Sample SPLK-2003 Test Online Free PDF | Pass-Sure Valid SPLK-2003 Test Pass4sure: Splunk Phantom Certified Admin

DOWNLOAD the newest TestKingIT SPLK-2003 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1Q2mQySZQfL0r7ZzVepGRD1abdidC33mT

Continuous improvement is a good thing. If you keep making progress and transcending yourself, you will harvest happiness and growth. The goal of our SPLK-2003 latest exam guide is prompting you to challenge your limitations. People always complain that they do nothing perfectly. The fact is that they never insist on one thing and give up quickly. Our SPLK-2003 Study Dumps will assist you to overcome your shortcomings and become a persistent person. Once you have made up your minds to change, come to purchase our SPLK-2003 training practice.

Splunk SPLK-2003 Exam is intended for Splunk Phantom administrators who are responsible for managing and maintaining their organization's Splunk Phantom deployment. Candidates for SPLK-2003 exam should have a solid understanding of Splunk Phantom's capabilities and be able to perform basic administration tasks such as configuring users and permissions, managing workflows, and troubleshooting common issues.

>> Sample SPLK-2003 Test Online <<

Valid SPLK-2003 Test Pass4sure, SPLK-2003 Accurate Study Material

We are dedicated to helping you pass your exam just one time. SPLK-2003 learning materials are high quality, and we have received plenty of good feedbacks from our customers, they thank us for helping the exam just one time. If you can't pass your exam in your first attempt by using SPLK-2003 exam materials of us, we ensure you that we will give you full refund, and no other questions will be asked. In addition, we provide you with free demo for one year for SPLK-2003 Exam Braindumps, and the update version for SPLK-2003 exam materials will be sent to your email address automatically.

Splunk Phantom Certified Admin Sample Questions (Q106-Q111):

NEW QUESTION # 106
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 existing content indexes on the SOAR server need to be re-indexed to migrate them to Splunk.
- C. The remote Splunk search head is currently offline.
- D. The user configured on the SOAR side with Phantomsearch capability is not enabled on Splunk.

Answer: D

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 # 107
After enabling multi-tenancy, which of the Mowing is the first configuration step?

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

Answer: C

Explanation:
Upon enabling multi-tenancy in Splunk SOAR, the first step in configuration typically involves setting up the default tenant. This foundational step is critical as it establishes the primary operating environment under which subsequent tenants can be created and managed. The default tenant serves as the template for permissions, settings, and configurations that might be inherited or customized by additional tenants. Proper configuration of the default tenant ensures a stable and consistent framework for multi-tenancy operations, allowing for segregated environments within the same SOAR instance, each tailored to specific operational needs or organizational units.

NEW QUESTION # 108
Which app allows a user to run Splunk queries from within Phantom?

- A. Splunk App for Phantom?
- B. Splunk App for Phantom Reporting.
- C. The Integrated Splunk/Phantom app.
- D. Phantom App for Splunk.

Answer: D

Explanation:
The Phantom App for Splunk allows a user to run Splunk queries from within Phantom. This app provides actions such as run query, ingest events, and save search, which enable the user to interact with Splunk from Phantom playbooks or the Phantom UI. The other apps are not relevant for this use case. The Splunk App for Phantom is used to send data from Splunk to Phantom. The Integrated Splunk/Phantom app is a deprecated app that was replaced by the Splunk App for Phantom. The Splunk App for Phantom Reporting is used to generate reports on Phantom activity from Splunk. The Phantom App for Splunk is the application that enables Splunk users to run Splunk queries from within the Splunk Phantom platform. This app integrates Splunk's data and search capabilities into Phantom's security automation and orchestration framework, allowing users to perform actions such as running searches, creating events, and updating records in Splunk directly from Phantom.

NEW QUESTION # 109
What users are included in a new installation of SOAR?

- A. Only the admin user is included by default.
- B. The admin, power, and user users are included by default.
- C. No users are included by default.
- D. The admin and automation users are included by default.

Answer: D

Explanation:
The admin and automation users are included by default. Comprehensive Explanation and References of answer: According to the Splunk SOAR (On-premises) default credentials, script options, and sample
configuration files documentation1, the default credentials on a new installation of Splunk SOAR (On-premises) are:
Web Interface Username: soar_local_admin password: password

On Splunk SOAR (On-premises) deployments which have been upgraded from earlier releases the user account admin becomes a normal user account with the Administrator role.
The automation user is a special user account that is used by Splunk SOAR (On-premises) to run actions and playbooks. It has the Automation role, which grants it full access to all objects and data in Splunk SOAR (On-premises).
The other options are incorrect because they either omit the automation user or include users that are not created by default. For example, option B includes the power and user users, which are not part of the default installation. Option C only includes the admin user, which ignores the automation user. Option D claims that no users are included by default, which is false.
In a new installation of Splunk SOAR, two default user accounts are typically created: admin and automation.
The admin account is intended for system administration tasks, providing full access to all features and settings within the SOAR platform. The automation user is a special account used for automated processes and scripts that interact with the SOAR platform, often without requiring direct human intervention. This user has specific permissions that can be tailored for automated tasks. Options B, C, and D do not accurately represent the default user accounts included in a new SOAR installation, making option A the correct answer.

NEW QUESTION # 110
After a playbook has run, where are the results stored?

- A. Log file
- B. Container
- C. Splunk Index
- D. Case

Answer: B

Explanation:
The correct answer is C because after a playbook has run, the results are stored in the container that triggered the playbook. The container is a data object that represents an event or a case in Phantom. The container contains information such as the name, the description, the severity, the status, the owner, and the labels of the event or case. The container also contains the artifacts, the action results, the comments, the notes, and the phases and tasks associated with the event or case. The answer A is incorrect because after a playbook has run, the results are not stored in a Splunk index, which is a data structure that stores events from various data sources in Splunk. The Splunk index is not directly accessible by Phantom, but can be queried by Phantom using the Splunk app. The answer B is incorrect because after a playbook has run, the results are not stored in a case, which is a type of container that represents a security incident in Phantom. The case is a subset of the container, and not all containers are cases. The answer D is incorrect because after a playbook has run, the results are not stored in a log file, which is a file that records the activities or events that occur in a system or a process. The log file is not a data object in Phantom, but can be a data source for Phantom. Reference: Splunk SOAR User Guide, page 19. In Splunk Phantom, after a playbook has been executed, the results of the actions within that playbook are stored in the container associated with the event. A container is a data structure that encapsulates all relevant information and data for an incident or event within Phantom, including action results, artifacts, notes, and more. The container allows users to see a consolidated view of all the data and activity related to a particular event. These results are not stored in the Splunk Index, a separate case, or a log file as their primary storage but may be sent to a Splunk index for further analysis.

NEW QUESTION # 111
.....

SPLK-2003 " and download it for free immediately on " www.vce4dumps.com " □Valid SPLK-2003 Exam Syllabus

- SPLK-2003 Test Papers □ Exam Dumps SPLK-2003 Provider □ Passing SPLK-2003 Score Feedback ➽ [www.pdfvce.com] is best website to obtain ➽ SPLK-2003 □ for free download □SPLK-2003 Detailed Answers
- Pass Leader SPLK-2003 Dumps □ Valid SPLK-2003 Exam Syllabus □ SPLK-2003 Associate Level Exam □ Open （ www.practicevce.com ） and search for ➥ SPLK-2003 □ to download exam materials for free □SPLK-2003 Official Study Guide
- Valid SPLK-2003 Exam Syllabus □ Valid SPLK-2003 Exam Syllabus □ SPLK-2003 Valid Test Duration □ Open website 「 www.pdfvce.com 」 and search for 【 SPLK-2003 】 for free download □SPLK-2003 Official Study Guide
- 100% Pass Quiz 2026 Authoritative Splunk Sample SPLK-2003 Test Online □ Search for □ SPLK-2003 □ on 《 www.practicevce.com 》 immediately to obtain a free download □SPLK-2003 Test Papers
- Pdf SPLK-2003 Torrent □ SPLK-2003 Detailed Answers □ Passing SPLK-2003 Score Feedback □ Enter " www.pdfvce.com " and search for 《 SPLK-2003 》 to download for free □SPLK-2003 Practice Guide
- Prepare Exam Effectively With Desktop Splunk SPLK-2003 Practice Test Software □ Open ➥ www.pdfdumps.com □ and search for " SPLK-2003 " to download exam materials for free □Valid SPLK-2003 Exam Syllabus
- Splunk Sample SPLK-2003 Test Online - Latest-updated Valid SPLK-2003 Test Pass4sure and Useful Splunk Phantom Certified Admin Accurate Study Material □ Search for ✔ SPLK-2003 □✔□ and download exam materials for free through ➤ www.pdfvce.com □ □SPLK-2003 Latest Braindumps Book
- SPLK-2003 Study Guide - SPLK-2003 Free Download pdf - SPLK-2003 Latest Pdf Vce □ Open { www.easy4engine.com } and search for { SPLK-2003 } to download exam materials for free □Reliable SPLK-2003 Exam Price
- bbs.t-firefly.com, 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, www.stes.tyc.edu.tw, yqc-future.com, www.mixcloud.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, Disposable vapes

What's more, part of that TestKingIT SPLK-2003 dumps now are free: https://drive.google.com/open?id=1Q2mQySZQfL0r7ZzVepGRD1abdidC33mT