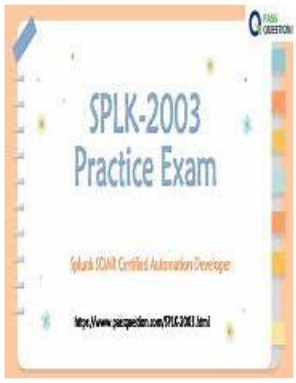
SPLK-2003 Exam Prep & SPLK-2003 Pdf Files



DOWNLOAD the newest ActualCollection SPLK-2003 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1bBvZppvcC9zO5hJcKVGd5NHgJBi6hVGx

ActualCollection offers up-to-date Splunk SPLK-2003 practice material consisting of three formats that will prove to be vital for you. You can easily ace the Splunk Phantom Certified Admin (SPLK-2003) exam on the first attempt if you prepare with this material. The Splunk SPLK-2003 Exam Dumps have been made under the expert advice of 90,000 highly experienced Splunk professionals from around the globe. They assure that anyone who prepares from it will get Splunk SPLK-2003 certified on the first attempt.

To prepare for the Splunk SPLK-2003 Exam, candidates can take the Splunk Phantom Certified Admin course, which covers all the topics that are relevant to the exam. This course is available online and includes hands-on exercises and simulations that help candidates develop their skills and knowledge. Candidates can also access various resources, such as official Splunk documentation, whitepapers, and forums, to supplement their learning.

>> SPLK-2003 Exam Prep <<

2025 SPLK-2003 Exam Prep 100% Pass | High Pass-Rate Splunk Splunk Phantom Certified Admin Pdf Files Pass for sure

To help you get the Splunk exam certification, we provide you with the best valid SPLK-2003 pdf prep material. The customizable and intelligence SPLK-2003 test engine will bring you to a high efficiency study way. The SPLK-2003 test engine contains self-assessment features like marks, progress charts, etc. Besides, the Easy-to-use SPLK-2003 layout will facilitate your preparation for SPLK-2003 real test. You can pass your SPLK-2003 certification without too much pressure.

Earning the Splunk Phantom Certified Admin certification can benefit professionals in a variety of roles, including security analysts, security engineers, and IT professionals. Splunk Phantom Certified Admin certification demonstrates a solid understanding of Splunk Phantom and the ability to effectively manage and automate security operations. Additionally, the certification can enhance job opportunities and increase earning potential in the cybersecurity industry.

The SPLK-2003 exam is intended for IT professionals who are responsible for managing and administering Splunk Phantom in their organization. This includes security analysts, automation engineers, security operations center (SOC) analysts, and IT administrators. SPLK-2003 Exam Tests candidates on their understanding of Splunk Phantom architecture, deployment, configuration, and administration, as well as their ability to troubleshoot common issues and perform routine maintenance tasks.

Splunk Phantom Certified Admin Sample Questions (Q68-Q73):

NEW QUESTION # 68
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. Make sure the Execute Playbook capability is removed from al roles except admin.
- B. Add a tag with restricted access to the restricted playbooks.
- C. Add a filter block to al restricted playbooks that Titters for runRole - "Admin".
- D. Place restricted playbooks in a second source repository that has restricted access.

Answer: A

Explanation:
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.
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 # 69
Which of the following queries would return all failed playbook runs from the REST API?

- A. https://<PHANTOM_URL>/rest/playbook_run?_search_status=failed
- B. https://<PHANTOM_URL>/rest/playbook_run?_filter_status failed
- C. https://<PHANTOM_URL>/rest/playbook_run?_query_status="failed"
- D. https://<PHANTOM_URL>/rest/playbook_run?_filter_status "failed"

Answer: C

NEW QUESTION # 70
Which of the following will show all artifacts that have the term results in a filePath CEF value?

- A. ...rest/artifacts/filePath="%results%"
- B. .../rest/artifact?_filter_cef_filePath_icontain="results"
- C. .../result/artifacts/cef/filePath= '%results%"
- D. .../result/artifact?_query_cef_filepath_icontains="results

Answer: B

Explanation:
The correct answer is A because the _filter parameter is used to filter the results based on a field value, and the icontain operator is used to perform a case-insensitive substring match. The filePath field is part of the Common Event Format (CEF) standard, and the cef_ prefix is used to access CEF fields in the REST API. The answer B is incorrect because it uses the wrong syntax for the REST

API. The answer C is incorrect because it uses the wrong endpoint (result instead of artifact) and the wrong syntax for the REST API. The answer D is incorrect because it uses the wrong syntax for the REST API and the wrong spelling for the icontains operator.
Reference: Splunk SOAR REST API Guide, page 18.
To query and display all artifacts that contain the term "results" in a filePath CEF (Common Event Format) value, using the REST API endpoint with a filter parameter is effective. The filter _filter_cef_filePath_icontain="results" is applied to search within the artifact data for filePath fields that contain the term "results", disregarding case sensitivity. This method allows users to precisely locate and work with artifacts that meet specific criteria, aiding in the investigation and analysis processes within Splunk SOAR.

NEW QUESTION # 71
After a playbook has run, where are the results stored?

- A. Log file
- B. Case
- C. Container
- D. Splunk Index

Answer: C

Explanation:
Explanation
The correct answer is C because after a playbook has run, the results are stored in the container that triggered the playbook. The container is a data object that represents an event or a case in Phantom. The container contains information such as the name, the description, the severity, the status, the owner, and the labels of the event or case. The container also contains the artifacts, the action results, the comments, the notes, and the phases and tasks associated with the event or case. The answer A is incorrect because after a playbook has run, the results are not stored in a Splunk index, which is a data structure that stores events from various data sources in Splunk. The Splunk index is not directly accessible by Phantom, but can be queried by Phantom using the Splunk app. The answer B is incorrect because after a playbook has run, the results are not stored in a case, which is a type of container that represents a security incident in Phantom. The case is a subset of the container, and not all containers are cases. The answer D is incorrect because after a playbook has run, the results are not stored in a log file, which is a file that records the activities or events that occur in a system or a process. The log file is not a data object in Phantom, but can be a data source for Phantom. Reference: Splunk SOAR User Guide, page 19.

NEW QUESTION # 72
Where can the Splunk App for SOAR Export be downloaded from?

- A. SOAR Community and GitHub.
- B. Splunk Answers and Splunkbase.
- C. Splunkbase and SOAR Community.
- D. GitHub and Splunkbase.

Answer: D

Explanation:
The Splunk App for SOAR Export can be downloaded from both GitHub and Splunkbase.
Splunkbase is the official source for Splunk apps, where users can find, try, and download apps that enhance and extend the capabilities of Splunk, including the Splunk App for SOAR Export.
GitHub is also a common platform for sharing and collaborating on code, including Splunk apps and integrations. It is important to ensure that you are downloading from the official repository or author to avoid any security risks.

NEW QUESTION # 73
.....

- Free PDF 2025 Pass-Sure Splunk SPLK-2003 Exam Prep □ Open ▹ www.pdfvce.com ◃ and search for 「 SPLK-2003 」 to download exam materials for free □SPLK-2003 Latest Practice Questions
- SPLK-2003 Real Dumps Free □ SPLK-2003 Latest Practice Questions □ Sure SPLK-2003 Pass □ Copy URL ➥ www.itcerttest.com □ open and search for 【 SPLK-2003 】 to download for free □VCE SPLK-2003 Dumps
- SPLK-2003 Real Dumps Free □ Test SPLK-2003 Preparation □ SPLK-2003 Real Exam Questions □ Search for ➽ SPLK-2003 □ and obtain a free download on ✔ www.pdfvce.com □✔□ □Reliable SPLK-2003 Exam Preparation
- Free PDF 2025 Pass-Sure Splunk SPLK-2003 Exam Prep □ Copy URL [www.examcollectionpass.com] open and search for ➽ SPLK-2003 □ to download for free □Reliable SPLK-2003 Exam Braindumps
- Quiz 2025 SPLK-2003: Authoritative Splunk Phantom Certified Admin Exam Prep □ Open （ www.pdfvce.com ） enter 「 SPLK-2003 」 and obtain a free download □Sure SPLK-2003 Pass
- SPLK-2003 Reliable Test Review □ Test SPLK-2003 Preparation ✔ SPLK-2003 Test Price □ Open 「 www.examsreviews.com 」 enter ▹ SPLK-2003 ◃ and obtain a free download □Valid SPLK-2003 Test Questions
- Valid SPLK-2003 Test Questions □ SPLK-2003 Latest Practice Questions □ VCE SPLK-2003 Dumps □ Search on { www.pdfvce.com } for ➠ SPLK-2003 □ to obtain exam materials for free download □SPLK-2003 Real Dumps Free
- Pass Guaranteed Quiz 2025 Trustable SPLK-2003: Splunk Phantom Certified Admin Exam Prep □ Open website ✔ www.real4dumps.com □✔□ and search for " SPLK-2003 " for free download □Practice SPLK-2003 Mock
- Free PDF 2025 Pass-Sure Splunk SPLK-2003 Exam Prep □ Easily obtain ➠ SPLK-2003 □ for free download through 「 www.pdfvce.com 」 □SPLK-2003 Reliable Test Review
- Quiz 2025 SPLK-2003: Authoritative Splunk Phantom Certified Admin Exam Prep □ Search for 《 SPLK-2003 》 and download exam materials for free through ➽ www.vceengine.com □ □SPLK-2003 Actual Exam
- 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, lms.ait.edu.za, 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, www.stes.tyc.edu.tw, 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, 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, mobile-maths.com, 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, Disposable vapes

P.S. Free 2025 Splunk SPLK-2003 dumps are available on Google Drive shared by ActualCollection: https://drive.google.com/open?id=1bBvZppvcC9zO5hJcKVGd5NHgJBi6hVGx