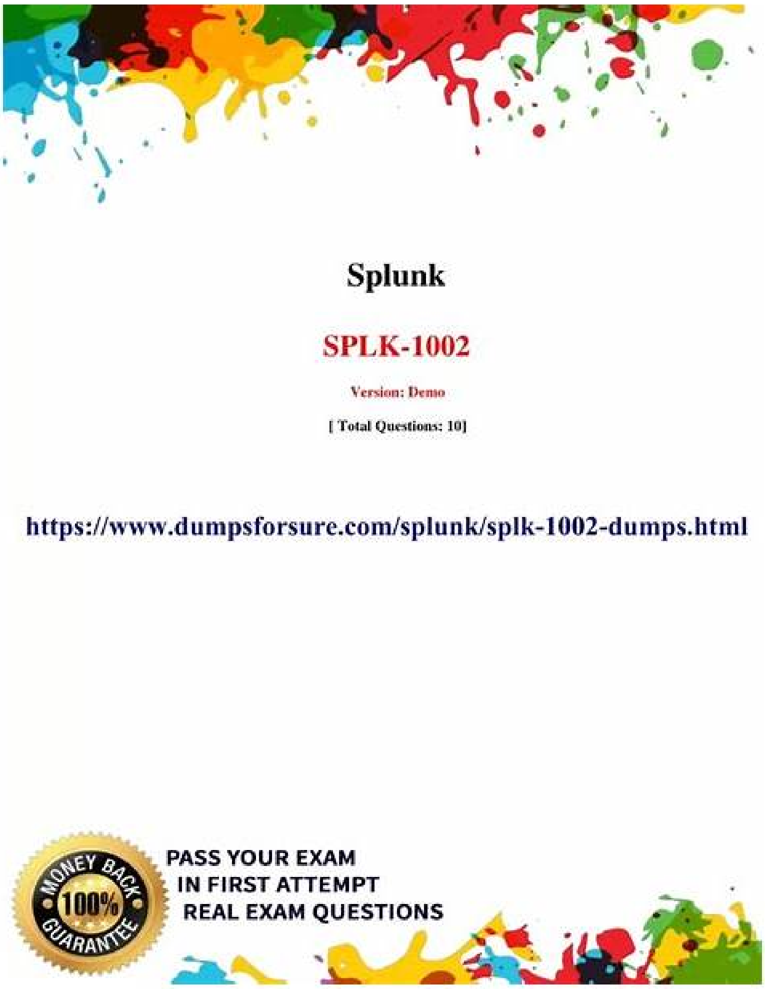
2025 Newest SPLK-2003–100% Free Real Exam Answers | Pdf SPLK-2003 Exam Dump



Splunk

SPLK-1002

Version: Demo

[Total Questions: 10]

https://www.dumpsforsure.com/splunk/splk-1002-dumps.html

P.S. Free & New SPLK-2003 dumps are available on Google Drive shared by Prep4King: https://drive.google.com/open?id=1InJqeTowukRjPnkixaTijRoSybH-kn3d

Our Prep4King website try our best for the majority of examinees to provide the best and most convenient service. Under the joint efforts of everyone for many years, the passing rate of Prep4King Splunk's SPLK-2003 Certification Exam has reached as high as100%. If you buy our SPLK-2003 exam certification training materials, we will also provide one year free renewal service. Hurry up!

One of the main unique qualities of the Prep4King Splunk Exam Questions is its ease of use. Our practice exam simulators are user and beginner friendly. You can use Splunk Phantom Certified Admin (SPLK-2003) PDF dumps and Web-based software without installation. Splunk Phantom Certified Admin (SPLK-2003) PDF questions work on all the devices like smartphones, Macs, tablets, Windows, etc. We know that it is hard to stay and study for the Splunk Phantom Certified Admin (SPLK-2003) exam dumps in one place for a long time.

>> SPLK-2003 Real Exam Answers <<

Free PDF Splunk - Professional SPLK-2003 Real Exam Answers

We have free demos of our SPLK-2003 study materials for your reference, as in the following, you can download which SPLK-2003 exam materials demo you like and make a choice. We have three versions of our SPLK-2003 exam guide, so we have according three versions of free demos. Therefore, if you really have some interests in our SPLK-2003 Study Materials, then trust our professionalism, we promise a full refund if you fail exam.

Splunk Phantom Certified Admin Sample Questions (Q96-Q101):

NEW QUESTION # 96
Which of the following accurately describes the Files tab on the Investigate page?

- A. Files tab items cannot be added to investigations. Instead, add them to action blocks.
- B. A user can upload the output from a detonate action to the the files tab for further investigation.
- C. Phantom memory requirements remain static, regardless of Files tab usage.
- D. Files tab items and artifacts are the only data sources that can populate active cases.

Answer: B

Explanation:
The Files tab on the Investigate page allows the user to upload, download, and view files related to an investigation. A user can upload the output from a detonate action to the Files tab for further investigation, such as analyzing the file metadata, content, or hash. Files tab items and artifacts are not the only data sources that can populate active cases, as cases can also include events, tasks, notes, and comments. Files tab items can be added to investigations by using the add file action block or the Add File button on the Files tab.
Phantom memory requirements may increase depending on the Files tab usage, as files are stored in the Phantom database.
The Files tab on the Investigate page in Splunk Phantom is an area where users can manage and analyze files related to an investigation. Users can upload files, such as outputs from a 'detonate file' action which analyzes potentially malicious files in a sandbox environment. The files tab allows users to store and further investigate these outputs, which can include reports, logs, or any other file types that have been generated or are relevant to the investigation. The Files tab is an integral part of the investigation process, providing easy access to file data for analysis and correlation with other incident data.

NEW QUESTION # 97
Which of the following is a step when configuring event forwarding from Splunk to Phantom?

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

Answer: D

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 # 98
When the Splunk App for SOAR Export executes a Splunk search, which activities are completed?

- A. CIM fields are mapped to CEF fields and a container is created on the SOAR server.
- B. CIM fields are mapped to CEF and a container is created on the Splunk server.
- C. CEF fields are mapped to CIM fields and a container is created on the SOAR server.
- D. CEF fields are mapped to CIM and a container is created on the Splunk server.

Answer: A

Explanation:
When the Splunk App for SOAR Export executes a Splunk search, it typically involves mapping Common Information Model (CIM) fields from Splunk to the Common Event Format (CEF) used by SOAR, after which a container is created on the SOAR server to house the related artifacts and information. This process allows for the integration of data between Splunk, which uses CIM for data normalization, and Splunk SOAR, which uses CEF as its data format for incidents and events.
Splunk App for SOAR Export is responsible for sending data from your Splunk Enterprise or Splunk Cloud instances to Splunk SOAR. The Splunk App for SOAR Export acts as a translation service between the Splunk platform and Splunk SOAR by

performing the following tasks:
*Mapping fields from Splunk platform alerts, such as saved searches and data models, to CEF fields.
*Translating CIM fields from Splunk Enterprise Security (ES) notable events to CEF fields.
*Forwarding events in CEF format to Splunk SOAR, which are stored as artifacts.
Therefore, option B is the correct answer, as it states the activities that are completed when the Splunk App for SOAR Export executes a Splunk search. Option A is incorrect, because CEF fields are not mapped to CIM fields, but the other way around. Option C is incorrect, because a container is not created on the Splunk server, but on the SOAR server. Option D is incorrect, because a container is not created on the Splunk server, but on the SOAR server.
1: Web search results from search_web(query="Splunk SOAR Automation Developer Splunk App for SOAR Export")

NEW QUESTION # 99
What are the differences between cases and events?

- A. Cases: contain a collection of containers.
  Events: contain potential threats.
- B. Cases: incidents with a known violation and a plan for correction.
  Events: occurrences in the system that may require a response.
- C. Case: potential threats.
  Events: identified as a specific kind of problem and need a structured approach.
- D. Cases: only include high-level incident artifacts.
  Events: only include low-level incident artifacts.

Answer: A

Explanation:
In Splunk SOAR, an event is a security occurrence that may require a response. It is ingested from a third-party source and can be labeled to group related events together. The default label for containers is "Events," which signifies potential threats. A case, on the other hand, is a container that holds several containers, consolidating multiple events into one logical management unit. Cases can include artifacts and external evidence such as screen captures, analyst notes, and event data from third-party products. They are used to manage and analyze investigation data tied to specific security events and incidents, providing a structured approach to incident response.

NEW QUESTION # 100
After a successful POST to a Phantom REST endpoint to create a new object what result is returned?

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

Answer: B

NEW QUESTION # 101
......

We all know that it is not easy to prepare the SPLK-2003 exam; there are thousands of candidates to compete with you. So it is a fierce competition. If you want to win out in the exam, you need the professional study materials to guide you. Our SPLK-2003 Study Materials are confident to ensure that you will acquire the certificate. And the pass rate of our SPLK-2003 practice guide is high to 98% to 100%.

Pdf SPLK-2003 Exam Dump: https://www.prep4king.com/SPLK-2003-exam-prep-material.html

Get the test SPLK-2003 certification is not achieved overnight, we need to invest a lot of time and energy to review, and the review process is less a week or two, more than a month or two, or even half a year, so SPLK-2003 exam questions are one of the biggest advantage is that it is the most effective tools for saving time for users, It will help you pass your SPLK-2003 exam in shortest time.

The Five Layers of Security, Cisco Log Severity Levels, Get the test SPLK-2003 certification is not achieved overnight, we need to invest a lot of time and energy to review, and the review process is less a week or two, more than a month or two, or even half a year, so SPLK-2003 Exam Questions are one of the biggest advantage is that it is the most effective tools for saving time for users.

Authoritative SPLK-2003 Real Exam Answers - Pass SPLK-2003 in One Time - Complete Pdf SPLK-2003 Exam Dump

It will help you pass your SPLK-2003 exam in shortest time, If a question specifies that you must choose multiple correct answers, you must select the exact number SPLK-2003 of correct answers determined in the question to earn a point for that item.

We are all ordinary human beings, They can also have an understanding of their mastery degree of our SPLK-2003 study materials.

- Valid SPLK-2003 Exam Objectives □ Valid SPLK-2003 Exam Objectives □ SPLK-2003 New Braindumps Pdf □ Copy URL ➤ www.lead1pass.com □ open and search for 【 SPLK-2003 】 to download for free □Top SPLK-2003 Dumps
- Splunk - SPLK-2003 - Splunk Phantom Certified Admin Real Exam Answers □ Immediately open ✔ www.pdfvce.com □✔□ and search for 「 SPLK-2003 」 to obtain a free download □Exam Dumps SPLK-2003 Collection
- Quiz Authoritative SPLK-2003 - Splunk Phantom Certified Admin Real Exam Answers □ Search for ➡ SPLK-2003 □□□ and download exam materials for free through （ www.pdfdumps.com ） □SPLK-2003 New APP Simulations
- Reliable SPLK-2003 Exam Sims □ SPLK-2003 Exam Exercise □ Exam SPLK-2003 Online □ Download “ SPLK-2003 ” for free by simply entering 【 www.pdfvce.com 】 website □Learning SPLK-2003 Materials
- Latest SPLK-2003 Test Questions □ Cert SPLK-2003 Guide □ SPLK-2003 New Braindumps Pdf □ Go to website 《 www.examsreviews.com 》 open and search for “ SPLK-2003 ” to download for free □Exam Dumps SPLK-2003 Collection
- 100% Pass Quiz 2025 Splunk Latest SPLK-2003: Splunk Phantom Certified Admin Real Exam Answers □ Download ✔ SPLK-2003 □✔□ for free by simply searching on “ www.pdfvce.com ” □SPLK-2003 Reliable Test Pattern
- Valid SPLK-2003 Test Pass4sure □ Exam SPLK-2003 Online ↙ Exam Dumps SPLK-2003 Collection □ Search for □ SPLK-2003 □ and easily obtain a free download on ➡ www.pdfdumps.com □□□ □Valid SPLK-2003 Exam Objectives
- Cert SPLK-2003 Guide □ Exam SPLK-2003 Online □ Exam Dumps SPLK-2003 Collection □ Download ✔ SPLK-2003 □✔□ for free by simply entering □ www.pdfvce.com □ website □Test SPLK-2003 Dumps Free
- 2025 SPLK-2003 Real Exam Answers 100% Pass | Reliable SPLK-2003: Splunk Phantom Certified Admin 100% Pass □ □ Search for ▹ SPLK-2003 ◃ on ☀ www.testsdumps.com □☀□ immediately to obtain a free download □Reliable SPLK-2003 Exam Sims
- Valid SPLK-2003 Test Pass4sure □ Latest SPLK-2003 Exam Test □ Top SPLK-2003 Dumps □ Open website “ www.pdfvce.com ” and search for [SPLK-2003] for free download ⤴Reliable SPLK-2003 Exam Sims
- Cert SPLK-2003 Guide □ Test SPLK-2003 Dumps Free □ Test SPLK-2003 Dumps Free □ Easily obtain ➥ SPLK-2003 □ for free download through “ www.prep4away.com ” □Reliable SPLK-2003 Exam Sims
- dz34.pushd.cn, www.stes.tyc.edu.tw, leowood610.anchor-blog.com, www.stes.tyc.edu.tw, pct.edu.pk, www.stes.tyc.edu.tw, learn-school.webtemplates.in, bbs.tejiegm.com, lineage95003.官網.com, nilocman.xzblogs.com, Disposable vapes

What's more, part of that Prep4King SPLK-2003 dumps now are free: https://drive.google.com/open?id=1InJqeTowukRjPnkixaTijRoSybH-kn3d