

100% Pass 2026 Splunk SPLK-2003 Updated Downloadable PDF



P.S. Free 2025 Splunk SPLK-2003 dumps are available on Google Drive shared by RealVCE: <https://drive.google.com/open?id=1FXqQ1fzEX-0JZkGoU9ZQ-OmGu1MdHIAo>

In order to serve you better, we have offline and online chat service stuff, and any questions about SPLK-2003 training materials, you can consult us directly or you can send your questions to us by email. In addition, SPLK-2003 exam dumps of us will offer you free demo, and you can have a try before purchasing. Free demo will help you to have a deeper understanding of what you are going to buy. If you have any question about the SPLK-2003 Training Materials of us, you can just contact us.

Splunk Phantom Certified Admin Exam is an advanced-level certification that requires a deep understanding of the Splunk Phantom platform. SPLK-2003 exam covers a variety of topics, including architecture, deployment, configuration, automation, integration, and troubleshooting. It is a 90-minute exam that consists of 60 multiple-choice questions. The passing score for the exam is 70%, and it is available in multiple languages.

Splunk SPLK-2003 exam, also known as the Splunk Phantom Certified Admin exam, is designed for IT professionals who have experience with Splunk Phantom, a security automation and orchestration platform. SPLK-2003 Exam measures an individual's knowledge and skills related to the administration of Splunk Phantom, including its installation, configuration, and management. Splunk Phantom Certified Admin certification is ideal for individuals who are responsible for managing security operations, incident response, and other security-related tasks using Splunk Phantom.

[**>> Downloadable SPLK-2003 PDF <<**](#)

SPLK-2003 Study Demo - Book SPLK-2003 Free

Our PDF version is a printable document of exam questions which are real and updated. We have included original Splunk Phantom Certified Admin questions in this format so that you can get ready for the exam quickly by just memorizing them. This format of Splunk Phantom Certified Admin (SPLK-2003) test questions is also usable on smart devices such as laptops, tablets, and smartphones.

Splunk Phantom Certified Admin Sample Questions (Q71-Q76):

NEW QUESTION # 71

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

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

Answer: B

NEW QUESTION # 72

Which of the following describes the use of labels in Phantom?

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

Answer: D

Explanation:

Explanation

The correct answer is D because labels determine which playbook(s) are executed when a container is created.

Labels are tags that can be applied to containers to categorize them and trigger playbook automation. Labels can be added manually or automatically based on rules or ingestion settings. The answer A is incorrect because labels do not determine the service level agreement (SLA) for a container, which is a metric that measures the time taken to resolve a case. The answer B is incorrect because labels do not control the default severity, ownership, and sensitivity for the container, which are attributes that can be set independently of labels. The answer C is incorrect because labels do not control which apps are allowed to execute actions on the container, which are determined by the asset configuration and the playbook logic. Reference: Splunk SOAR User Guide, page 23.

NEW QUESTION # 73

When writing a custom function that uses regex to extract the domain name from a URL, a user wants to create a new artifact for the extracted domain. Which of the following Python API calls will create a new artifact?

- A. phantom.add_artifact()
- B. phantom.create_artifact()
- C. phantom.update()
- D. phantom.new_artifact()

Answer: B

Explanation:

In the Splunk SOAR platform, when writing a custom function in Python to handle data such as extracting a domain name from a URL, you can create a new artifact using the Python API call `phantom.create_artifact()`. This function allows you to specify the details of the new artifact, such as the type, CEF (Common Event Format) data, container it belongs to, and other relevant information necessary to create an artifact within the system.

NEW QUESTION # 74

Which of the following roles is appropriate for a Splunk SOAR account that will only be used to execute automated tasks?

- A. Non-Human
- B. Automation
- C. Service Account
- D. Automation Engineer

Answer: B

Explanation:

In Splunk SOAR, the appropriate role for an account that will only be used to execute automated tasks is the "Automation" role. This service account role is specifically designed for automated tasks, including REST API operations, playbook execution, and ingestion. It is intended for use by systems rather than human users and provides the necessary permissions for automated interactions with the SOAR platform.

In Splunk SOAR, the "Automation" role is designed specifically for accounts that are intended for executing automated tasks. These tasks can include REST API operations, playbook actions, and data ingestion processes. The Automation role is a type of service account role intended for system-to-system interactions and is not meant to be used by human operators. It provides a tailored set of permissions that allows for the execution of automated processes without granting broader access that would be unnecessary or insecure for an automated account.

The designation of this role is critical in maintaining proper security and operational boundaries within the SOAR platform. By

restricting the automated account to just the Automation role, Splunk SOAR ensures that automated processes run with the least privilege necessary, reducing the risk of unauthorized actions and maintaining a clear separation between human users and automated systems.

NEW QUESTION # 75

Under Asset Ingestion Settings, how many labels must be applied when configuring an asset?

- A. One.
- B. Labels are not configured under Asset Ingestion Settings.
- C. Zero or more.
- D. One or more.

Answer: C

Explanation:

Under Asset Ingestion Settings in Splunk SOAR, when configuring an asset, the number of labels that must be applied can be zero or more. Labels are optional and are used to categorize data and control access. They are not a requirement under Asset Ingestion Settings, but they can be used to enhance organization and filtering if chosen.

NEW QUESTION # 76

• • • • •

If you are new to our SPLK-2003 exam questions, you may doubt about them a lot. And that is normal. Many of our loyal customers first visited our website, or even they have bought and studied with our SPLK-2003 practice engine, they would worried a lot. But when they finally passed the exam with our SPLK-2003 simulating exam, they knew that it is valid and helpful. And we also have free demos on our website, then you will know the quality of our SPLK-2003 training quiz.

SPLK-2003 Study Demo: https://www.realvce.com/SPLK-2003_free-dumps.html

BONUS!!! Download part of RealVCE SPLK-2003 dumps for free: <https://drive.google.com/open?id=1FXqQ1fzEX-0JZkGoU9ZQ-OmGu1MdHIAo>