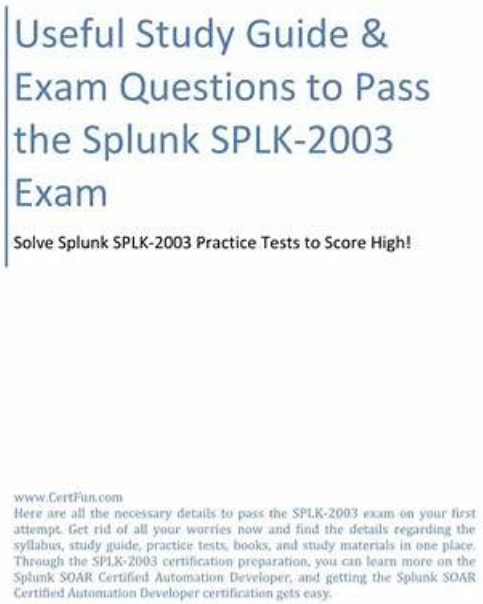
Splunk SPLK-2003 Exam Questions Vce - Valid SPLK-2003 Exam Materials



2026 Latest ActualVCE SPLK-2003 PDF Dumps and SPLK-2003 Exam Engine Free Share: https://drive.google.com/open?id=1rIpMcB7qjjElZRFCr4wVNHC2eeuc77Zw

Are you still worrying about how to safely pass Splunk certification SPLK-2003 exams? Do you have thought to select a specific training? Choosing a good training can effectively help you quickly consolidate a lot of IT knowledge, so you can be well ready for Splunk certification SPLK-2003 exam. ActualVCE's expert team used their experience and knowledge unremitting efforts to do research of the previous years exam, and finally have developed the best pertinence training program about Splunk Certification SPLK-2003 Exam. Our training program can effectively help you have a good preparation for Splunk certification SPLK-2003 exam. ActualVCE's training program will be your best choice.

Splunk Phantom platform is a powerful tool for automating IT processes and securing your organization's digital assets. By becoming a certified Splunk Phantom admin, you will gain the skills and knowledge necessary to leverage the full potential of this platform. Splunk Phantom Certified Admin certification is recognized globally and demonstrates to employers that you have the expertise to manage and automate complex IT processes using the Splunk Phantom platform.

>> Splunk SPLK-2003 Exam Questions Vce <<

Valid Splunk SPLK-2003 Exam Materials | Certification SPLK-2003 Exam Infor

With the rapid market development, there are more and more companies and websites to sell SPLK-2003 guide torrent for learners to help them prepare for exam. If you have known before, it is not hard to find that the study materials of our company are very

popular with candidates, no matter students or businessman. Welcome your purchase for our SPLK-2003 Exam Torrent. As is an old saying goes: Client is god! Service is first! SPLK-2003 Guide Braindumps can simulate limited-timed examination and online error correcting, and have 24/7 Service Online, SPLK-2003 Exam Torrent is the best and wisest choice for you to prepare your test.

Splunk is a leading platform for operational intelligence and security information and event management. It offers a comprehensive range of analytics tools that help organizations make more informed decisions based on the data generated by their IT systems. Splunk Phantom is an extension of the Splunk platform that focuses on automating security and IT incident response workflows. It enables organizations to streamline their incident response processes by automating repetitive tasks and orchestrating responses across different systems and teams.

Splunk Phantom Certified Admin Sample Questions (Q81-Q86):

NEW QUESTION # 81
A customer wants to design a modular and reusable set of playbooks that all communicate with each other.
Which of the following is a best practice for data sharing across playbooks?

- A. Cal the child playbooks getter function.
- B. Use the py-postgresq1 module to directly save the data in the Postgres database.
- C. Create artifacts using one playbook and collect those artifacts in another playbook.
- D. Use the Handle method to pass data directly between playbooks.

Answer: C

Explanation:
The correct answer is C because creating artifacts using one playbook and collecting those artifacts in another playbook is a best practice for data sharing across playbooks. Artifacts are data objects that are associated with a container and can be used to store information such as IP addresses, URLs, file hashes, etc. Artifacts can be created using the add artifact action in any playbook block and can be collected using the get artifacts action in the filter block. Artifacts can also be used to trigger active playbooks based on their label or type. See Splunk SOAR Documentation for more details.
In the context of Splunk SOAR, one of the best practices for data sharing across playbooks is to create artifacts in one playbook and use another playbook to collect and utilize those artifacts. Artifacts in Splunk SOAR are structured data related to security incidents (containers) that playbooks can act upon. By creating artifacts in one playbook, you can effectively pass data and context to subsequent playbooks, allowing for modular, reusable, and interconnected playbook designs. This approach promotes efficiency, reduces redundancy, and enhances the playbook's ability to handle complex workflows.

NEW QUESTION # 82
Which of the following are the steps required to complete a full backup of a Splunk Phantom deployment' Assume the commands are executed from /opt/phantom/bin and that no other backups have been made.

- A. On the command line enter: rode sudo python ibackup.pyc --setup, then audo phenv python ibackup. pyc --backup.
- B. Within the UI: Select from the main menu Administration > Product Settings > Backup.
- C. On the command line enter: sudo phenv python ibackup.pyc --backup -backup-type full, then sudo phenv python ibackup.pyc --setup.
- D. Within the UI: Select from the main menu Administration > System Health > Backup.

Answer: C

Explanation:
The correct answer is B because the steps required to complete a full backup of a Splunk Phantom deployment are to first run the --backup --backup-type full command and then run the --setup command.
The --backup command creates a backup file in the /opt/phantom/backup directory. The --backup-type full option specifies that the backup file includes all the data and configuration files of the Phantom server.
The --setup command creates a configuration file that contains the encryption key and other information needed to restore the backup file. See Splunk SOAR Certified Automation Developer Track for more details.
Performing a full backup of a Splunk Phantom deployment involves using the command-line interface, primarily because Phantom's architecture and data management processes are designed to be managed at the server level for comprehensive backup and recovery. The correct sequence involves initiating a full backup first using the --backup --backup-type full option to ensure all configurations, data, and necessary components are included in the backup. Following the completion of the backup, the --setup

option might be used to configure or verify the backup settings, although typically, the setup would precede backup operations in practical scenarios. This process ensures that all aspects of the Phantom deployment are preserved, including configurations, playbooks, cases, and other data, which is crucial for disaster recovery and system migration.

NEW QUESTION # 83
In the SOAR main menu, there are sub-options below Sources. What is the purpose of these options?

- A. They filter the container list based on default or user-saved filters.
- B. They are only available for admins and would never be used by an analyst.
- C. They permit analysts to select the app that is polled to create the containers.
- D. They permit analysts to select cases related to an investigation.

Answer: A

NEW QUESTION # 84
What is the default embedded search engine used by Phantom?

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

Answer: A

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 # 85
If the SOAR New status is removed and replaced by In Progress, what status is shown for containers that had the new status before the replacement?

- A. In Progress
- B. New
- C. New
- D. In Progress

Answer: A

NEW QUESTION # 86

......

Valid SPLK-2003 Exam Materials: https://www.actualvce.com/Splunk/SPLK-2003-valid-vce-dumps.html

P.S. Free 2026 Splunk SPLK-2003 dumps are available on Google Drive shared by ActualVCE: https://drive.google.com/open?id=1rIpMcB7qjjElZRFCr4wVNHC2eeuc77Zw