



SPLK-3001^{Q&As}

Splunk Enterprise Security Certified Admin

Pass Splunk SPLK-3001 Exam with 100% Guarantee

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

<https://www.pass4itsure.com/splk-3001.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**

Glass tables can display static images and text, the results of ad-hoc searches, and which of the following objects?

- A. Lookup searches.
- B. Summarized data.
- C. Security metrics.
- D. Metrics store searches.

Correct Answer: C

Reference: <https://docs.splunk.com/Documentation/ES/6.1.0/User/CreateGlassTable>

QUESTION 2

When installing Enterprise Security, what should be done after installing the add-ons necessary for normalizing data?

- A. Configure the add-ons according to their README or documentation.
- B. Disable the add-ons until they are ready to be used, then enable the add-ons.
- C. Nothing, there are no additional steps for add-ons.
- D. Configure the add-ons via the Content Management dashboard.

Correct Answer: A

QUESTION 3

The Remote Access panel within the User Activity dashboard is not populating with the most recent hour of data. What data model should be checked for potential errors such as skipped searches?

- A. Web
- B. Risk
- C. Performance
- D. Authentication

Correct Answer: D

Reference: <https://answers.splunk.com/answers/565482/how-to-resolve-skipped-scheduled-searches.html>

QUESTION 4



A site has a single existing search head which hosts a mix of both CIM and non-CIM compliant applications. All of the applications are mission-critical. The customer wants to carefully control cost, but wants good ES performance. What is the best practice for installing ES?

- A. Install ES on the existing search head.
- B. Add a new search head and install ES on it.
- C. Increase the number of CPUs and amount of memory on the search head, then install ES.
- D. Delete the non-CIM-compliant apps from the search head, then install ES.

Correct Answer: B

Reference: <https://www.splunk.com/pdfs/technical-briefs/splunk-validated-architectures.pdf>

QUESTION 5

A customer site is experiencing poor performance. The UI response time is high and searches take a very long time to run. Some operations time out and there are errors in the scheduler logs, indicating too many concurrent searches are being started. 6 total correlation searches are scheduled and they have already been tuned to weed out false positives.

Which of the following options is most likely to help performance?

- A. Change the search heads to do local indexing of summary searches.
- B. Add heavy forwarders between the universal forwarders and indexers so inputs can be parsed before indexing.
- C. Increase memory and CPUs on the search head(s) and add additional indexers.
- D. If indexed realtime search is enabled, disable it for the notable index.

Correct Answer: C

[SPLK-3001 PDF Dumps](#)

[SPLK-3001 VCE Dumps](#)

[SPLK-3001 Practice Test](#)