



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

Which indexes are searched by default for CIM data models?

- A. notable and default
- B. summary and notable
- C. _internal and summary
- D. All indexes

Correct Answer: D

Reference: <https://answers.splunk.com/answers/600354/indexes-searched-by-cim-data-models.html>

QUESTION 2

What are the steps to add a new column to the Notable Event table in the Incident Review dashboard?

- A. Configure -> Incident Management -> Notable Event Statuses
- B. Configure -> Content Management -> Type: Correlation Search
- C. Configure -> Incident Management -> Incident Review Settings -> Event Management
- D. Configure -> Incident Management -> Incident Review Settings -> Table Attributes

Correct Answer: D

Reference: <https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Customizenotables>

QUESTION 3

Both "Recommended Actions" and "Adaptive Response Actions" use adaptive response.

How do they differ?

- A. Recommended Actions show a textual description to an analyst, Adaptive Response Actions show them encoded.
- B. Recommended Actions show a list of Adaptive Responses to an analyst, Adaptive Response Actions run them automatically.
- C. Recommended Actions show a list of Adaptive Responses that have already been run, Adaptive Response Actions run them automatically.
- D. Recommended Actions show a list of Adaptive Responses to an analyst, Adaptive Response Actions run manually with analyst intervention.

Correct Answer: D



Reference: <https://docs.splunk.com/Documentation/ES/latest/Admin/Configureadaptiveveresponse>

QUESTION 4

How should an administrator add a new lookup through the ES app?

- A. Upload the lookup file in Settings -> Lookups -> Lookup Definitions
- B. Upload the lookup file in Settings -> Lookups -> Lookup table files
- C. Add the lookup file to /etc/apps/SplunkEnterpriseSecuritySuite/lookups
- D. Upload the lookup file using Configure -> Content Management -> Create New Content -> Managed Lookup

Correct Answer: D

Reference: <https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Createlookups>

QUESTION 5

In order to include an eventtype in a data model node, what is the next step after extracting the correct fields?

- A. Save the settings.
- B. Apply the correct tags.
- C. Run the correct search.
- D. Visit the CIM dashboard.

Correct Answer: C

Reference: <https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizeOSSECdata>

[Latest SPLK-3001 Dumps](#)

[SPLK-3001 VCE Dumps](#)

[SPLK-3001 Practice Test](#)