

Splunk SPLK-2003 Real Exam Questions in Three Formats

Useful Study Guide & Exam Questions to Pass the Splunk SPLK-2003 Exam

Solve Splunk SPLK-2003 Practice Tests to Score High!

www.CertFun.com

Here are all the necessary details to pass the SPLK-2003 exam on your first attempt. Get rid of all your worries now and find the details regarding the syllabus, study guide, practice tests, books, and study materials in one place. Through the SPLK-2003 certification preparation, you can learn more on the Splunk SOAR Certified Automation Developer, and getting the Splunk SOAR Certified Automation Developer certification gets easy.

DOWNLOAD the newest ActualTestsQuiz SPLK-2003 PDF dumps from Cloud Storage for free: <https://drive.google.com/open?id=1kRcrSPp69wHOBwBwdyJvArNC0g5RxXh>

The most important part of Splunk SPLK-2003 exam preparation is practice, and the right practice is often the difference between success and failure. ActualTestsQuiz also makes your preparation easier with practice test software to help you get hands-on exam experience before the actual Splunk Phantom Certified Admin (SPLK-2003) exam. After consistent practice, the final exam will not be too difficult for a student who has already practiced from real Splunk SPLK-2003 exam questions.

Splunk SPLK-2003 (Splunk Phantom Certified Admin) Certification Exam is a valuable certification for professionals who work with the Splunk Phantom platform. It validates the knowledge and skills required to effectively manage and utilize the platform, and provides a competitive edge in the job market. Candidates who pass the exam demonstrate their ability to troubleshoot issues, manage users and resources, and integrate Phantom with other tools and platforms, making them highly sought after in the industry.

The SPLK-2003 Exam is an excellent choice for professionals who are looking to validate their knowledge and skills in Splunk Phantom and demonstrate their expertise in security automation and orchestration. By passing SPLK-2003 exam and earning the Splunk Phantom Certified Admin certification, professionals can enhance their career prospects and play a vital role in securing their organization's infrastructure.

>>> SPLK-2003 Online Test <<<

SPLK-2003 Exam Course, Premium SPLK-2003 Files

There are many merits of our product on many aspects and we can guarantee the quality of our Splunk Phantom Certified Admin SPLK-2003 practice engine. Firstly, our experienced expert team compile them elaborately based on the real exam. Secondly, both the language and the content of our Splunk SPLK-2003 Study Materials are simple.

Successful completion of the SPLK-2003 Exam leads to the Splunk Phantom Certified Admin certification, which validates the knowledge and skills required to effectively manage and administer Splunk Phantom in a production environment. Splunk Phantom Certified Admin certification is recognized by employers and organizations worldwide, and demonstrates an individual's commitment to staying up-to-date with the latest security automation and orchestration technologies.

Splunk Phantom Certified Admin Sample Questions (Q54-Q59):

NEW QUESTION # 54

Some of the playbooks on the Phantom server should only be executed by members of the admin role. How can this rule be applied?

- A. Add a filter block to all restricted playbooks that filters for runRole - "Admin".
- **B. Make sure the Execute Playbook capability is removed from all roles except admin.**
- C. Add a tag with restricted access to the restricted playbooks.
- D. Place restricted playbooks in a second source repository that has restricted access.

Answer: B

Explanation:

Explanation

The correct answer is B because the best way to restrict the execution of playbooks to members of the admin role is to make sure the Execute Playbook capability is removed from all roles except admin. The Execute Playbook capability is a permission that allows a user to run any playbook on any container. By default, all roles have this capability, but it can be removed or added in the Phantom UI by going to Administration > User Management > Roles. Removing this capability from all roles except admin will ensure that only admin users can execute playbooks. See Splunk SOAR Documentation for more details.

NEW QUESTION # 55

Which of the following is a step when configuring event forwarding from Splunk to Phantom?

- A. Create a saved search that generates the JSON for the new container on Phantom.
- **B. Create a Splunk alert that uses the event_forward.py script to send events to Phantom.**
- C. Map CIM to CEF fields.
- D. Map CEF to CIM fields.

Answer: B

Explanation:

Explanation

A step when configuring event forwarding from Splunk to Phantom is to create a Splunk alert that uses the event_forward.py script to send events to Phantom. This script will convert the Splunk events to CEF format and send them to Phantom as containers. The other options are not valid steps for event forwarding.

See Forwarding events from Splunk to Phantom for more details.

NEW QUESTION # 56

What is the default embedded search engine used by Phantom?

- A. Embedded Phantom search engine.
- B. Embedded Splunk search engine.
- **C. Embedded Elastic search engine.**
- D. Embedded Django search engine.

Answer: C

NEW QUESTION # 57

What is the main purpose of using a customized workbook?

- A. Workbooks may not be customized; only default workbooks are permitted within Phantom.
- B. Workbooks apply service level agreements (SLAs) to containers and monitor completion status on the ROI dashboard.
- C. Workbooks automatically implement a customized processing of events using Python code.
- **D. Workbooks guide user activity and coordination during event analysis and case operations.**

Answer: D

Explanation:

The main purpose of using a customized workbook is to guide user activity and coordination during event analysis and case operations. Workbooks can be customized to include different phases, tasks, and instructions for the users. The other options are not valid purposes of using a customized workbook.

Customized workbooks in Splunk SOAR are designed to guide users through the process of analyzing events and managing cases. They provide a structured framework for documenting investigations, tracking progress, and ensuring that all necessary steps are followed during incident response and case management. This helps in coordinating team efforts, maintaining consistency in response activities, and ensuring that all aspects of an incident are thoroughly investigated and resolved.

Workbooks can be customized to fit the specific processes and procedures of an organization, making them a versatile tool for managing security operations.

NEW QUESTION # 58

Which app allows a user to run Splunk queries from within Phantom?

- A. Splunk App for Phantom?
- B. The Integrated Splunk/Phantom app.
- C. Splunk App for Phantom Reporting.
- **D. Phantom App for Splunk.**

Answer: D

Explanation:

Explanation

The Phantom App for Splunk allows a user to run Splunk queries from within Phantom. This app provides actions such as run query, ingest events, and save search, which enable the user to interact with Splunk from Phantom playbooks or the Phantom UI. The other apps are not relevant for this use case. The Splunk App for Phantom is used to send data from Splunk to Phantom. The Integrated Splunk/Phantom app is a deprecated app that was replaced by the Splunk App for Phantom. The Splunk App for Phantom Reporting is used to generate reports on Phantom activity from Splunk. Reference, page 1.

NEW QUESTION # 59

.....

SPLK-2003 Exam Course: <https://www.actualtestsquiz.com/SPLK-2003-test-torrent.html>

- New SPLK-2003 Study Guide ☐ Reliable SPLK-2003 Braindumps ☐ Latest SPLK-2003 Exam Price ☐ Immediately open ➡ www.examcollectionpass.com ☐ and search for ➡ SPLK-2003 ☐ to obtain a free download ☐ Certification SPLK-2003 Training
- Valid Test SPLK-2003 Tutorial ↔ SPLK-2003 Exam Vce ☐ Authorized SPLK-2003 Certification ☐ The page for free download of “SPLK-2003 ” on ➡ www.pdfvce.com ☐ will open immediately ☐ SPLK-2003 Preparation
- Reliable Splunk SPLK-2003 Online Test Are Leading Materials - Free PDF SPLK-2003 Exam Course ☐ Search for ➡ SPLK-2003 ☐ ☐ ☐ and obtain a free download on ➡ www.practicevce.com ☐ ☐ ☐ SPLK-2003 Exam Vce
- 100% Pass 2026 Splunk SPLK-2003: Professional Splunk Phantom Certified Admin Online Test ☐ Search for ☐ SPLK-2003 ☐ and download exam materials for free through ➡ www.pdfvce.com ☐ ☐ Valid SPLK-2003 Exam Question
- Free PDF 2026 Splunk SPLK-2003: Reliable Splunk Phantom Certified Admin Online Test ☐ The page for free download of ➡ SPLK-2003 ☐ ☐ ☐ on [www.prepawayexam.com] will open immediately ☐ SPLK-2003 New Dumps Pdf
- Latest updated Splunk SPLK-2003: Splunk Phantom Certified Admin Online Test - Reliable Pdfvce SPLK-2003 Exam Course ☐ Simply search for ☐ SPLK-2003 ☐ for free download on ☐ www.pdfvce.com ☐ ☐ Authorized SPLK-2003 Certification
- SPLK-2003 Latest Exam Notes ☐ SPLK-2003 Certification Sample Questions ☐ Exam SPLK-2003 Training ☐

[illegible]

What's more, part of that ActualTestsQuiz SPLK-2003 dumps now are free: <https://drive.google.com/open?id=1kRcrSPp69wHOBRowBwdyJvArNC0g5RxXh>