Latest SPLK-2003 Braindumps - Exam SPLK-2003 Labs

P.S. Free 2025 Splunk SPLK-2003 dumps are available on Google Drive shared by TestKingIT: https://drive.google.com/open?id=1lxLU057WUtgKbxZORdncCB9X-2VIgWWe

A Splunk Phantom Certified Admin (SPLK-2003) practice questions is a helpful, proven strategy to crack the Splunk Phantom Certified Admin (SPLK-2003) exam successfully. It helps candidates to know their weaknesses and overall performance. TestKingIT software has hundreds of Splunk Phantom Certified Admin (SPLK-2003) exam dumps that are useful to practice in real-time. The Splunk Phantom Certified Admin (SPLK-2003) practice questions have a close resemblance with the actual SPLK-2003 exam.

Splunk SPLK-2003 exam is designed for IT professionals who are seeking to become certified administrators of the Splunk Phantom platform. Splunk Phantom is a security orchestration, automation, and response (SOAR) solution that helps organizations streamline their security operations and improve their incident response capabilities. SPLK-2003 exam covers a range of topics, including installation and configuration, user management, workflow design, automation, and integration with other security tools. Passing the SPLK-2003 exam demonstrates a candidate's knowledge and skills in using Splunk Phantom to automate and orchestrate security tasks, enabling organizations to respond more quickly and effectively to security incidents.

Splunk SPLK-2003 Exam is a valuable certification for individuals who want to demonstrate their expertise in Splunk Phantom administration. Splunk Phantom Certified Admin certification can help individuals advance their careers in the field of cybersecurity and is recognized by organizations around the world. Candidates who pass the exam will have demonstrated their knowledge and skills in managing and configuring the Splunk Phantom platform, making them valuable assets to any organization.

>> Latest SPLK-2003 Braindumps <<

Is Splunk SPLK-2003 Questions – Best Way To Clear The Exam?

Our SPLK-2003 exam simulation is a great tool to improve our competitiveness. After we use our study materials, we can get the Splunk certification faster. This certification gives us more opportunities. Compared with your colleagues around you, with the help of our SPLK-2003 preparation questions, you will also be able to have more efficient work performance. Our SPLK-2003 Study Materials can bring you so many benefits because they have the following features. I hope you can use a cup of coffee to learn about our SPLK-2003 training engine. Perhaps this is the beginning of your change.

Splunk Phantom Certified Admin Sample Questions (Q16-Q21):

NEW QUESTION # 16
Which of the following describes the use of labels in Phantom?

- A. Labels determine which playbook(s) are executed when a container is created.
- B. Labels control which apps are allowed to execute actions on the container.
- C. Labels determine the service level agreement (SLA) for a container.
- D. Labels control the default seventy, ownership, and sensitivity for the container.

Answer: A

Explanation:
In Splunk Phantom, labels are used to categorize containers and trigger specific automated responses. When a container is created, labels can be assigned to it based on the nature of the event, type of incident, or other criteria. These labels are then matched against playbooks, which have label conditions defined within them.
When the conditions are met, the corresponding playbooks are automatically executed. Labels do not directly control service level agreements, default severity, ownership, sensitivity, or app execution permissions.

NEW QUESTION # 17
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?_filter_status "failed"
- D. https://<PHANTOM_URL>/rest/playbook_run?_query_status="failed"

Answer: D

NEW QUESTION # 18
When configuring a Splunk asset for Phantom to connect to a SplunkC loud instance, the user discovers that they need to be able to run two different on_poll searches. How is this possible

- A. Configure the second query in the Phantom app for Splunk.
- B. Configure a second Splunk asset with the second query.
- C. Install a second Splunk app and configure the query in the second app.
- D. Enter the two queries in the asset as comma separated values.

Answer: B

Explanation:
Explanation
The correct answer is D because to run two different on_poll searches, you need to configure a second Splunk asset with the second query. The on_poll search is the query that Phantom uses to fetch events from Splunk and create containers and artifacts. You can only specify one on_poll search per Splunk asset. If you want to run another on_poll search, you need to create another Splunk asset with a different name and IP address and configure the second query in the asset settings. See Splunk SOAR Documentation for more details.

NEW QUESTION # 19
Which of the following are the default ports that must be configured on Splunk to allow connections from SOAR?

- A. SplunkWeb (8088), SplunkD (8089), HTTP Collector (8000)
- B. SplunkWeb (8089), SplunkD (8088), HTTP Collector (8000)
- C. SplunkWeb (8421), SplunkD (8061), HTTP Collector (8798)
- D. SplunkWeb (8000), SplunkD (8089), HTTP Collector (8088)

Answer: D

Explanation:
The default ports that must be configured on Splunk to allow connections from Phantom are SplunkWeb (8000), SplunkD (8089), and HTTP Collector (8088). SplunkWeb is the port used to access the Splunk web interface. SplunkD is the port used to communicate with the Splunk server. HTTP Collector is the port used to send data to Splunk using the HTTP Event Collector (HEC). These ports must be configured on Splunk and Phantom to enable the integration between the two products.
To allow connections from Splunk Phantom to Splunk, certain default ports need to be open and properly configured. The default ports include SplunkWeb (8000) for web access, SplunkD (8089) for Splunk's management port, and the HTTP Event Collector (HEC) on port 8088, which is used for ingesting data into Splunk. These ports are essential for the communication between Splunk Phantom and Splunk, facilitating data exchange, search capabilities, and the integration of various functionalities between the two platforms.

NEW QUESTION # 20
Which of the following can be done with the System Health Display?

- A. View a single column of status for SOAR processes. For metrics, click Details.
- B. Partially rewind processes, which is useful for debugging.
- C. Create a temporary, edited version of a process and test the results.
- D. Reset DECIDED to reset playbook environments back to at-start conditions.

Answer: A

Explanation:
System Health Display is a dashboard that shows the status and performance of the SOAR processes and components, such as the automation service, the playbook daemon, the DECIDED process, and the REST API. One of the things that can be done with the System Health Display is to reset DECIDED, which is a core component of the SOAR automation engine that handles the execution of playbooks and actions. Resetting DECIDED can be useful for troubleshooting or debugging purposes, as it resets the playbook environments back to at-start conditions, meaning that any changes made by the playbooks are discarded and the playbooks are reloaded. To reset DECIDED, you need to click on the Reset DECIDED button on the System Health Display dashboard.

NEW QUESTION # 21
.....

The TestKingIT SPLK-2003 exam questions are being offered in three different formats. These formats are SPLK-2003 PDF dumps files, desktop practice test software, and web-based practice test software. All these three SPLK-2003 exam dumps formats contain the Real SPLK-2003 Exam Questions that assist you in your Splunk Phantom Certified Admin practice exam preparation and finally, you will be confident to pass the final Splunk Phantom Certified Admin (SPLK-2003) exam easily.

Exam SPLK-2003 Labs: https://www.testkingit.com/Splunk/latest-SPLK-2003-exam-dumps.html

- Latest SPLK-2003 Braindumps - Free PDF Quiz Splunk Splunk Phantom Certified Admin Realistic Exam Labs □ Enter □ www.examcollectionpass.com □ and search for □ SPLK-2003 □ to download for free □Certification SPLK-2003 Exam Dumps
- Splunk SPLK-2003 PDF Dumps - Pass Your Exam In First Attempt [Updated-2025] □ Open { www.pdfvce.com } enter ➽ SPLK-2003 □ and obtain a free download □SPLK-2003 Valid Test Duration
- SPLK-2003 Authorized Test Dumps □ SPLK-2003 Pdf Braindumps □ Test SPLK-2003 Pdf □ The page for free download of ⇛ SPLK-2003 ⇚ on ➤ www.itcerttest.com □ will open immediately □SPLK-2003 Real Dumps Free
- Useful Splunk - SPLK-2003 - Latest Splunk Phantom Certified Admin Braindumps □ Download ☀ SPLK-2003 □☀□ for free by simply searching on ➠ www.pdfvce.com □ □Test SPLK-2003 Pdf
- Authoritative Latest SPLK-2003 Braindumps bring you Practical Exam SPLK-2003 Labs for Splunk Splunk Phantom Certified Admin □ Search for □ SPLK-2003 □ and download exam materials for free through （ www.passcollection.com ） □New SPLK-2003 Test Book
- Latest SPLK-2003 Braindumps - Free PDF Quiz Splunk Splunk Phantom Certified Admin Realistic Exam Labs □ ▸ www.pdfvce.com ◂ is best website to obtain ☀ SPLK-2003 □☀□ for free download □SPLK-2003 Useful Dumps
- Free PDF 2025 Useful SPLK-2003: Latest Splunk Phantom Certified Admin Braindumps □ Search for □ SPLK-2003 □ and download exam materials for free through 【 www.passtestking.com 】 □Valid SPLK-2003 Test Duration
- Valid SPLK-2003 Test Duration □ Certification SPLK-2003 Exam Dumps □ SPLK-2003 Reliable Exam Syllabus ♣ Open [www.pdfvce.com] and search for ⇛ SPLK-2003 ⇚ to download exam materials for free □New SPLK-2003 Test Book
- SPLK-2003 Valid Test Duration □ SPLK-2003 Valid Dumps Ppt □ New SPLK-2003 Test Cost ↗ Easily obtain free download of ➽ SPLK-2003 □ by searching on （ www.vceengine.com ） □Valid SPLK-2003 Test Materials
- Accurate SPLK-2003 Practice Engine gives you high-effective Exam Quiz - Pdfvce □ Easily obtain ▸ SPLK-2003 ◂ for free download through ➽ www.pdfvce.com □ □New SPLK-2003 Test Book
- Splunk SPLK-2003 Exam | Latest SPLK-2003 Braindumps - Try Exam SPLK-2003 Labs Free and Buy Easily □ Immediately open 「 www.examsreviews.com 」 and search for { SPLK-2003 } to obtain a free download □SPLK-2003 Reliable Exam Syllabus
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, techsafetycourses.com, www.stes.tyc.edu.tw, ncon.edu.sa, pct.edu.pk, www.stes.tyc.edu.tw, tutr.online, brainchips.liuyanze.com, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New SPLK-2003 dumps are available on Google Drive shared by TestKingIT: https://drive.google.com/open?id=1lxLU057WUtgKbxZORdncCB9X-2VIgWWe