SPLK-1003 Q&As

Splunk Enterprise Certified Admin

Pass Splunk SPLK-1003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/splk-1003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

When configuring HTTP Event Collector (HEC) input, how would one ensure the events have been indexed?

A. Enable indexer acknowledgment.

B. Enable forwarder acknowledgment.

C. splunk check-integrity -index

D. index=_internal component=ACK | stats count by host

Correct Answer: A

Per the provided Splunk reference URL

"While HEC has precautions in place to prevent data loss, it\\'s impossible to completely prevent such an occurrence, especially in the event of a network failure or hardware crash.

This is where indexer acknolwedgment comes in."

Reference https://docs.splunk.com/Documentation/Splunk/8.0.5/Data/AboutHECIDXAck

QUESTION 2

Consider a company with a Splunk distributed environment in production. The Compliance Department wants to start using Splunk; however, they want to ensure that no one can see their reports or any other knowledge objects. Which Splunk Component can be added to implement this policy for the new team?

A. Indexer

B. Deployment server

C. Universal forwarder

D. Search head

Correct Answer: D

QUESTION 3

An organization wants to collect Windows performance data from a set of clients, however, installing Splunk software on these clients is not allowed. What option is available to collect this data in Splunk Enterprise?

A. Use Local Windows host monitoring.

B. Use Windows Remote Inputs with WMI.

C. Use Local Windows network monitoring.

D. Use an index with an Index Data Type of Metrics.

Correct Answer: B

https://docs.splunk.com/Documentation/Splunk/8.1.0/Data/ConsiderationsfordecidinghowtomonitorWindowsdata

"The Splunk platform collects remote Windows data for indexing in one of two ways: From Splunk forwarders, Using Windows Management Instrumentation (WMI). For Splunk Cloud deployments, you must use the Splunk Universal Forwarder on a Windows machines to montior remote Windows data."

QUESTION 4

Which of the following is a benefit of distributed search?

A. Peers run search in sequence.

B. Peers run search in parallel.

C. Resilience from indexer failure.

D. Resilience from search head failure.

Correct Answer: B

https://docs.splunk.com/Documentation/Splunk/8.2.2/DistSearch/Whatisdistributedsearch

Parallel reduce search processing If you struggle with extremely large high-cardinality searches, you might be able to apply parallel reduce processing to them to help them complete faster. You must have a distributed search environment to use parallel reduce search processing.

QUESTION 5

What is required when adding a native user to Splunk? (select all that apply)

A. Password

B. Username

C. Full Name

D. Default app

Correct Answer: AB

According to the Splunk system admin course PDF, When adding native users, Username and Password ARE REQUIRED