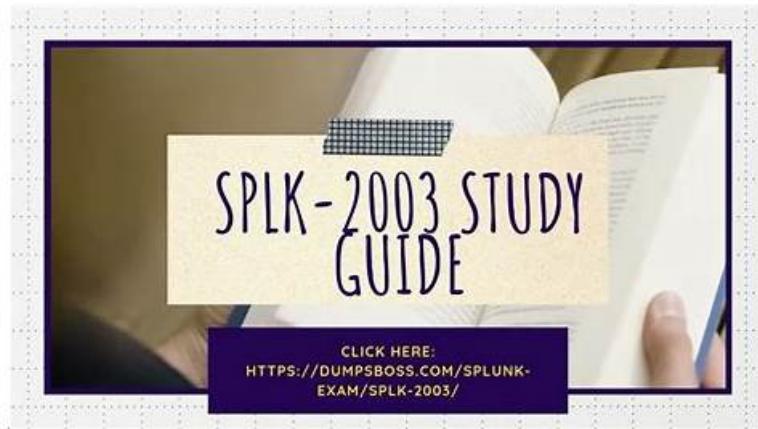


SPLK-2003 Reliable Study Guide & Exam SPLK-2003 Simulator Fee



P.S. Free & New SPLK-2003 dumps are available on Google Drive shared by VCE4Dumps: https://drive.google.com/open?id=1qEEoc_UYhSSdXKJPu82IO29wqI_eGiZ

It would be really helpful to purchase Splunk Phantom Certified Admin exam dumps right away. If you buy this Splunk Certification Exams product right now, we'll provide you with up to 1 year of free updates for SPLK-2003 authentic questions. You can prepare using these no-cost updates in accordance with the most recent test content changes provided by the SPLK-2003 Exam Dumps. The SPLK-2003 actual questions we sell also come with a free demo.

Splunk SPLK-2003: Splunk Phantom Certified Admin exam is a certification program designed for IT professionals who have knowledge and experience in the field of security automation and orchestration. SPLK-2003 Exam is intended to validate the knowledge and skills of candidates in the areas of Phantom platform administration, automation design, and incident response management.

Achieving the Splunk Phantom Certified Admin certification demonstrates an individual's expertise in administering the Splunk Phantom platform. Splunk Phantom Certified Admin certification is ideal for security professionals, system administrators, and IT professionals who are responsible for managing security operations. Splunk Phantom Certified Admin certification validates an individual's ability to configure and manage the Splunk Phantom platform, enabling them to effectively automate and orchestrate security operations, detect and respond to security incidents, and improve overall security posture.

>> SPLK-2003 Reliable Study Guide <<

Exam SPLK-2003 Simulator Fee, SPLK-2003 Exam Blueprint

Since our childhood, we have always been guided to study hard to clear the Splunk SPLK-2003 exams but if you still believe in the same pattern for clearing your Splunk Phantom Certified Admin SPLK-2003 certification exam, I must say it's a bad idea. Studying hard is good only when you have enough time and no liability to check. When you are in your professional career, you don't have enough time to study hard but you have time to study smart. The smart study includes to prepare VCE4Dumps SPLK-2003 Exam Questions that will help you concentrate on the core study and not follow up on the stories and background.

Splunk Phantom Certified Admin Sample Questions (Q20-Q25):

NEW QUESTION # 20

Which of the following cannot be marked as evidence in a container?

- A. Comment
- B. Artifact
- C. Note
- D. Action result

Answer: A

Explanation:

In Splunk SOAR, the following elements can be marked as evidence within a container: action results, artifacts, and notes. These are crucial elements that contribute directly to incident analysis and can be selected as evidence to support investigation outcomes or legal proceedings.

However, comments cannot be marked as evidence. Comments are usually informal and meant for communication between users, providing context or updates but not serving as formal evidence within the system. Action results, artifacts, and notes, on the other hand, contain critical data related to the incident that could be useful for audit and investigative purposes, making them eligible to be marked as evidence.

References:

- * Splunk SOAR Documentation: Working with Evidence.
- * Splunk SOAR Best Practices: Evidence Collection and Management.

NEW QUESTION # 21

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

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

Answer: B

NEW QUESTION # 22

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 Files tab for further investigation.
- C. Files tab items and artifacts are the only data sources that can populate active cases.
- D. Phantom memory requirements remain static, regardless of Files tab usage.

Answer: B

Explanation:

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. Reference, page 23.

NEW QUESTION # 23

The SOAR server has been configured to use an external Splunk search head for search and searching on SOAR works; however, the search results don't include content that was being returned by search before configuring external search. Which of the following could be the problem?

- A. Content that existed before configuring external search must be backed up on SOAR and restored on the Splunk search head.
- B. The user configured on the SOAR side with Phantomsearch capability is not enabled on Splunk.
- C. The remote Splunk search head is currently offline.
- D. The existing content indexes on the SOAR server need to be re-indexed to migrate them to Splunk.

Answer: B

Explanation:

If, after configuring an external Splunk search head for search in SOAR, the search results do not include content that was previously returned, one possible issue could be that the user account configured on the SOAR side does not have the required permissions (such as the 'phantomsearch' capability) enabled on the Splunk side. This capability is necessary for the SOAR server to execute

searches and retrieve results from the Splunk search head.

NEW QUESTION # 24

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

- A. SplunkWeb (8469), SplunkD (8702), HTTP Collector (8864)
- B. **SplunkWeb (8000), SplunkD (8089), HTTP Collector (8088)**
- C. SplunkWeb (8088), SplunkD (8089), HTTP Collector (8000)
- D. SplunkWeb (8089), SplunkD (8088), HTTP Collector (8000)

Answer: B

Explanation:

For Splunk SOAR to connect with Splunk Enterprise, certain default ports must be configured to facilitate communication between the two platforms. Typically, SplunkWeb, which serves the Splunk Enterprise web interface, uses port 8000. SplunkD, the Splunk daemon that handles most of the back-end services, listens on port 8089. The HTTP Event Collector (HEC), which allows HTTP clients to send data to Splunk, typically uses port 8088. These ports are essential for the integration, allowing SOAR to send data to Splunk for indexing, searching, and visualization.

NEW QUESTION # 25

.....

So rest assured that you will get top-notch and easy-to-use Splunk SPLK-2003 practice questions. The Splunk Phantom Certified Admin (SPLK-2003) PDF dumps file is the PDF version of real Splunk Phantom Certified Admin (SPLK-2003) exam questions that work with all devices and operating systems. Just download the Splunk Phantom Certified Admin (SPLK-2003) PDF dumps file and start the Splunk Phantom Certified Admin (SPLK-2003) exam questions preparation right now. Whereas the other two Splunk Phantom Certified Admin (SPLK-2003) practice test software is concerned, both are the mock Splunk SPLK-2003 exam dumps and help you to provide the real-time Splunk Phantom Certified Admin (SPLK-2003) exam environment for preparation.

Exam SPLK-2003 Simulator Fee: <https://www.vce4dumps.com/SPLK-2003-valid-torrent.html>

- Study SPLK-2003 Tool SPLK-2003 Valid Study Notes Reliable SPLK-2003 Study Plan Easily obtain ⇒ SPLK-2003 for free download through { www.vce4dumps.com } SPLK-2003 Dumps Collection
- SPLK-2003 Books PDF New SPLK-2003 Dumps Sheet SPLK-2003 Training Kit Search for (SPLK-2003) on www.pdfvce.com immediately to obtain a free download SPLK-2003 Books PDF
- Pass SPLK-2003 Exam with Unparalleled SPLK-2003 Reliable Study Guide by www.easy4engine.com Search for ✓ SPLK-2003 ✓ on www.easy4engine.com immediately to obtain a free download Reliable SPLK-2003 Study Plan
- Certification SPLK-2003 Questions New SPLK-2003 Dumps Sheet SPLK-2003 Dumps Collection Search for ▶ SPLK-2003 on www.pdfvce.com immediately to obtain a free download Reliable SPLK-2003 Study Plan
- Features Of SPLK-2003 Practice Questions Formats Copy URL www.testkingpass.com open and search for [SPLK-2003] to download for free SPLK-2003 Books PDF
- Free PDF Splunk SPLK-2003 Splunk Phantom Certified Admin First-grade Reliable Study Guide Enter (www.pdfvce.com) and search for SPLK-2003 to download for free SPLK-2003 Reliable Study Notes
- Certification SPLK-2003 Sample Questions Free SPLK-2003 Braindumps SPLK-2003 Dumps Collection Easily obtain free download of [SPLK-2003] by searching on www.troytecdumps.com SPLK-2003 Latest Study Guide
- Free PDF Quiz Splunk - SPLK-2003 - Splunk Phantom Certified Admin - Trustable Reliable Study Guide Open www.pdfvce.com and search for [SPLK-2003] to download exam materials for free Certification SPLK-2003 Cost
- Free PDF Quiz Splunk - SPLK-2003 - Splunk Phantom Certified Admin - Trustable Reliable Study Guide Search on www.examcollectionpass.com for [SPLK-2003] to obtain exam materials for free download SPLK-2003 Latest Study Guide
- New SPLK-2003 Dumps Sheet Certification SPLK-2003 Sample Questions New SPLK-2003 Dumps Sheet Search for SPLK-2003 and download it for free immediately on “ www.pdfvce.com ” SPLK-2003 Valid Study Notes
- SPLK-2003 Dumps Collection Exam SPLK-2003 Consultant SPLK-2003 Valid Study Notes Search for (SPLK-2003) and download it for free on { www.exam4labs.com } website New SPLK-2003 Dumps Files

- wanderlog.com, www.stes.tyc.edu.tw, bbs.t-firefly.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

BTW, DOWNLOAD part of VCE4Dumps SPLK-2003 dumps from Cloud Storage: https://drive.google.com/open?id=1qEEoc_UYhSSdXKJPu82IO29wqI_eGiZ