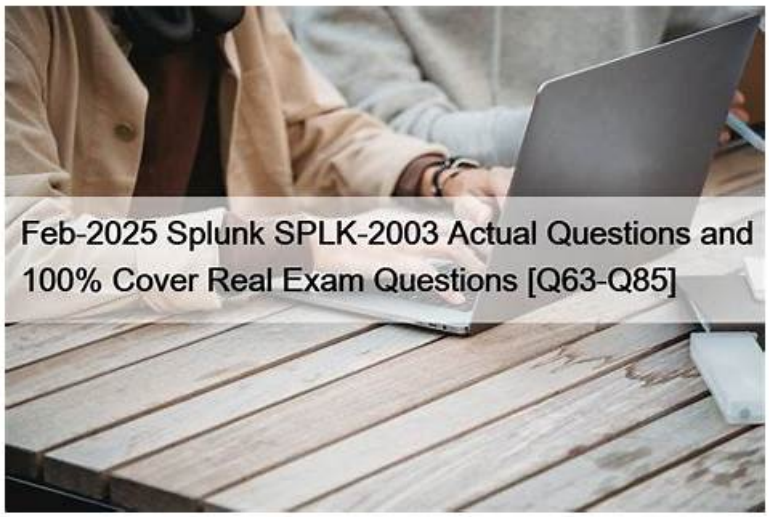
Quiz SPLK-2003 - Splunk Phantom Certified Admin– Valid Exam Dumps Pdf



2026 Latest Exams4sures SPLK-2003 PDF Dumps and SPLK-2003 Exam Engine Free Share: https://drive.google.com/open?id=1V20PAOxhe67p8Yn7wzk27j6MpP--nV6g

Well preparation is half done, so choosing good SPLK-2003 training materials is the key of clear exam in your first try with less time and efforts. Our website offers you the latest preparation materials for the SPLK-2003 real exam and the study guide for your review. There are three versions according to your study habit and you can practice our SPLK-2003 Dumps PDF with our test engine that help you get used to the atmosphere of the formal test.

Splunk SPLK-2003 exam is a certification exam designed for individuals who want to become certified Splunk Phantom administrators. Splunk Phantom is a security orchestration, automation, and response (SOAR) platform that allows organizations to automate and streamline their security operations. The SPLK-2003 Exam Tests knowledge and skills related to the administration and configuration of the Splunk Phantom platform.

>> Exam Dumps SPLK-2003 Pdf <<

Intereactive SPLK-2003 Testing Engine | New SPLK-2003 Dumps Book

SPLK-2003 exam certification is one of the most important certification recently. When qualified by the SPLK-2003 certification, you will get a good job easily with high salary. Besides, the career opportunities will be open for a certified person. Now, you can get the valid and best useful SPLK-2003 Exam Training material. Our SPLK-2003 study torrent is with 100% correct questions & answers, which can ensure you pass at first attempt. All SPLK-2003 practice torrents can be easily and instantly downloaded after purchase.

The SPLK-2003 certification exam is a proctored exam that consists of 60 multiple-choice questions. Candidates have two hours to complete the exam and must achieve a score of 70% or higher to pass. SPLK-2003 exam is available in English and Japanese and can be taken at any Pearson VUE testing center worldwide.

Splunk SPLK-2003 certification exam is a comprehensive exam designed to test the knowledge and skills of individuals who are interested in becoming Splunk Phantom Certified Administrators. SPLK-2003 Exam covers topics such as installation and configuration of Splunk Phantom, administration of Splunk Phantom, automation and orchestration, and integration with other tools and systems. Passing the certification exam demonstrates expertise in the administration and management of the Splunk Phantom platform.

Splunk Phantom Certified Admin Sample Questions (Q93-Q98):

NEW QUESTION # 93
Configuring Phantom search to use an external Splunk server provides which of the following benefits?

- A. The ability to ingest Splunk notable events into Phantom.
- B. The ability to display results as Splunk dashboards within Phantom.
- C. The ability to run more complex reports on Phantom activities.
- D. The ability to automate Splunk searches within Phantom.

Answer: D

Explanation:
Configuring Phantom (now known as Splunk SOAR) to use an external Splunk server enhances the automation capabilities within Phantom by allowing the execution of Splunk searches as part of the automation and orchestration processes. This integration facilitates the automation of tasks that involve querying data from Splunk, thereby streamlining security operations and incident response workflows. Splunk SOAR's ability to integrate with over 300 third-party tools, including Splunk, supports a wide range of automatable actions, thus enabling a more efficient and effective security operations center (SOC) by reducing the time to respond to threats and by making repetitive tasks more manageable.
https://www.splunk.com/en_us/products/splunk-security-orchestration-and-automation- features.html

NEW QUESTION # 94
What are the differences between cases and events?

- A. Cases: incidents with a known violation and a plan for correction.
  Events: occurrences in the system that may require a response.
- B. Cases: contain a collection of containers.
  Events: contain potential threats.
- 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: B

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 threats13. 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 products22. They are used to manage and analyze investigation data tied to specific security events and incidents, providing a structured approach to incident response34.
References:
* Manage the status, severity, and resolution of events in Splunk SOAR (Cloud) - Splunk Documentation
* Managing cases in SOAR - Splunk Lantern
* What is Splunk Phantom (Renamed to Splunk SOAR)? - BlueVoyant
* Overview of cases - Splunk Documentation

NEW QUESTION # 95
Which app allows a user to send Splunk Enterprise Security notable events to Phantom?

- A. Splunk App for Phantom Reporting.
- B. Splunk App for Phantom.
- C. Any of the integrated Splunk/Phantom Apps
- D. Phantom App for Splunk.

Answer: D

Explanation:
Explanation
The correct answer is D because the Phantom App for Splunk is the app that allows a user to send Splunk Enterprise Security notable events to Phantom. The Phantom App for Splunk is a Splunk app that can be installed on the Splunk server and configured to connect to the Phantom server. The app provides a custom command called sendtophantom that can be used to send any Splunk events to Phantom as containers and artifacts. The app also provides a dashboard that shows the status of the events sent to

Phantom. See Splunk SOAR Documentation for more details.

NEW QUESTION # 96
A user wants to use their Splunk Cloud instance as the external Splunk instance for Phantom.
What ports need to be opened on the Splunk Cloud instance to facilitate this? Assume default ports are in use.

- A. TCP 8080 and TCP 8191.
- B. Splunk Cloud is not supported.
- C. TCP 80 and TCP 443.
- D. TCP 8088 and TCP 8099.

Answer: C

Explanation:
To integrate Splunk Phantom with a Splunk Cloud instance, network communication over certain ports is necessary. The default ports for web traffic are TCP 80 for HTTP and TCP 443 for HTTPS. Since Splunk Cloud instances are accessed over the internet, ensuring that these ports are open is essential for Phantom to communicate with Splunk Cloud for various operations, such as running searches, sending data, and receiving results. It is important to note that TCP 8088 is typically used by Splunk's HTTP Event Collector (HEC), which may also be relevant depending on the integration specifics.

NEW QUESTION # 97
On a multi-tenant Phantom server, what is the default tenant's ID?

- A. 0
- B. Default
- C. *
- D. 1

Answer: D

Explanation:
The default tenant's ID is 1. The tenant ID is a unique identifier for each tenant on a multi-tenant Phantom server. The default tenant is the tenant that is created when Phantom is installed and contains all the existing data and assets. The default tenant's ID is always 1 and cannot be changed. Other tenants have IDs that are assigned sequentially starting from 2.
In a multi-tenant Splunk SOAR environment, the default tenant is typically assigned an ID of 1.
This ID is system-generated and is used to uniquely identify the default tenant within the SOAR database and system configurations.
The default tenant serves as the primary operational environment before any additional tenants are configured, and its ID is crucial for database operations, API calls, and internal reference within the SOAR platform. Understanding and correctly using tenant IDs is essential for managing resources, permissions, and data access in a multi-tenant SOAR setup.

NEW QUESTION # 98
.....

- SPLK-2003 Reliable Test Practice □ Test SPLK-2003 Result □ New SPLK-2003 Practice Materials □ Easily obtain free download of ➥ SPLK-2003 □ by searching on ➥ www.pdfvce.com □ □Exam SPLK-2003 Course
- 2026 Exam Dumps SPLK-2003 Pdf | Updated 100% Free Intereactive Splunk Phantom Certified Admin Testing Engine □ □ Search for （ SPLK-2003 ） and download exam materials for free through ▹ www.pdfdumps.com ◃ □SPLK-2003 Latest Exam Dumps
- SPLK-2003 Useful Dumps □ New SPLK-2003 Practice Materials □ Online SPLK-2003 Test □ ➡ www.pdfvce.com □□□ is best website to obtain ➡ SPLK-2003 □□□ for free download □SPLK-2003 Useful Dumps
- SPLK-2003 Training Materials are Your Excellent Chance to Master More Useful Knowledge - www.vce4dumps.com □ Search on 「 www.vce4dumps.com 」 for ➽ SPLK-2003 □ to obtain exam materials for free download □SPLK-2003 Reliable Test Practice
- Reliable SPLK-2003 Study Notes □ Test SPLK-2003 Result □ SPLK-2003 New Real Exam □ Download ✔ SPLK-2003 □✔□ for free by simply entering ⇛ www.pdfvce.com ⇚ website □Valid Exam SPLK-2003 Practice
- SPLK-2003 Mock Test □ SPLK-2003 New Real Exam □ SPLK-2003 Unlimited Exam Practice □ { www.examdiscuss.com } is best website to obtain □ SPLK-2003 □ for free download □SPLK-2003 Useful Dumps
- www.stes.tyc.edu.tw, myportal.utt.edu.tt, bbs.t-firefly.com, www.stes.tyc.edu.tw, ishiwishi.shop, tutor.mawgood-eg.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

2026 Latest Exams4sures SPLK-2003 PDF Dumps and SPLK-2003 Exam Engine Free Share: https://drive.google.com/open?id=1V20PAOxhe67p8Yn7wzk27j6MpP--nV6g