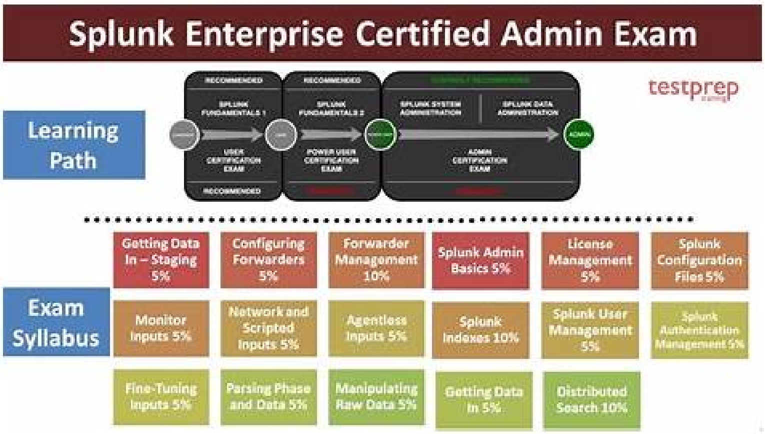
Splunk Phantom Certified Admin Exam Simulator & SPLK-2003 Pass4sure Vce & Splunk Phantom Certified Admin Study Torrent



BTW, DOWNLOAD part of Actual4Exams SPLK-2003 dumps from Cloud Storage: https://drive.google.com/open?id=13E5joiWOrRkGDZYbU6J6HAGOn4JZTr5z

The Actual4Exams Free Splunk SPLK-2003 Sample Questions, allow you to enjoy the process of buying risk-free. This is a version of the exercises, so you can see the quality of the questions, and the value before you decide to buy. We are confident that Actual4Exams the Splunk SPLK-2003 sample enough you satisfied with the product. In order to ensure your rights and interests, Actual4Exams commitment examination by refund. Our aim is not just to make you pass the exam, we also hope you can become a true IT Certified Professional. Help you get consistent with your level of technology and technical posts, and you can relaxed into the IT white-collar workers to get high salary.

Actual4Exams almost aimed to meet the needs of all candidates who want to pass the SPLK-2003 exam. If someone who don't have enough time to prepare for their exam, our website provide they with test answers which only need 20-30 hours to grasp; If someone who worry about failed the SPLK-2003 Exam, our website can guarantee that they can get full refund. In summary, the easiest way to prepare for SPLK-2003 certification exam is to complete SPLK-2003 study material.

>> SPLK-2003 Test Braindumps <<

SPLK-2003 actual exam torrent & SPLK-2003 practice materials & SPLK-2003 valid practice material

As long as you study with our SPLK-2003 exam braindumps for 20 to 30 hours that we can claim that you will pass the exam for sure. We really need this efficiency. Perhaps you have doubts about this "shortest time." I believe that after you understand the professional configuration of SPLK-2003 Training Questions, you will agree with what I said. What our SPLK-2003 study materials contain are all the real questions and answers that will come out in the real exam.

Splunk SPLK-2003 certification exam is designed for individuals who want to demonstrate their expertise in Splunk Phantom administration. SPLK-2003 exam is ideal for those who are responsible for managing and maintaining Splunk Phantom in an enterprise environment. SPLK-2003 exam is designed to test the candidate's knowledge and skills in areas such as Phantom architecture, automation and orchestration, incident response, and security operations. Passing SPLK-2003 Exam demonstrates that the candidate has the skills and knowledge required to successfully administer Splunk Phantom.

Splunk Phantom Certified Admin Sample Questions (Q21-Q26):

NEW QUESTION # 21
When configuring a Splunk asset for SOAR to connect to a Splunk Cloud instance, the user discovers that they need to be able to run two different on_poll searches. How is this possible?

- A. Install a second Splunk app and configure the query in the second app.

- B. Configure a second Splunk asset with the second query.
- C. Enter the two queries in the asset as comma separated values.
- D. Configure the second query in the Splunk App for SOAR Export.

Answer: B

Explanation:
In Splunk SOAR, when needing to run multiple on_poll searches to a Splunk Cloud instance, the recommended approach is to configure a second Splunk asset specifically for the second query. This method allows each Splunk asset to maintain its own settings and query configurations, ensuring that each search can be managed and optimized independently. This separation also helps in troubleshooting and maintaining clarity in the configuration.
Option A, installing a second Splunk app, is not necessarily relevant as the app itself does not determine the number of queries but rather how they are managed and processed through assets.
Option B, configuring the second query in the Splunk App for SOAR Export, does not apply as this app typically handles data exportation from SOAR to Splunk, not managing multiple polling queries.
Option C, entering the two queries as comma-separated values, would not be practical or functional as Splunk SOAR's asset configuration does not process multiple queries in this manner for polling purposes.
When configuring a Splunk asset for SOAR to connect to a Splunk Cloud instance and there is a need to run two different on_poll searches, the appropriate action is to configure a second Splunk asset with the second query. This allows each Splunk asset to have its own unique on_poll search configuration, enabling them to run independently and retrieve different sets of data as required. The other options, such as installing a second app or entering queries as comma-separated values, are not standard practices for managing multiple on_poll searches in Splunk SOAR1.
References:Splunk SOAR documentation on configuring search in Splunk SOAR1.

NEW QUESTION # 22
Where can the Splunk App for SOAR Export be downloaded from?

- A. Splunkbase and SOAR Community.
- B. SOAR Community and GitHub.
- C. GitHub and Splunkbase.
- D. Splunk Answers and Splunkbase.

Answer: C

Explanation:
The Splunk App for SOAR Export can be downloaded from both GitHub and Splunkbase. Splunkbase is the official source for Splunk apps, where users can find, try, and download apps that enhance and extend the capabilities of Splunk, including the Splunk App for SOAR Export1. GitHub is also a common platform for sharing and collaborating on code, including Splunk apps and integrations. It is important to ensure that you are downloading from the official repository or author to avoid any security risks.
References:
Splunkbase, the official source for downloading the Splunk App for SOAR Export

NEW QUESTION # 23
Which of the following is a step when configuring event forwarding from Splunk to Phantom?

- A. Map CEF to CIM fields.
- B. Create a Splunk alert that uses the event_forward.py script to send events to Phantom.
- C. Map CIM to CEF fields.
- D. Create a saved search that generates the JSON for the new container on Phantom.

Answer: B

Explanation:
A step when configuring event forwarding from Splunk to Phantom is to create a Splunk alert that uses the event_forward.py script to send events to Phantom. This script will convert the Splunk events to CEF format and send them to Phantom as containers. The other options are not valid steps for event forwarding.
See Forwarding events from Splunk to Phantom for more details.
Configuring event forwarding from Splunk to Phantom typically involves creating a Splunk alert that leverages a script (like event_forward.py) to automatically send triggered event data to Phantom. This setup enables Splunk to act as a detection

mechanism that, upon identifying notable events based on predefined criteria, forwards these events to Phantom for further orchestration, automation, and response actions. This integration streamlines the process of incident management by connecting Splunk's powerful data analysis capabilities with Phantom's orchestration and automation framework.

NEW QUESTION # 24

To limit the impact of custom code on the VPE, where should the custom code be placed?

- A. A custom container or a separate KV store.
- B. A separate code repository.
- C. A separate container.
- D. A custom function block.

Answer: D

Explanation:

To limit the impact of custom code on the Visual Playbook Editor (VPE) in Splunk SOAR, custom code should be placed within a custom function block. Custom function blocks are designed to encapsulate code within a playbook, allowing users to input their own Python code and execute it as part of the playbook run.

By confining custom code to these blocks, it maintains the VPE's performance and stability by isolating the custom code from the core functions of the playbook.

A custom function block is a way of adding custom Python code to your playbook, which can expand the functionality and processing of your playbook logic. Custom functions can also interact with the REST API in a customizable way. You can share custom functions across your team and across multiple playbooks to increase collaboration and efficiency. To create custom functions, you must have Edit Code permissions, which can be configured by an Administrator in Administration > User Management > Roles and Permissions. Therefore, option C is the correct answer, as it is the recommended way of placing custom code on the VPE, which limits the impact of custom code on the VPE performance and security. Option A is incorrect, because a custom container or a separate KV store are not valid ways of placing custom code on the VPE, but rather ways of storing data or artifacts. Option B is incorrect, because a separate code repository is not a way of placing custom code on the VPE, but rather a way of managing and versioning your code outside of Splunk SOAR. Option D is incorrect, because a separate container is not a way of placing custom code on the VPE, but rather a way of creating a new event or case.

1: Add custom code to your Splunk SOAR (Cloud) playbook with the custom function block using the classic playbook editor

NEW QUESTION # 25

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. Automation Engineer
- D. Service Account

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 # 26

......

The Splunk SPLK-2003 certification exam is a valuable asset for beginners and seasonal professionals. If you want to improve your career prospects then SPLK-2003 certification is a step in the right direction. Whether you're just starting your career or looking to advance your career, the SPLK-2003 Certification Exam is the right choice. With the SPLK-2003 certification you can gain a range of career benefits which include credibility, marketability, validation of skills, and access to new job opportunities.

Pass4sure SPLK-2003 Dumps Pdf: https://www.actual4exams.com/SPLK-2003-valid-dump.html

- High Pass-Rate Splunk SPLK-2003 Test Braindumps Are Leading Materials - Trustworthy Pass4sure SPLK-2003 Dumps Pdf □ Download ▹ SPLK-2003 ◃ for free by simply searching on （ www.torrentvce.com ） □Exam SPLK-2003 Pattern
- 100% Pass Updated Splunk - SPLK-2003 Test Braindumps □ The page for free download of { SPLK-2003 } on ➡ www.pdfvce.com □□□ will open immediately □SPLK-2003 Latest Exam Discount
- 100% Pass Updated Splunk - SPLK-2003 Test Braindumps □ Search for ▹ SPLK-2003 ◃ and obtain a free download on ➡ www.examcollectionpass.com □□□ □Valid SPLK-2003 Test Forum
- SPLK-2003 Excellect Pass Rate □ SPLK-2003 Excellect Pass Rate □ Cost Effective SPLK-2003 Dumps □ The page for free download of " SPLK-2003 " on ➠ www.pdfvce.com □ will open immediately □Exam SPLK-2003 Success
- Trusted SPLK-2003 Test Braindumps - Useful Splunk Certification Training - Trustworthy Splunk Splunk Phantom Certified Admin □ The page for free download of " SPLK-2003 " on ▹ www.practicevce.com ◃ will open immediately □SPLK-2003 Excellect Pass Rate
- Valid SPLK-2003 Test Forum □ Reliable SPLK-2003 Test Braindumps ✉ SPLK-2003 Real Sheets □ Easily obtain ✔ SPLK-2003 □✔□ for free download through ➡ www.pdfvce.com □□□ □Updated SPLK-2003 Demo
- Exam SPLK-2003 Simulator Free □ SPLK-2003 Book Free □ Reliable SPLK-2003 Test Braindumps □ Search for □ SPLK-2003 □ and easily obtain a free download on ➤ www.testkingpass.com □ □SPLK-2003 Book Free
- Trusted SPLK-2003 Test Braindumps - Useful Splunk Certification Training - Trustworthy Splunk Splunk Phantom Certified Admin □ Go to website □ www.pdfvce.com □ open and search for （ SPLK-2003 ） to download for free □Valid SPLK-2003 Test Forum
- Updated SPLK-2003 Demo □ Updated SPLK-2003 Demo □ SPLK-2003 Book Free □ Simply search for ▹ SPLK-2003 ◃ for free download on （ www.pdfdumps.com ） □Cost Effective SPLK-2003 Dumps
- Precise SPLK-2003 Test Braindumps bring you First-Grade Pass4sure SPLK-2003 Dumps Pdf for Splunk Splunk Phantom Certified Admin □ Enter ▸ www.pdfvce.com ◂ and search for 《 SPLK-2003 》 to download for free □Reliable SPLK-2003 Test Braindumps
- Free PDF Quiz 2026 First-grade Splunk SPLK-2003: Splunk Phantom Certified Admin Test Braindumps □ Open [www.prepawayexam.com] enter 「 SPLK-2003 」 and obtain a free download □Exam SPLK-2003 Simulator Free
- myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, telegra.ph, Disposable vapes

2026 Latest Actual4Exams SPLK-2003 PDF Dumps and SPLK-2003 Exam Engine Free Share: https://drive.google.com/open?id=13E5joiWOrRkGDZYbU6J6HAGOn4JZTr5z