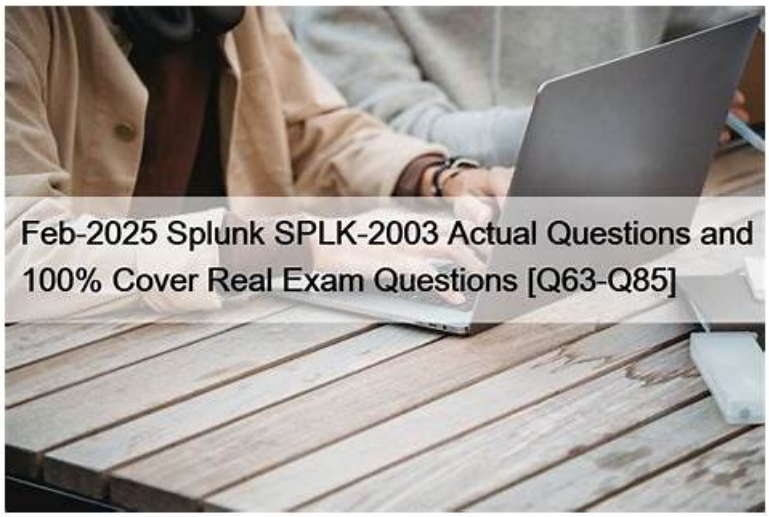
Free PDF Quiz 2025 Splunk SPLK-2003: Reliable Splunk Phantom Certified Admin Key Concepts



2025 Latest PassCollection SPLK-2003 PDF Dumps and SPLK-2003 Exam Engine Free Share: https://drive.google.com/open?id=1JD2n69KMovIsaXDwGAsgDmVz_a6M72lr

PassCollection is a website to improve the pass rate of Splunk certification SPLK-2003 exam. Senior IT experts in the PassCollection constantly developed a variety of successful programs of passing Splunk certification SPLK-2003 exam, so the results of their research can 100% guarantee you Splunk certification SPLK-2003 exam for one time. PassCollection's training tools are very effective and many people who have passed a number of IT certification exams used the practice questions and answers provided by PassCollection. Some of them who have passed the Splunk Certification SPLK-2003 Exam also use PassCollection's products. Selecting PassCollection means choosing a success

Splunk SPLK-2003 certification exam is designed to test the skills and knowledge of individuals who want to become certified Splunk Phantom administrators. Splunk Phantom Certified Admin certification exam covers a range of topics related to the Splunk Phantom platform, including installation, configuration, management, and troubleshooting. Splunk Phantom Certified Admin certification is ideal for IT professionals who need to manage and automate security operations, incident response, and other IT processes using the Splunk Phantom platform.

The SPLK-2003 exam covers a wide range of topics related to Splunk Phantom administration. These include setting up the Phantom platform, creating and managing assets, creating and managing playbooks, creating and managing roles and users, and monitoring and troubleshooting the platform. SPLK-2003 Exam is designed to test a candidate's knowledge of various aspects of Splunk Phantom administration and their ability to apply that knowledge in real-world scenarios.

Splunk SPLK-2003, also known as the Splunk Phantom Certified Admin exam, is designed for IT professionals who want to validate their expertise in using Splunk Phantom to automate and orchestrate tasks in their organization's security operations center (SOC). Splunk Phantom Certified Admin certification demonstrates that an individual has the skills and knowledge to manage, configure, and troubleshoot Splunk Phantom, which is a security automation and orchestration platform that enables SOC teams to respond to cyber threats more efficiently and effectively.

>> SPLK-2003 Key Concepts <<

Free PDF 2025 Splunk Perfect SPLK-2003 Key Concepts

Before purchasing our SPLK-2003 practice guide, we will offer you a part of questions as free demo for downloading so that you can know our SPLK-2003 exam question style and PDF format deeper then you will feel relieved to purchase certification SPLK-2003 study guide. We try our best to improve ourselves to satisfy all customers' demands. If you have any doubt or hesitate, please feel free to contact us about your issues. If you have doubt about our SPLK-2003 Exam Preparation questions the demo will prove that our product is helpful and high-quality.

Splunk Phantom Certified Admin Sample Questions (Q63-Q68):

NEW QUESTION # 63
What do assets provide for app functionality?

- A. Assets provide hostnames, passwords, and other artifacts needed to run actions.
- B. Assets provide location, credentials, and other parameters needed to run actions.
- C. Assets provide Python code, REST API, and other capabilities needed to run actions.
- D. Assets provide firewall, network, and data sources needed to run actions.

Answer: B

Explanation:
The correct answer is A because assets provide location, credentials, and other parameters needed to run actions. Assets are configurations that define how Phantom connects to external systems or devices, such as firewalls, endpoints, or threat intelligence sources. Assets specify the app, the IP address or hostname, the username and password, and any other settings required to run actions on the target system or device. The answer B is incorrect because assets do not provide hostnames, passwords, and other artifacts needed to run actions, which are data objects that can be created or retrieved by playbooks. The answer C is incorrect because assets do not provide Python code, REST API, and other capabilities needed to run actions, which are provided by apps. The answer D is incorrect because assets do not provide firewall, network, and data sources needed to run actions, which are external systems or devices that can be connected to by assets.
Reference: Splunk SOAR Admin Guide, page 45. Assets in Splunk Phantom are configurations that contain the necessary information for apps to connect to external systems and services. This information can include IP addresses, domain names, credentials like usernames and passwords, and other necessary parameters such as API keys or tokens. These parameters enable the apps to perform actions like running queries, executing commands, or gathering data. Assets do not provide the actual Python code, REST API capabilities, or network infrastructure; they are the bridge between the apps and the external systems with the configuration data needed for successful communication and action execution

NEW QUESTION # 64
Which of the following queries would return all artifacts that contain a SHA1 file hash?

- A. https://<PHANTOM_URL>/rest/artifact?_filter_cef_Sha1_contains=""
- B. https://<PHANTOM_URL>/rest/artifact?_filter_cef_md5_insull=false
- C. https://<PHANTOM_URL>/rest/artifact?_filter_cef_sha1_insull=False
- D. https://<PHANTOM_URL>/rest/artifact?_filter_sha1__insull=False

Answer: C

Explanation:
To retrieve all artifacts containing a SHA1 file hash via the Splunk SOAR REST API, the appropriate query would filter for artifacts where the 'cef_sha1' field is not null, indicating that a SHA1 hash is present. The correct REST API call should use the filter parameter _filter_cef_sha1__isnull=False (assuming 'sha1' is a typo and it should be 'sha1'). This query parameter is used to filter out artifacts that do not have a SHA1 hash, thus returning only those that do.

NEW QUESTION # 65
Which of the following is a best practice for use of the global block?

- A. Import packages which will be used within the playbook.
- B. Execute custom code after each run of the playbook.
- C. Execute code at the beginning of each run of the playbook.
- D. Declare outputs which will be selectable within playbook blocks.

Answer: A

Explanation:
Explanation
The correct answer is C because the global block can be used to import packages that will be used within the playbook. This can be useful for importing external libraries or custom modules that provide additional functionality or logic for the playbook. The answer A is incorrect because the global block cannot be used to execute code at the beginning of each run of the playbook, as the global block is only executed once when the playbook is loaded. The answer B is incorrect because the global block cannot be used to declare outputs that will be selectable within playbook blocks, as the outputs are declared in the individual blocks that produce them.

The answer D is incorrect because the global block cannot be used to execute custom code after each run of the playbook, as the global block is only executed once when the playbook is loaded. Reference: Splunk SOAR Playbook Development Guide, page 34.

NEW QUESTION # 66
Which of the following actions will store a compressed, secure version of an email attachment with suspected malware for future analysis?

- A. Use the Upload action of the Secure Store app to store the file in the database.
- B. Copy/paste the attachment into a note.
- C. Use the Files tab on the Investigation page to upload the attachment.
- D. Add a link to the file in a new artifact.

Answer: A

Explanation:
To securely store a compressed version of an email attachment suspected of containing malware for future analysis, the most effective approach within Splunk SOAR is to use the Upload action of the Secure Store app. This app is specifically designed to handle sensitive or potentially dangerous files by securely storing them within the SOAR database, allowing for controlled access and analysis at a later time. This method ensures that the file is not only safely contained but also available for future forensic or investigative purposes without risking exposure to the malware.

NEW QUESTION # 67
What does a user need to do to have a container with an event from Splunk use context-aware actions designed for notable events?

- A. Add a custom field to the container named event_id and set the custom field's data type to splunk notable event id.
- B. Include the event_id field in the search results and add a CEF definition to Phantom for event_id, datatype splunk notable event id.
- C. Rename the event_id field from the notable event to splunkNotableEventId.
- D. Include the notable event's event_id field and set the artifacts label to aplunk notable event id.

Answer: B

Explanation:
For a container in Splunk SOAR to utilize context-aware actions designed for notable events from Splunk, it is crucial to ensure that the notable event's unique identifier (event_id) is included in the search results pulled into SOAR. Moreover, by adding a Common Event Format (CEF) definition for the event_id field within Phantom, and setting its data type to something that denotes it as a Splunk notable event ID, SOAR can recognize and appropriately handle these identifiers. This setup facilitates the correct mapping and processing of notable event data within SOAR, enabling the execution of context-aware actions that are specifically tailored to the characteristics of Splunk notable events.

NEW QUESTION # 68
.....

searching on ➠ www.pdfvce.com □ □Pass4sure SPLK-2003 Pass Guide

- Unparalleled Splunk SPLK-2003 Key Concepts: Splunk Phantom Certified Admin Pass Guaranteed □ The page for free download of [SPLK-2003] on 【 www.examcollectionpass.com 】 will open immediately □SPLK-2003 Exam Overview
- SPLK-2003 Study Materials: Splunk Phantom Certified Admin - SPLK-2003 Actual Questions - SPLK-2003 Quiz Guide □ “ www.pdfvce.com ” is best website to obtain 《 SPLK-2003 》 for free download □New SPLK-2003 Dumps Sheet
- Latest SPLK-2003 Exam Questions □ Online SPLK-2003 Lab Simulation □ Instant SPLK-2003 Discount □ Search for ⇛ SPLK-2003 ⇚ and download exam materials for free through ▸ www.lead1pass.com ◂ □SPLK-2003 Valid Test Topics
- Pass SPLK-2003 Exam with Fantastic SPLK-2003 Key Concepts by Pdfvce □ Search for ➠ SPLK-2003 □ and download it for free immediately on “ www.pdfvce.com ” □Exam SPLK-2003 Cram
- SPLK-2003 Latest Test Format □ Latest SPLK-2003 Test Online □ SPLK-2003 Valid Exam Voucher □ Search for ➠ SPLK-2003 □ and easily obtain a free download on [www.actual4labs.com] □SPLK-2003 Valid Dumps Ppt
- SPLK-2003 Learning Materials - SPLK-2003 Study Guide - SPLK-2003 Test Braindumps □ Search for ➡ SPLK-2003 □□□ and obtain a free download on [www.pdfvce.com] □Online SPLK-2003 Lab Simulation
- SPLK-2003 Materials □ Latest SPLK-2003 Exam Price □ Latest Braindumps SPLK-2003 Book □ Search for □ SPLK-2003 □ and download it for free on “ www.torrentvce.com ” website □Latest SPLK-2003 Test Online
- myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, divorceparentshub.com, ahlebaitacademy.com, lineage95003.官網.com, techavally.com, blueskyacademy.in, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, 40bbk.com, Disposable vapes

What's more, part of that PassCollection SPLK-2003 dumps now are free: https://drive.google.com/open?id=1JD2n69KMovIsaXDwGAsgDmVz_a6M72lr