Newest SPLK-2003 - Exam Splunk Phantom Certified Admin Revision Plan

What's more, part of that Exam-Killer SPLK-2003 dumps now are free: https://drive.google.com/open?id=12ygGavgrqt4VlYv_OETSxVFWZwbaI__S

Exam-Killer Splunk Phantom Certified Admin (SPLK-2003) practice test software is another great way to reduce your stress level when preparing for the Splunk Exam Questions. With our software, you can practice your excellence and improve your competence on the Splunk SPLK-2003 Exam Dumps. Each Splunk SPLK-2003 practice exam, composed of numerous skills, can be measured by the same model used by real examiners.

Splunk SPLK-2003 certification exam is a valuable certification for IT professionals who want to validate their skills in managing and maintaining Splunk Phantom instances. By earning this certification, professionals can demonstrate their expertise in the field and increase their value to their organization.

Splunk SPLK-2003 exam is designed for IT professionals who are seeking to become certified administrators of the Splunk Phantom platform. Splunk Phantom is a security orchestration, automation, and response (SOAR) solution that helps organizations streamline their security operations and improve their incident response capabilities. SPLK-2003 Exam covers a range of topics, including installation and configuration, user management, workflow design, automation, and integration with other security tools. Passing the SPLK-2003 exam demonstrates a candidate's knowledge and skills in using Splunk Phantom to automate and orchestrate security tasks, enabling organizations to respond more quickly and effectively to security incidents.

>> Exam SPLK-2003 Revision Plan <<

Reliable SPLK-2003 Exam Vce - SPLK-2003 Latest Guide Files

Our SPLK-2003 exam questions can assure you that you will pass the SPLK-2003 exam as well as getting the related certification under the guidance of our SPLK-2003 study materials as easy as pie. Firstly, the pass rate among our customers has reached as high as 98% to 100%, which marks the highest pass rate in the field. Secondly, you can get our SPLK-2003 Practice Test only in 5 to 10 minutes after payment, which enables you to devote yourself to study as soon as possible.

Splunk SPLK-2003 (Splunk Phantom Certified Admin) certification exam is an excellent way for IT professionals to validate their skills and knowledge in the administration of the Splunk Phantom platform. Passing the exam demonstrates that the candidate has a solid understanding of the platform and is capable of managing and supporting Splunk Phantom deployments.

Splunk Phantom Certified Admin Sample Questions (Q30-Q35):

NEW QUESTION # 30
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: sudo phenv python ibackup.pyc --backup -backup-type full, then sudo phenv python ibackup.pyc --setup.
- B. Within the UI: Select from the main menu Administration > System Health > Backup.
- C. Within the UI: Select from the main menu Administration > Product Settings > Backup.

- D. On the command line enter: rode sudo python ibackup.pyc --setup, then audo phenv python ibackup.pyc --backup.

Answer: A

Explanation:
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.

NEW QUESTION # 31
What is the main purpose of using a customized workbook?

- A. Workbooks guide user activity and coordination during event analysis and case operations.
- B. Workbooks apply service level agreements (SLAs) to containers and monitor completion status on the ROI dashboard.
- C. Workbooks may not be customized; only default workbooks are permitted within Phantom.
- D. Workbooks automatically implement a customized processing of events using Python code.

Answer: C

NEW QUESTION # 32
Is it possible to import external Python libraries such as the time module?

- A. No, but this can be changed by setting the proper permissions.
- B. Yes. from a drop down menu.
- C. No.
- D. Yes, in the global block.

Answer: D

NEW QUESTION # 33
Which of the following supported approaches enables Phantom to run on a Windows server?

- A. Install the Phantom RPM in a GNU Cygwin implementation.
- B. Run the Phantom OVA as a virtual machine.
- C. Run the Phantom OVA as a cloud instance.
- D. Install the Phantom RPM file in Windows Subsystem for Linux (WSL).

Answer: B

Explanation:
Explanation
The correct answer is D because the Phantom OVA can be run as a virtual machine on a Windows server using a hypervisor such as VMware Workstation or Hyper-V. This is the recommended approach for installing Phantom on a Windows server. The answer A is incorrect because the Phantom RPM cannot be installed in a GNU Cygwin implementation, as Cygwin does not support RPM packages. The answer B is incorrect because running the Phantom OVA as a cloud instance does not enable Phantom to run on a Windows server, but on a cloud platform such as AWS or Azure. The answer C is incorrect because the Phantom RPM file cannot be installed in Windows Subsystem for Linux (WSL), as WSL does not support RPM packages.
Reference: Splunk SOAR Installation Guide, page 9.

NEW QUESTION # 34
How can a playbook run searches on a Splunk search head?

- A. Using the phantom.run_query() API function.
- B. Using the search action of the Search app.
- C. Using the run_query action from the Splunk app.
- D. Use the HTTP app's get_data action to access the SOAR .../rest/splunk/query endpoint.

Answer: C

NEW QUESTION # 35

.....