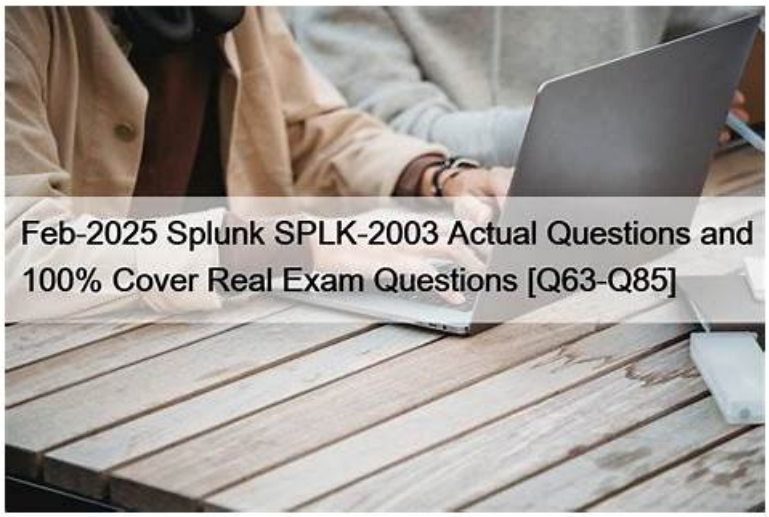
Quiz 2026 Splunk SPLK-2003: Splunk Phantom Certified Admin–High Pass-Rate New Exam Duration



What's more, part of that ITexamReview SPLK-2003 dumps now are free: https://drive.google.com/open?id=19HDtHnFO0auJNKB9z6iB_uxAe7uaSwVN

If you don't have well-knit special basic knowledge and be block by SPLK-2003 exam so that you can't obtain the Splunk certification. However your company needs this certification, your supervisor requests you to obtain as soon as possible, please don't worry, SPLK-2003 valid exam questions vce can help you pass exam soon. If you don't know about our company and don't trust this kind of products in website, you may be out. Now purchasing SPLK-2003 Valid Exam Questions vce is a popular thing in this field since it is high pass rate at the first attempt.

Splunk SPLK-2003 certification exam is designed for individuals who wish to become certified Splunk Phantom administrators. Splunk Phantom Certified Admin certification exam tests the candidate's knowledge of the Splunk Phantom platform and their ability to configure, manage, and troubleshoot Phantom instances. SPLK-2003 exam measures the candidate's skills in areas such as deployment, automation, and integration with other technologies.

The Splunk Phantom Certified Admin certification exam consists of 60 multiple-choice questions that need to be completed within 90 minutes. The passing score for the exam is 70%. SPLK-2003 Exam is available in English, Japanese, and Simplified Chinese. SPLK-2003 exam fee is $200 USD, and it can be taken online from anywhere in the world. Splunk Phantom Certified Admin certification is valid for two years, after which the candidate needs to retake the exam to maintain their certification status.

>> New SPLK-2003 Exam Duration <<

Exam SPLK-2003 Vce & SPLK-2003 Reliable Exam Price

ITexamReview offers a free trial for all the products and give you an open chance to test its various features. If you are satisfied with the demo so, you can buy SPLK-2003 exam questions PDF or Practice software. We updated our product frequently, our determined team is always ready to make certain alterations as and when SPLK-2003 announce any changing.

Splunk Phantom Certified Admin Sample Questions (Q106-Q111):

NEW QUESTION # 106
Which of the following is a step when configuring event forwarding from Splunk to Phantom?

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

Answer: B

NEW QUESTION # 107
How is a Django filter query performed?

- A. By adding parameters to the URL similar to the following: phantom/rest/container?_filter_tags_contains="sumo".
- B. phantom/rest/search/app/contains/"sumo"
- C. Install the SOAR Django App first, then configure the search query in the App editor.
- D. Browse to the Django Filter Query Editor in the Administration panel.

Answer: A

Explanation:
Django filter queries in Splunk SOAR are performed by appending filter parameters directly to the REST API URL. This allows users to refine their search and retrieve specific data. For example, to filter containers by tags containing the word "sumo", the following URL structure would be used:
https://<PHANTOM_URL>/rest/container?_filter_tags_contains="sumo". This format enables users to construct dynamic queries that can filter results based on specified criteria within the Django framework used by Splunk SOAR.
The correct way to perform a Django filter query in Splunk SOAR is to add parameters to the URL similar to the following: phantom/rest/container?_filter_tags_contains="sumo". This will return a list of containers that have the tag "sumo" in them. You can use various operators and fields to filter the results according to your needs. For more details, see Query for Data and Use filters in your Splunk SOAR (Cloud) playbook to specify a subset of artifacts before further processing. The other options are either incorrect or irrelevant for this question. For example:
*phantom/rest/search/app/contains/"sumo" is not a valid URL for a Django filter query. It will return an error message saying "Invalid endpoint".
*There is no Django Filter Query Editor in the Administration panel of Splunk SOAR. You can use the REST API Tester to test your queries, but not to edit them.
*There is no SOAR Django App that needs to be installed or configured for performing Django filter queries.
Splunk SOAR uses the Django framework internally, but you do not need to install or use any additional apps for this purpose.

NEW QUESTION # 108
Which of the following are the steps required to complete a full backup of a Splunk Phantom deployment' Assume the commands are executed from /opt/phantom/bin and that no other backups have been made.

- A. Within the UI: Select from the main menu Administration > Product Settings > Backup.
- B. On the command line enter: rode sudo python ibackup.pyc --setup, then audo phenv python ibackup.pyc --backup.
- C. On the command line enter: sudo phenv python ibackup.pyc --backup --backup-type full, then sudo phenv python ibackup.pyc --setup.
- D. Within the UI: Select from the main menu Administration > System Health > Backup.

Answer: C

Explanation:
The steps required to complete a full backup of a Splunk Phantom deployment are to first run the --backup --backup-type full command and then run the --setup command. The --backup command creates a backup file in the /opt/phantom/backup directory. The --backup-type full option specifies that the backup file includes all the data and configuration files of the Phantom server. The --setup command creates a configuration file that contains the encryption key and other information needed to restore the backup file.
Performing a full backup of a Splunk Phantom deployment involves using the command-line interface, primarily because Phantom's architecture and data management processes are designed to be managed at the server level for comprehensive backup and recovery. The correct sequence involves initiating a full backup first using the --backup --backup-type full option to ensure all configurations, data, and necessary components are included in the backup. Following the completion of the backup, the --setup option might be used to configure or verify the backup settings, although typically, the setup would precede backup operations in practical scenarios.
This process ensures that all aspects of the Phantom deployment are preserved, including configurations, playbooks, cases, and other data, which is crucial for disaster recovery and system migration.

NEW QUESTION # 109

What are indicators?

- A. Artifact values that can appear in multiple containers.
- B. Action result items that determine the flow of execution in a playbook.
- C. Action results that may appear in multiple containers.
- D. Artifact values with special security significance.

Answer: D

Explanation:
Indicators within the context of Splunk SOAR refer to artifact values that have special security significance.
These are typically derived from the data within artifacts and are identified as having particular importance in the analysis and investigation of security incidents. Indicators might include items such as IP addresses, domain names, file hashes, or other data points that can be used to detect, correlate, and respond to security threats. Recognizing and managing indicators effectively is key to leveraging SOAR for enhanced threat intelligence, incident response, and security operations efficiency.

NEW QUESTION # 110
What is enabled if the Logging option for a playbook's settings is enabled?

- A. More detailed logging information Is available m the Investigation page.
- B. All modifications to the playbook will be written to the audit log.
- C. The playbook will write detailed execution information into the spawn.log.
- D. More detailed information is available in the debug window.

Answer: A

Explanation:
In Splunk SOAR (formerly known as Phantom), enabling the Logging option for a playbook's settings primarily affects how logging information is displayed on the Investigation page. When this option is enabled, more detailed logging information is made available on the Investigation page, which can be crucial for troubleshooting and understanding the execution flow of the playbook. This detailed information can include execution steps, actions taken, and conditional logic paths followed during the playbook run.
It's important to note that enabling logging does not affect the audit logs or the debug window directly, nor does it write execution details to the spawn.log. Instead, it enhances the visibility and granularity of logs displayed on the specific Investigation page related to the playbook's execution.
References:
Splunk Documentation and SOAR User Guides typically outline the impacts of enabling various settings within the playbook configurations, explaining how these settings affect the operation and logging within the system. For specific references, consulting the latest Splunk SOAR documentation would provide the most accurate and detailed guidance.
Enabling the Logging option for a playbook's settings in Splunk SOAR indeed affects the level of detail provided on the Investigation page. Here's a comprehensive explanation of its impact:
Investigation Page Logging:
The Investigation page serves as a centralized location for reviewing all activities related to an incident or event within Splunk SOAR. When the Logging option is enabled, it enhances the level of detail available on this page, providing a granular view of the playbook's execution.
This includes detailed information about each action's execution, such as parameters used, results obtained, and any conditional logic that was evaluated.
Benefits of Detailed Logging:
Troubleshooting: It becomes easier to diagnose issues within a playbook when you can see a detailed log of its execution.
Incident Analysis: Analysts can better understand the sequence of events and the decisions made by the playbook during an incident.
Playbook Optimization: Developers can use the detailed logs to refine and improve the playbook's logic and performance.
Non-Impacted Areas:
The audit log, which tracks changes to the playbook itself, is not affected by the Logging option.
The debug window, used for real-time debugging during playbook development, also remains unaffected.
The spawn.log file, which contains internal operational logs for the Splunk SOAR platform, does not receive detailed execution information from playbooks.
Best Practices:
Enable detailed logging during the development and testing phases of a playbook to ensure thorough analysis and debugging.
Consider the potential impact on storage and performance when enabling detailed logging in a production environment.
References:
For the most accurate and up-to-date guidance on playbook settings and their effects, I recommend consulting the latest Splunk

SOAR documentation and user guides. These resources provide in-depth information on configuring playbooks and understanding the implications of various settings within the Splunk SOAR platform.
In summary, the Logging option is a powerful feature that enhances the visibility of playbook operations on the Investigation page, aiding in incident analysis and ensuring that playbooks are functioning correctly. It is an essential tool for security teams to effectively manage and respond to incidents within their environment.

NEW QUESTION # 111
.....

Our SPLK-2003 training materials make it easier to prepare exam with a variety of high quality functions. We are committed to your achievements, so make sure you try preparation exam at a time to win. Our SPLK-2003 exam prep is of reasonably great position from highly proficient helpers who have been devoted to their quality over ten years to figure your problems out. Their quality function of our SPLK-2003 learning quiz is observably clear once you download them.