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.leads4pass.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

When using distributed configuration management to create the Splunk_TA_ForIndexers package, which three files can be included?

A. indexes.conf, props.conf, transforms.conf

B. web.conf, props.conf, transforms.conf

C. inputs.conf, props.conf, transforms.conf

D. eventtypes.conf, indexes.conf, tags.conf

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/ES/6.4.1/Install/InstallTechnologyAdd-ons

QUESTION 2

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

QUESTION 3

Enterprise Security\\'s dashboards primarily pull data from what type of knowledge object?

A. Tstats

B. KV Store

C. Data models

D. Dynamic lookups

Correct Answer: C

Reference: https://docs.splunk.com/Splexicon:Knowledgeobject

QUESTION 4

How is it possible to navigate to the list of currently-enabled ES correlation searches?

A. Configure -> Correlation Searches -> Select Status "Enabled"

B. Settings -> Searches, Reports, and Alerts -> Filter by Name of "Correlation"

C. Configure -> Content Management -> Select Type "Correlation" and Status "Enabled"

D. Settings -> Searches, Reports, and Alerts -> Select App of "SplunkEnterpriseSecuritySuite" and filter by "-Rule"

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Listcorrelationsearches

QUESTION 5

Which of the following is part of tuning correlation searches for a new ES installation?

A. Configuring correlation notable event index.

B. Configuring correlation permissions.

C. Configuring correlation adaptive responses.

D. Configuring correlation result storage.

Correct Answer: A