the priority or concurrency settings if needed³.

* Different users seeing different extracted fields from the same search is not a problem that can be investigated using the Search Job Inspector, as it is related to the user permissions and the knowledge object sharing settings. You can use the Access Controls page or the Knowledge Manager to manage the user roles and the knowledge object visibility⁴.

* Events not being sorted in reverse chronological order is not a problem that can be investigated using the Search Job Inspector, as it is related to the search syntax and the sort command. You can use the Search Manual or the Search Reference to learn how to use the sort command and its options to sort the events by any field or criteria.

NEW QUESTION # 145

What is the algorithm used to determine captaincy in a Splunk search head cluster?

- A. Rapt distributed consensus.
- **B. Raft distributed consensus.**
- C. Round-robin distribution consensus.
- D. Rift distributed consensus.

Answer: B

Explanation:

Explanation/Reference: <https://answers.splunk.com/answers/664102/need-to-know-about-raft-directory-on-search-head- c.html>

NEW QUESTION # 146

Splunk Enterprise platform instrumentation refers to data that the Splunk Enterprise deployment logs in the _introspection index. Which of the following logs are included in this index? (Select all that apply.)

- **A. disk_objects.log**
- **B. resource_usage.log**
- C. metrics.log
- D. audit.log

Answer: A,B

NEW QUESTION # 147

A Splunk instance has crashed, but no crash log was generated. There is an attempt to determine what user activity caused the crash

by running the following search:

What does searching for `closed_txn=0` do in this search?

- A. Filters results to situations where Splunk was started, but not stopped.
- B. Filters results to situations where Splunk was started and stopped multiple times.
- C. Filters results to situations where Splunk was started and stopped once.
- D. Filters results to situations where Splunk was stopped and then immediately restarted.

Answer: A

Explanation:

Searching for `closed_txn=0` in this search filters results to situations where Splunk was started, but not stopped. This means that the transaction was not completed, and Splunk crashed before it could finish the pipelines. The `closed_txn` field is added by the transaction command, and it indicates whether the transaction was closed by an event that matches the `endswith` condition¹. A value of 0 means that the transaction was not closed, and a value of 1 means that the transaction was closed¹. Therefore, option D is the correct answer, and options A, B, and C are incorrect.

1: transaction command overview

NEW QUESTION # 148

How many cluster managers are required for a multisite indexer cluster?

- A. Two for the entire cluster.
- B. Two for each site.
- C. One for each site.
- D. One for the entire cluster.

Answer: D

Explanation:

A multisite indexer cluster is a type of indexer cluster that spans multiple geographic locations or sites. A multisite indexer cluster requires only one cluster manager, also known as the master node, for the entire cluster. The cluster manager is responsible for coordinating the replication and search activities among the peer nodes across all sites. The cluster manager can reside in any site, but it must be accessible by all peer nodes and search heads in the cluster. Option C is the correct answer. Option A is incorrect because having two cluster managers for the entire cluster would introduce redundancy and complexity. Option B is incorrect because having one cluster manager for each site would create separate clusters, not a multisite cluster. Option D is incorrect because having two cluster managers for each site would be unnecessary and inefficient².

1: <https://docs.splunk.com/Documentation/Splunk/9.1.2/Indexer/Multisiteoverview> 2:

<https://docs.splunk.com/Documentation/Splunk/9.1.2/Indexer/Clustermanageroverview>

NEW QUESTION # 149

.....

SPLK-2002 Question Explanations: <https://www.dumpsquestion.com/SPLK-2002-exam-dumps-collection.html>

- SPLK-2002 Pass-Sure Dumps - SPLK-2002 Exam Dumps - SPLK-2002 Exam Simulator ☐ Download ➡ SPLK-2002 ☐ for free by simply entering ✓ www.examdiscuss.com ☐ ✓ ☐ website ☐ SPLK-2002 Test Topics Pdf
- SPLK-2002 Pass-Sure Dumps - SPLK-2002 Exam Dumps - SPLK-2002 Exam Simulator ☐ Open ▶ www.pdfvce.com ◀ and search for 《 SPLK-2002 》 to download exam materials for free ✖ SPLK-2002 Test Topics Pdf
- SPLK-2002 Training Materials ☐ Best SPLK-2002 Study Material ☐ SPLK-2002 Training Materials ☐ Download ➡ SPLK-2002 ☐ ☐ ☐ for free by simply searching on ☼ www.verifiddumps.com ☐ ☼ ☐ ☐ SPLK-2002 Vce File
- Best SPLK-2002 Study Material ☐ SPLK-2002 Latest Exam Answers ☐ Valid SPLK-2002 Learning Materials ☐ Open 《 www.pdfvce.com 》 and search for ➡ SPLK-2002 ☐ ☐ ☐ to download exam materials for free ☐ Passing SPLK-2002 Score Feedback
- SPLK-2002 Valid Exam Simulator ☐ Best SPLK-2002 Study Material ☐ SPLK-2002 Valid Exam Simulator ☐ Search for ➡ SPLK-2002 ☐ ☐ ☐ and download it for free on ✓ www.troytecdumps.com ☐ ✓ ☐ website ☐ SPLK-2002 Training Materials
- New Valid SPLK-2002 Test Cost 100% Pass | Reliable SPLK-2002: Splunk Enterprise Certified Architect 100% Pass ☐ Open { www.pdfvce.com } and search for [SPLK-2002] to download exam materials for free ☐ SPLK-2002 Vce File
- Pass SPLK-2002 Exam with Professional Valid SPLK-2002 Test Cost by www.pdf.dumps.com ☐ Download ☐ SPLK-

[illegible]

What's more, part of that DumpsQuestion SPLK-2002 dumps now are free: https://drive.google.com/open?id=1F9fauV86W-6cK1Vb0owuX-O_WMu4akqg