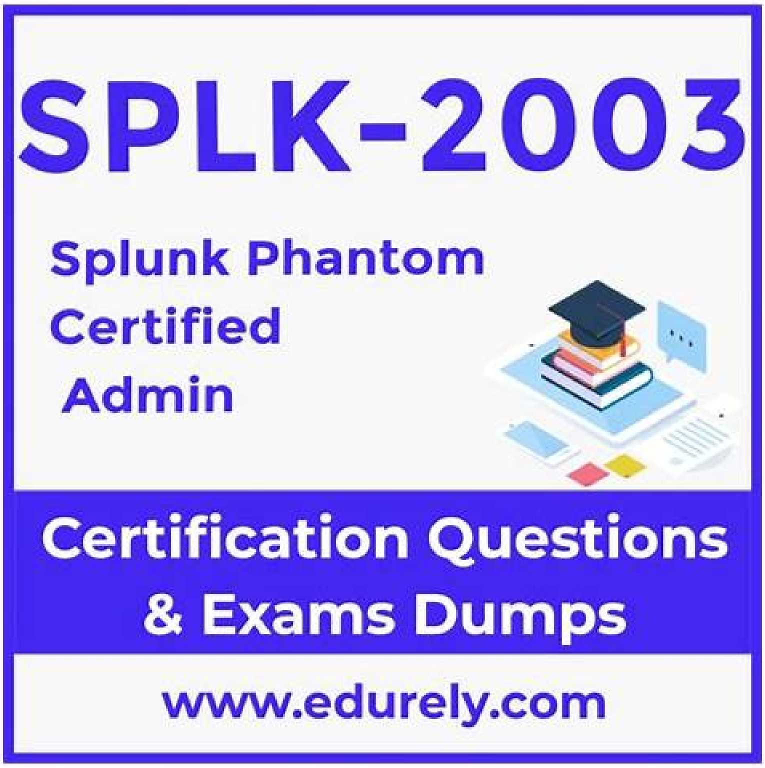
Hot Reliable SPLK-2003 Exam Camp Free PDF | Valid Test SPLK-2003 Questions Pdf: Splunk Phantom Certified Admin


SPLK-2003
Splunk Phantom Certified Admin
Certification Questions & Exams Dumps
www.edurely.com

What's more, part of that TestBraindump SPLK-2003 dumps now are free: https://drive.google.com/open?id=1OUJET7tdINl1D0sjdAMnB5E6r-lK0fl-

TestBraindump Splunk Phantom Certified Admin (SPLK-2003) exam questions are consistently updated to make sure they are according to the Splunk latest exam syllabus. If you choose TestBraindump, you can be sure that you'll always get the updated and real SPLK-2003 exam questions, which are essential to go through the SPLK-2003 test in one go. In addition, we also offer up to 1 year of free Splunk SPLK-2003 certification exam question updates. These free updates ensure that candidates get access to the latest Splunk exam questions even after they have made their initial purchase.

The Splunk Phantom Certified Admin certification is ideal for IT professionals who want to enhance their skills in Splunk Phantom and its administration. It is also suitable for security analysts, SOC analysts, incident responders, and IT administrators who want to automate their security operations and improve their overall security posture. Splunk Phantom Certified Admin certification is recognized globally and is highly valued by employers.

>> Reliable SPLK-2003 Exam Camp <<

Test SPLK-2003 Questions Pdf, SPLK-2003 Test Study Guide

Our company is considerably cautious in the selection of talent and always hires employees with store of specialized knowledge and skills on our SPLK-2003 exam questions. All the members of our experts and working staff maintain a high sense of responsibility, which is why there are so many people choose our SPLK-2003 Exam Materials and to be our long-term partner. For we carry forward the spirit of "firm & indomitable, developing & innovative, achieving the first class", serving customers with all our heart and soul with our wonderful SPLK-2003 practice braindumps.

Splunk Phantom Certified Admin Sample Questions (Q26-Q31):

NEW QUESTION # 26

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

Answer: B

Explanation:
The correct answer is C 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. To ensure that only members of the admin role can execute specific playbooks on the Phantom server, the most effective approach is to manage role-based access controls (RBAC) directly. By configuring the system to remove the "Execute Playbook" capability from all roles except for the admin role, you can enforce this rule. This method leverages Phantom's built-in RBAC mechanisms to restrict playbook execution privileges. It is a straightforward and secure way to ensure that only users with the necessary administrative privileges can initiate the execution of sensitive or critical playbooks, thus maintaining operational security and control.

NEW QUESTION # 27
What is enabled if the Logging option for a playbook's settings is enabled?

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

Answer: B

NEW QUESTION # 28
After a successful POST to a Phantom REST endpoint to create a new object what result is returned?

- A. The PostGres UUID.
- B. The new object ID.
- C. The full CEF name.
- D. The new object name.

Answer: B

Explanation:
The correct answer is A because after a successful POST to a Phantom REST endpoint to create a new object, the result returned is the new object ID. The object ID is a unique identifier for each object in Phantom, such as a container, an artifact, an action, or a playbook. The object ID can be used to retrieve, update, or delete the object using the Phantom REST API. The answer B is incorrect because after a successful POST to a Phantom REST endpoint to create a new object, the result returned is not the new object name, which is a human-readable name for the object. The object name can be used to search for the object using the Phantom web interface. The answer C is incorrect because after a successful POST to a Phantom REST endpoint to create a new object, the result returned is not the full CEF name, which is a standard format for event data. The full CEF name can be used to access the CEF fields of an artifact using the Phantom REST API. The answer D is incorrect because after a successful POST to a Phantom REST endpoint to create a new object, the result returned is not the PostGres UUID, which is a unique identifier for each row in a PostGres database. The PostGres UUID is not exposed to the Phantom REST API. Reference: Splunk SOAR REST API Guide, page 17. When a POST request is made to a Phantom REST endpoint to create a new object, such as an event, artifact, or container, the typical response includes the ID of the newly created object. This ID is a unique identifier that can be used to reference the object within the system for future operations, such as updating, querying, or deleting the object. The response does not usually include the full name or other specific details of the object, as the ID is the most important piece of information needed immediately after creation for reference purposes.

NEW QUESTION # 29
Which of the following can be edited or deleted in the Investigation page?

- A. Action results
- B. Approval records
- C. Artifact values
- D. Comments

Answer: D

Explanation:
On the Investigation page in Splunk SOAR, users have the ability to edit or delete comments associated with an event or a container. Comments are generally used for collaboration and to provide additional context to an investigation. While action results, approval records, and artifact values are typically not editable or deletable to maintain the integrity of the investigative data, comments are more flexible and can be managed by users to reflect the current state of the investigation.
Investigation page allows you to view and edit various information and data related to an event or a case. One of the things that you can edit or delete in the Investigation page is the comments that you or other users have added to the activity feed. Comments are a way of communicating and collaborating with other users during the investigation process. You can edit or delete your own comments by clicking on the three-dot menu icon next to the comment and selecting the appropriate option. You can also reply to other users' comments by clicking on the reply icon.

NEW QUESTION # 30
Which of the following is a step when configuring event forwarding from Splunk to Phantom?

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

Answer: A

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 # 31
......

The software version is one of the three versions of our SPLK-2003 exam prep. The software version has many functions which are different with other versions'. On the one hand, the software version of SPLK-2003 test questions can simulate the real examination for all users. By actually simulating the test environment, you will have the opportunity to learn and correct self-shortcoming in study course. On the other hand, although you can just apply the software version in the windows operation system, the software version of SPLK-2003 Exam Prep will not limit the number of your computer. If you use the software version, you can download the app more than one computer, but you can just apply the software version in the windows operation system. We believe the software version of our SPLK-2003 test torrent will be very useful for you, we hope you can pass you exam and get your certificate successfully.

Test SPLK-2003 Questions Pdf: https://www.testbraindump.com/SPLK-2003-exam-prep.html

- New SPLK-2003 Test Online □ SPLK-2003 Reliable Test Braindumps □ New SPLK-2003 Test Online □ Simply search for ➤ SPLK-2003 □ for free download on ➥ www.pass4test.com □ ➡SPLK-2003 Study Guide Pdf
- Reliable SPLK-2003 Exam Camp - 100% Pass Quiz First-grade Splunk SPLK-2003 - Test Splunk Phantom Certified Admin Questions Pdf □ Search for （ SPLK-2003 ） and obtain a free download on 《 www.pdfvce.com 》 □Free SPLK-2003 Test Questions
- Free PDF Quiz 2026 SPLK-2003: Splunk Phantom Certified Admin Marvelous Reliable Exam Camp □ Download ✔

SPLK-2003 □✔□ for free by simply entering [www.exam4labs.com] website □Complete SPLK-2003 Exam Dumps

- SPLK-2003 Study Guide Pdf □ SPLK-2003 Reliable Exam Preparation □ SPLK-2003 Hottest Certification □ Go to website “ www.pdfvce.com ” open and search for ☀ SPLK-2003 □☀□ to download for free □SPLK-2003 Brain Dump Free
- New SPLK-2003 Test Online □ SPLK-2003 Valid Exam Dumps □ SPLK-2003 Study Guide Pdf □ Open ➻ www.prepawayete.com □ enter { SPLK-2003 } and obtain a free download □SPLK-2003 Hottest Certification
- Reliable SPLK-2003 Exam Camp - 100% Pass Quiz First-grade Splunk SPLK-2003 - Test Splunk Phantom Certified Admin Questions Pdf □ Download ⇛ SPLK-2003 ⇚ for free by simply entering ✔ www.pdfvce.com □✔□ website ↖SPLK-2003 Valid Exam Bootcamp
- Splunk Phantom Certified Admin Exam Simulator - SPLK-2003 Free Demo - SPLK-2003 Training Pdf □□ Easily obtain free download of 「 SPLK-2003 」 by searching on □ www.dumpsquestion.com □ ℹLatest SPLK-2003 Test Simulator
- Free SPLK-2003 Test Questions □ SPLK-2003 Valid Exam Bootcamp □ SPLK-2003 Vce File □ Search for ▶ SPLK-2003 ◀ on ☀ www.pdfvce.com □☀□ immediately to obtain a free download □SPLK-2003 Vce Torrent
- High Hit-Rate Splunk - SPLK-2003 - Reliable Splunk Phantom Certified Admin Exam Camp □ Easily obtain free download of ➥ SPLK-2003 □ by searching on ➠ www.examcollectionpass.com □ □Latest SPLK-2003 Test Simulator
- SPLK-2003 Dumps Save Your Money with Up to one year of Free Updates □ Download { SPLK-2003 } for free by simply entering □ www.pdfvce.com □ website □Latest SPLK-2003 Test Simulator
- Splunk Phantom Certified Admin exam training solutions - SPLK-2003 latest practice questions - Splunk Phantom Certified Admin free download material □ Enter □ www.examdiscuss.com □ and search for ▷ SPLK-2003 ◁ to download for free □Latest SPLK-2003 Test Simulator
- www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, lms.treasurehall.net, myportal.utt.edu.tt, Disposable vapes

P.S. Free & New SPLK-2003 dumps are available on Google Drive shared by TestBraindump: https://drive.google.com/open?id=1OUJET7tdINl1D0sjdAMnB5E6r-IK0fl-