高效最新SPLK-2003題庫資源和資格考試中的領先供應平臺和免費PDF Splunk Splunk Phantom Certified Admin

2026 KaoGuTi最新的SPLK-2003 PDF版考試題庫和SPLK-2003考試問題和答案免費分享：https://drive.google.com/open?id=10jlVQTusZgAWEqcQtYIbkkioeLGHQqcE

現在有許多IT培訓機構都能為你提供Splunk SPLK-2003 認證考試相關的培訓資料，但通常考生通過這些網站得不到詳細的資料。因為他們提供的關於Splunk SPLK-2003 認證考試資料都比較寬泛，不具有針對性，所以吸引不了考生的注意力。

Splunk SPLK-2003考試是為了想成為認證Splunk Phantom管理員的IT專業人士而設計的。考試測試候選人對Splunk Phantom平台的了解程度以及他們有效配置和管理平台的能力。它包含了許多主題，包括平台架構、安裝和配置、自動化和協調，以及高級功能，例如自定義操作和整合。

Splunk SPLK-2003：Splunk Phantom認證管理員是專為IT管理員和安全專業人員設計的認證考試，他們負責管理和維護Splunk Phantom平臺。Splunk Phantom是一個結合了安全自動化和協調技術的安全協調、自動化和響應（SOAR）解決方案。此考試驗證候選人在配置、部署和管理Splunk Phantom方面的知識和技能。

>> 最新SPLK-2003題庫資源 <<

確保通過的最新SPLK-2003題庫資源 |第一次嘗試輕鬆學習並通過考試和完美的SPLK-2003：Splunk Phantom Certified Admin

針對企業競爭形勢的新要求，像 Splunk 的 SPLK-2003 一些熱門的專業證照考試誕生了，其中包括ISC、Fortinet、Adobe、EMC、Veritas、GAQM和HP等。在國際上，許多企業已從1995年起安排員工參加了各專業的證照考試。他們的實踐證明，專業的SPLK-2003 證照不僅提高了員工的技術水準，增強了企業的市場競爭能力，而且更重要的是，這些企業由於在更新員工技能方面所付出的努力以及所表現出的遠見卓識，使KaoGuTi SPLK-2003 證照已贏得了企業內外的一致好評。

Splunk SPLK-2003認證考試專為希望成為經過認證的Splunk Phantom管理員的個人而設計。認證考試測試候選人對Splunk Phantom平台的了解及其配置，管理和故障排除幻影實例的能力。考試衡量了候選人在部署，自動化和與其他技術集成等領域的技能。

最新的 Splunk SOAR Certified Automation Developer SPLK-2003 免費考試真題 (Q98-Q103):

問題 #98
On the Splunk search head, when configuring the app to search SOAR searchable content, what are the two requirements to complete the app setup?

- A. User accounts and universal forwarder.
- B. User accounts and syslog.

- C. User accounts and REST API.
- D. User accounts and an HTTP Event Collector token.

答案：D

解題說明：
When configuring the Splunk app on the search head to search SOAR (Splunk's Security Orchestration, Automation, and Response) searchable content, two key components are required:
* User Accounts: The user accounts are necessary to authenticate and authorize users who are accessing SOAR data through the Splunk app. These accounts manage permissions and access levels to ensure the proper users can search and interact with the data coming from SOAR.
* HTTP Event Collector (HEC) Token: The HEC token is crucial because it allows the Splunk app to receive data from Splunk SOAR. SOAR sends events and other data to the Splunk platform via HEC.
This token is used for secure communication and authentication between Splunk and SOAR. The token must be configured in the Splunk app to allow it to collect and search SOAR data seamlessly.
Other options like syslog, REST API, or a universal forwarder are commonly used methods for ingesting data into Splunk but are not specific requirements for setting up the Splunk app to search SOAR content. The HTTP Event Collector is the primary method for this setup, along with the correct user accounts.
References:
* Splunk Documentation on HTTP Event Collector and SOAR Integration.
* Splunk SOAR App Setup Guide for Splunk Search Head Configuration.

問題 #99
How can more than one user perform tasks in a workbook?

- A. Add the required users to the authorized list for the container.
- B. Any user with a role that has Perform Task enabled can execute tasks for workbooks.
- C. Any user in a role with write access to the case's workbook can be assigned to tasks.
- D. The container owner can assign any authorized user to any task in a workbook.

答案：B

解題說明：
In Splunk SOAR, tasks within workbooks can be performed by any user whose role has the
'Perform Task' capability enabled. This capability is assigned within the role configuration and allows users with the appropriate permissions to execute tasks. It is not limited to users with write access or the container owner; rather, it is based on the specific permissions granted to the role with which the user is associated.

問題 #100
A user wants to use their Splunk Cloud instance as the external Splunk instance for Phantom. What ports need to be opened on the Splunk Cloud instance to facilitate this? Assume default ports are in use.

- A. TCP 80 and TCP 443.
- B. TCP 8088 and TCP 8099.
- C. Splunk Cloud is not supported.
- D. TCP 8080 and TCP 8191.

答案：D

問題 #101
A filter block with only one condition configured which states: artifact.*.cef .sourceAddress !- , would permit which of the following data to pass forward to the next block?

- A. Null IP addresses
- B. Non-null IP addresses
- C. Non-null destinationAddresses
- D. Null values

答案：B

解題說明：
Explanation
A filter block with only one condition configured which states: artifact.*.cef .sourceAddress !- , would permit only non-null IP addresses to pass forward to the next block. The !- operator means "is not null". The other options are not valid because they either include null values or other fields than sourceAddress. See Filter block for more details.

問題 #102
How does a user determine which app actions are available?

- A. Add an action block to a playbook canvas area.
- B. Search the Apps category in the global search field.
- C. From the Apps menu, click the supported actions dropdown for each app.
- D. In the visual playbook editor, click Active and click the Available App Actions dropdown.

答案：C

解題說明：
In Splunk SOAR, a user can determine which app actions are available by navigating to the Apps menu. From there, the user can click on the supported actions dropdown for each app to view the actions that can be performed by that app. This dropdown menu provides a list of all the actions that the app is capable of executing, allowing the user to understand the functionality provided by the app and how it can be utilized within playbooks11.
References:
* Add and configure apps and assets to provide actions in Splunk SOAR (Cloud) - Splunk Documentation

問題 #103
.....

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, 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, Disposable vapes

此外，這些KaoGuTi SPLK-2003考試題庫的部分內容現在是免費的：https://drive.google.com/open?id=10jlVQTusZgAWEqcQtYIbkkioeLGHQqcE