Pass Guaranteed 2026 Splunk The Best New SPLK-2003 Test Tutorial

P.S. Free 2026 Splunk SPLK-2003 dumps are available on Google Drive shared by SurePassExams: https://drive.google.com/open?id=1IWLPLz5xAvFCFsdPtXCcdPkdo1Pne5fU

Without bothering to stick to any formality, our Splunk Phantom Certified Admin SPLK-2003 learning quiz can be obtained within five minutes. No need to line up or queue up to get our SPLK-2003 practice materials. They are not only efficient on downloading aspect, but can expedite your process of review. No harangue is included within Splunk SPLK-2003 Training Materials and every page is written by our proficient experts with dedication.

The SPLK-2003 certification exam is a multiple-choice, online exam that consists of 60 questions. Candidates have 90 minutes to complete the exam and must score at least 70% to pass. SPLK-2003 Exam is administered by Splunk and can be taken from anywhere with a reliable internet connection.

>> New SPLK-2003 Test Tutorial <<

SPLK-2003 Valid Exam Papers | Trustworthy SPLK-2003 Practice

Our SPLK-2003 learning guide boosts many advantages and it is your best choice to prepare for the test. Firstly, our SPLK-2003 training prep is compiled by our first-rate expert team and linked closely with the real exam. So that if you practice with our SPLK-2003 Exam Questions, then you will pass for sure. Secondly, our SPLK-2003 study materials provide 3 versions and multiple functions to make the learners have no learning obstacles. They are the PDF, Software and APP online.

Splunk SPLK-2003 Certification Exam is designed for individuals who are interested in becoming certified as a Splunk Phantom Certified Admin. Splunk Phantom is a security automation and orchestration platform that helps organizations automate their security operations workflows. The SPLK-2003 exam tests the candidates' knowledge and skills in managing and administering Splunk Phantom, including tasks such as setting up and configuring the platform, managing workflows, and creating and managing playbooks. Splunk Phantom Certified Admin certification is intended for security professionals who want to become experts in security automation and orchestration using the Splunk Phantom platform.

Splunk Phantom Certified Admin Sample Questions (Q108-Q113):

NEW QUESTION # 108
Seventy can be set during ingestion and later changed manually. What other mechanism can change the severity or a container?

- A. Service level agreement (SLA) expiration
- B. Actions
- C. Notes
- D. Playbooks

Answer: B

NEW QUESTION # 109

Which of the following can the format block be used for?

- A. To create text strings that merge state text with dynamic values for input or output.
- B. To generate arrays for input into other functions.
- C. To generate string parameters for automated action blocks.
- D. To generate HTML or CSS content for output in email messages, user prompts, or comments.

Answer: A

Explanation:
The format block in Splunk SOAR is utilized to construct text strings by merging static text with dynamic values, which can then be used for both input to other playbook blocks and output for reports, emails, or other forms of communication. This capability is essential for customizing messages, commands, or data processing tasks within a playbook, allowing for the dynamic insertion of variable data into predefined text templates. This feature enhances the playbook's ability to present information clearly and to execute actions that require specific parameter formats.

NEW QUESTION # 110
When writing a custom function that uses regex to extract the domain name from a URL, a user wants to create a new artifact for the extracted domain. Which of the following Python API calls will create a new artifact?

- A. phantom.create_artifact ()
- B. phantom. update ()
- C. phantom.add_artifact ()
- D. phantom.new_artifact ()

Answer: A

Explanation:
In the Splunk SOAR platform, when writing a custom function in Python to handle data such as extracting a domain name from a URL, you can create a new artifact using the Python API call phantom.create_artifact().
This function allows you to specify the details of the new artifact, such as the type, CEF (Common Event Format) data, container it belongs to, and other relevant information necessary to create an artifact within the system.

NEW QUESTION # 111
A user has written a playbook that calls three other playbooks, one after the other. The user notices that the second playbook starts executing before the first one completes. What is the cause of this behavior?

- A. Synchronous execution has not been configured.
- B. Incorrect Join configuration on the second playbook.
- C. The steep option for the second playbook is not set to a long enough interval.
- D. The first playbook is performing poorly.

Answer: A

Explanation:
The correct answer is D because synchronous execution has not been configured. Synchronous execution is a feature that allows you to control the order of execution of playbook blocks. By default, Phantom executes playbook blocks asynchronously, meaning that it does not wait for one block to finish before starting the next one. This can cause problems when you have dependencies between blocks or when you call other playbooks.
To enable synchronous execution, you need to use the sync action in the run playbook block and specify the name of the next block to run after the called playbook completes. See Splunk SOAR Documentation for more details.
In Splunk SOAR, playbooks can be executed either synchronously or asynchronously. Synchronous execution ensures that a playbook waits for a called playbook to complete before proceeding to the next step. If the second playbook starts executing before the first one completes, it indicates that synchronous execution was not configured for the playbooks. Without synchronous execution, playbooks will execute independently of each other's completion status, leading to potential overlaps in execution. This behavior can be controlled by properly configuring the playbook execution settings to ensure that dependent playbooks complete their tasks in the desired order.

NEW QUESTION # 112
Splunk user account(s) with which roles must be created to configure Phantom with an external Splunk Enterprise instance?

- A. admin,user
- B. phantomsearch, phantomdelete
- C. superuser, administrator
- D. phantomcreate. phantomedit

Answer: C

Explanation:
When configuring Splunk Phantom to integrate with an external Splunk Enterprise instance, it is typically required to have user accounts with sufficient privileges to access data and perform necessary actions. The roles of "superuser" and "administrator" in Splunk provide the broad set of permissions needed for such integration, enabling comprehensive access to data, management capabilities, and the execution of searches or actions that Phantom may require as part of its automated playbooks or investigations.

NEW QUESTION # 113
......