

Valid Exam SPLK-2003 Braindumps - Valid SPLK-2003 Exam Review



BONUS!!! Download part of VCEdumps SPLK-2003 dumps for free: https://drive.google.com/open?id=1oJih4yU_nH2FcqcSBkci5vD4J-Veq6uw

We assure you that we are focused on providing you with guidance about our SPLK-2003 exam question, but all services are free. If you encounter installation problems, we will have professionals to provide you with remote assistance. Of course, we will humbly accept your opinions on our SPLK-2003 Quiz guide. If you have good suggestions to make better use of our SPLK-2003 test prep, we will accept your proposal and make improvements. Each of your progress is our driving force. We sincerely serve for you any time.

Splunk SPLK-2003 (Splunk Phantom Certified Admin) Exam is a certification exam designed for professionals who wish to demonstrate their proficiency in the administration of Splunk Phantom. SPLK-2003 exam is intended for individuals who want to enhance their knowledge and skills in the areas of incident response, security automation, and orchestration using Splunk Phantom.

Splunk SPLK-2003 Exam is a multiple-choice test that consists of 60 questions. Candidates have 90 minutes to complete the exam, and they must score at least 70% to pass. SPLK-2003 exam is available in English and Japanese, and it can be taken at any Pearson VUE testing center or online through the Pearson VUE OnVUE platform.

>> Valid Exam SPLK-2003 Braindumps <<

Top Valid Exam SPLK-2003 Braindumps | High-quality Valid SPLK-2003 Exam Review: Splunk Phantom Certified Admin

VCEdumps is also offering 90 days free SPLK-2003 updates. You can update your SPLK-2003 study material for one year from the date of purchase. The SPLK-2003 updated package will include all the past questions from the past papers. You can pass the SPLK-2003 exam easily with the help of the PDF dumps included in the package. It will have all the questions that you should cover for the SPLK-2003 SPLK-2003 exam. If you are facing any issues with the products you have, then you can always contact our 24/7 support to get assistance.

Splunk Phantom Certified Admin Sample Questions (Q30-Q35):

NEW QUESTION # 30

What is the default embedded search engine used by Phantom?

- A. Embedded Phantom search engine.
- B. Embedded Splunk search engine.
- C. Embedded Django search engine.
- D. Embedded Elastic search engine.

Answer: B

Explanation:

The default embedded search engine used by Splunk SOAR (formerly known as Phantom) is the embedded Splunk search engine.

Here's a detailed explanation:

Embedded Splunk Search Engine:

Splunk SOAR uses an embedded, preconfigured version of Splunk Enterprise as its native search engine.

This integration allows for powerful searching capabilities within Splunk SOAR, leveraging Splunk's robust search and indexing features.

Search Configuration:

While the embedded Splunk search engine is the default, organizations have the option to configure Splunk SOAR to use a different Splunk Enterprise deployment or an external Elasticsearch instance.

This flexibility allows organizations to tailor their search infrastructure to their specific needs and existing environments.

Search Capabilities:

The embedded Splunk search engine enables users to perform complex searches, analyze data, and generate reports directly within the Splunk SOAR platform.

It supports the full range of Splunk's search processing language (SPL) commands, functions, and visualizations.

References:

Splunk SOAR Documentation: Configure search in Splunk Phantom¹.

Splunk SOAR Documentation: Configure search in Splunk SOAR (On-premises)².

In summary, the embedded Splunk search engine is the default search engine in Splunk SOAR, providing a seamless and powerful search experience for users within the platform.

NEW QUESTION # 31

After enabling multi-tenancy, which of the Mowing is the first configuration step?

- A. Select the associated tenant artifacts.
- B. Configure the default tenant.
- **C. Change the tenant permissions.**
- D. Set default tenant base address.

Answer: C

NEW QUESTION # 32

What is the main purpose of using a customized workbook?

- **A. Workbooks may not be customized; only default workbooks are permitted within Phantom.**
- B. Workbooks automatically implement a customized processing of events using Python code.
- C. Workbooks apply service level agreements (SLAs) to containers and monitor completion status on the ROI dashboard.
- D. Workbooks guide user activity and coordination during event analysis and case operations.

Answer: A

NEW QUESTION # 33

When assigning an input parameter to an action while building a playbook, a user notices the artifact value they are looking for does not appear in the auto-populated list.

How is it possible to enter the unlisted artifact value?

- A. Edit the container to allow CEF parameters.
- B. Delete and recreate the artifact.
- **C. Type the CEF datapath in manually.**
- D. Edit the artifact to enable the List as Parameter option for the CEF value.

Answer: C

Explanation:

When building a playbook in Splunk SOAR, if the desired artifact value does not appear in the auto-populated list of input parameters for an action, users have the option to manually enter the Common Event Format (CEF) datapath for that value. This allows for greater flexibility and customization in playbook design, ensuring that specific data points can be targeted even if they're

not immediately visible in the interface. This manual entry of CEF datapaths allows users to directly reference the necessary data within artifacts, bypassing limitations of the auto-populated list.

NEW QUESTION # 34

Why does SOAR use wildcards within artifact data paths?

- A. To make data access in playbooks easier.
- B. To make playbooks more specific.
- C. To make decision execution in playbooks run faster.
- D. To make playbooks filter out nulls.

Answer: A

Explanation:

Wildcards are used within artifact data paths in Splunk SOAR playbooks to simplify the process of accessing data. They allow playbooks to reference dynamic or variable data structures without needing to specify exact paths, which can vary between artifacts. This flexibility makes it easier to write playbooks that work across different events and scenarios, without hard-coding data paths. SOAR uses wildcards within artifact data paths to make data access in playbooks easier. A data path is a way of specifying the location of a piece of data within an artifact. For example, `artifact.cef.sourceAddress` is a data path that refers to the source address field of the artifact. A wildcard is a special character that can match any value or subfield within a data path. For example, `artifact.*.cef.sourceAddress` is a data path that uses a wildcard to match any field name before the `cef` subfield. This allows the playbook to access the source address data regardless of the field name, which can vary depending on the app or source that generated the artifact. Therefore, option C is the correct answer, as it explains why SOAR uses wildcards within artifact data paths. Option A is incorrect, because wildcards do not make playbooks more specific, but more flexible and adaptable. Option B is incorrect, because wildcards do not make playbooks filter out nulls, but match any value or subfield. Option D is incorrect, because wildcards do not make decision execution in playbooks run faster, but make data access in playbooks easier.

1: Understanding datapaths in Administer Splunk SOAR (Cloud)

NEW QUESTION # 35

.....

To get success in exams and especially in a professional certification test like the Splunk Phantom Certified Admin SPLK-2003 test is very important to build a bright career. People from all over the world can get the best-paying jobs after passing the Splunk SPLK-2003 Exam. So VCEdumps will help you to study well for the Splunk Phantom Certified Admin SPLK-2003 certification exam. And price is benefit and reliable.

Valid SPLK-2003 Exam Review: <https://www.vcedumps.com/SPLK-2003-examcollection.html>

- How Can You Avoid Wasting Your Money by Purchasing the Splunk SPLK-2003 Exam Questions? ☐ Open ☐ www.pass4test.com ☐ enter ☐ SPLK-2003 ☐ and obtain a free download ☐ SPLK-2003 Advanced Testing Engine
- SPLK-2003 Latest Braindumps Pdf ☐ Valid Braindumps SPLK-2003 Sheet ☐ SPLK-2003 Exam Cost ☐ Search for ☐ SPLK-2003 ☐ and download it for free immediately on { www.pdfvce.com } ☐ SPLK-2003 Relevant Questions
- 100% Pass Useful Splunk - SPLK-2003 - Valid Exam Splunk Phantom Certified Admin Braindumps ☐ Copy URL ☐ www.troytecdumps.com ☐ open and search for ☐ SPLK-2003 ☐ to download for free ☐ Test SPLK-2003 Tutorials
- SPLK-2003 Exam Dumps ☐ Trusted SPLK-2003 Exam Resource ☐ SPLK-2003 Practice Engine ☐ Download ☐ SPLK-2003 ☐ for free by simply searching on ☐ www.pdfvce.com ☐ SPLK-2003 Relevant Questions
- Free PDF Valid Exam SPLK-2003 Braindumps - Accurate Valid SPLK-2003 Exam Review Ensure You a High Passing Rate ☐ Search for ☐ SPLK-2003 ☐ and easily obtain a free download on ☐ www.prepawaypdf.com ☐ SPLK-2003 Exam Tutorials
- SPLK-2003 Exam Cost ☐ SPLK-2003 Relevant Questions ☐ Top SPLK-2003 Exam Dumps ☐ Search for ☐ SPLK-2003 ☐ and obtain a free download on ☐ www.pdfvce.com ☐ Valid Braindumps SPLK-2003 Sheet
- Actual SPLK-2003 Test Training Questions are Very Helpful Exam Materials ☐ Simply search for ☐ SPLK-2003 ☐ for free download on (www.testkingpass.com) ☐ SPLK-2003 Latest Braindumps Pdf
- SPLK-2003 Exam Tutorials ☐ SPLK-2003 Latest Exam Cost ☐ Test SPLK-2003 Prep ☐ Search for "SPLK-2003" and download exam materials for free through ☐ www.pdfvce.com ☐ SPLK-2003 Latest Braindumps Pdf
- Useful Valid Exam SPLK-2003 Braindumps - Leading Offer in Qualification Exams - Unparalleled SPLK-2003: Splunk Phantom Certified Admin ☐ Search on (www.dumpsmaterials.com) for ☐ SPLK-2003 ☐ to obtain exam materials for free download ☐ SPLK-2003 Exam Dumps
- SPLK-2003 Latest Exam Simulator ☐ SPLK-2003 Exam Dumps ☐ SPLK-2003 Printable PDF ☐ Easily obtain free

- SPLK-2023 Exam Dumps ☐ SPLK-2023 Relevant Questions ☐ SPLK-2023 Dump ☐ The page for free download of SPLK-2023 ☐ on ☐ www.vceengine.com ☐ will open immediately ☐ ☐ Top SPLK-2023 Exam Dumps

- www.stes.tyc.edu.tw, belajarformula.com, www.stes.tyc.edu.tw, 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, onartbook.co, ncon.edu.sa, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

BTW, DOWNLOAD part of VCEDumps SPLK-2003 dumps from Cloud Storage: https://drive.google.com/open?id=1oJih4yU_nH2FcqcSBkci5vD4J-Veq6uw