

# Hot Splunk SPLK-2003 Online Bootcamps Carefully Researched by Splunk Experienced Trainers



2025 Latest PrepAwayExam SPLK-2003 PDF Dumps and SPLK-2003 Exam Engine Free Share: <https://drive.google.com/open?id=1KMuo0XW5ekD4UMK2snDKSrs30egQjeZK>

Tens of thousands of our worthy customers have been benefited by our SPLK-2003 exam questions. Of course, your gain is definitely not just a SPLK-2003 certificate. Our SPLK-2003 study materials will change your working style and lifestyle. You will work more efficiently than others. Our SPLK-2003 Training Materials can play such a big role. What advantages does it have? You can spend a few minutes free downloading our demos to check it out. And you will be surprised by the high-quality.

Splunk SPLK-2003 certification exam consists of multiple-choice questions that cover various aspects of Splunk Phantom administration. SPLK-2003 exam is designed to test the candidate's understanding of Splunk Phantom's architecture, deployment, configuration, and management. SPLK-2003 exam also covers topics related to Splunk Phantom's integrations with other technologies, such as security information and event management (SIEM) systems and security orchestration, automation and response (SOAR) solutions.

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 Certification Exam is aimed at IT professionals who are responsible for managing Splunk Phantom in an enterprise environment. This includes security analysts, incident response teams, and IT administrators. Splunk Phantom Certified Admin certification is also useful for consultants and professionals who work with clients to implement and manage Splunk Phantom. The SPLK-2003 certification is a valuable credential that demonstrates a candidate's expertise in Splunk Phantom administration and can help to advance their career in the field of security operations and incident response.

>> **SPLK-2003 Online Bootcamps** <<

## **SPLK-2003 Test Quiz - Pdf SPLK-2003 Dumps**

The price for SPLK-2003 training materials is quite reasonable, and no matter you are a student at school or an employee in the company, you can afford the expense. You just think that you only need to spend some money, and you can pass the exam and get the certificate, which is quite self-efficient. In addition, SPLK-2003 Exam Dumps are edited by the professional experts, who are quite familiar with the professional knowledge and testing center, and the quality and accuracy can be guaranteed. We have 24 hours service stuff, and if you any questions about SPLK-2003 training materials, just contact us.

## **Splunk Phantom Certified Admin Sample Questions (Q52-Q57):**

### NEW QUESTION # 52

Which of the following are examples of things commonly done with the Phantom REST APP

- A. Use SQL queries; use curl to create a container and add artifacts to it; remove temporary lists.
- **B. Use Django queries; use curl to create a container and add artifacts to it; remove temporary lists.**
- C. Use Django queries; use curl to create a container and add artifacts to it; add action blocks.
- D. Use Django queries; use Docker to create a container and add artifacts to it; remove temporary lists.

**Answer: B**

Explanation:

Explanation

The correct answer is A because using Django queries, using curl to create a container and add artifacts to it, and removing temporary lists are examples of things commonly done with the Phantom REST APP. The Phantom REST APP is a built-in app that allows you to interact with the Phantom server using REST API calls. You can use the run query action to execute Django queries on the Phantom database and return the results as JSON. You can use the curl command to send HTTP requests to the Phantom server and perform various operations, such as creating containers, adding artifacts, running playbooks, etc. You can use the remove list action to delete temporary lists that are no longer needed. See Splunk SOAR Documentation for more details.

### NEW QUESTION # 53

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. Browse to the Django Filter Query Editor in the Administration panel.
- D. Install the SOAR Django App first, then configure the search query in the App editor.

**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 # 54

Which of the following is the complete list of the types of backups that are supported by Phantom?

- **A. Full and incremental backups.**
- B. Full and delta backups.
- C. Full backups.
- D. Full, delta, and incremental backups.

**Answer: A**

Explanation:

Splunk Phantom supports different types of backups to safeguard data. Full backups create a complete copy of the current state of the system, while incremental backups only save the changes made since the last backup. This approach allows for efficient use of storage space and faster backups after the initial full backup. Delta backups, which would save changes since the last full or incremental backup, are not a standard part of Phantom's backup capabilities according to available documentation. Therefore, the complete list of backups supported by Phantom would be Full and Incremental backups.

#### NEW QUESTION # 55

During a second test of a playbook, a user receives an error that states: 'an empty parameters list was passed to phantom.act()'. What does this indicate?

- A. The playbook is using an incorrect container.
- **B. The playbook debugger's scope is set to new.**
- C. The playbook debugger's scope is set to all.
- D. The container has artifacts not parameters.

**Answer: B**

Explanation:

Explanation

The correct answer is C because the error message indicates that the playbook debugger's scope is set to new.

The scope option determines which containers are used for debugging the playbook. If the scope is set to new, the debugger will only use containers that are created after the debugger is started. If the scope is set to all, the debugger will use all containers that match the playbook's filter criteria. The error message means that the debugger did not find any new containers with parameters to pass to the phantom.act() function. See Splunk SOAR Documentation for more details.

#### NEW QUESTION # 56

In a playbook, more than one Action block can be active at one time. What is this called?

- **A. Parallel Processing**
- B. Juggle Processing
- C. Serial Processing
- D. Multithreaded Processing

**Answer: A**

Explanation:

In Splunk SOAR, when a playbook is designed such that more than one Action block is active at the same time, it is referred to as 'Parallel Processing'. This allows for multiple actions to be executed concurrently, which can significantly speed up the execution of a playbook as it does not have to wait for one action to complete before starting another. Parallel processing enables more efficient use of resources and time, particularly in complex playbooks that perform numerous actions.

#### NEW QUESTION # 57

.....

We will provide you with comprehensive study experience by give you SPLK-2003 free study material & Splunk exam prep torrent. The questions & answers from the Splunk practice torrent are all valid and accurate, made by the efforts of a professional IT team. The authority and validity of Splunk SPLK-2003 training practice are the guarantee for all the IT candidates. We arrange our experts to check the update every day. Once there is any new technology about SPLK-2003 Exam Dumps, we will add the latest questions into the SPLK-2003 study pdf, and remove the useless study material out, thus to ensure the SPLK-2003 exam torrent you get is the best valid and latest. So 100% pass is our guarantee.

**SPLK-2003 Test Quiz:** <https://www.prepawayexam.com/Splunk/braindumps.SPLK-2003.etc.file.html>

- SPLK-2003 Official Study Guide ☐ New SPLK-2003 Test Dumps ☐ SPLK-2003 Frenquent Update ☐ Search for ➡ SPLK-2003 ☐ and obtain a free download on ➤ [www.torrentvce.com](http://www.torrentvce.com) ☐ ☐ SPLK-2003 Reliable Exam Answers
- SPLK-2003 Official Study Guide ☐ Valid SPLK-2003 Test Vce ☐ Knowledge SPLK-2003 Points ☐ Search for ➤ SPLK-2003 ☐ and obtain a free download on ➤ [www.pdfvce.com](http://www.pdfvce.com) < ☐ Original SPLK-2003 Questions
- SPLK-2003 Reliable Exam Answers ☐ Original SPLK-2003 Questions ☐ SPLK-2003 Reliable Exam Online ☐

BONUS!!! Download part of PrepAwayExam SPLK-2003 dumps for free: <https://drive.google.com/open?id=1KMuo0XW5ekD4UMK2snDKSrs30egQjeZK>