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.pass2lead.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

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 2

What is the main purpose of the Dashboard Requirements Matrix document?

A. Identifies on which data model(s) each dashboard depends.

B. Provides instructions for customizing each dashboard for local data models.

C. Identifies the searches used by the dashboards.

D. Identifies which data model(s) depend on each dashboard.

Correct Answer: D

QUESTION 3

Which of the following actions would not reduce the number of false positives from a correlation search?

A. Reducing the severity.

B. Removing throttling fields.

C. Increasing the throttling window.

D. Increasing threshold sensitivity.

Correct Answer: A

QUESTION 4

Which of the following is a recommended pre-installation step?

A. Disable the default search app.

B. Configure search head forwarding.

C. Download the latest version of KV Store from MongoDBxom.

D. Install the latest Python distribution on the search head.

Correct Answer: B

QUESTION 5

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 6

Which setting is used in indexes.conf to specify alternate locations for accelerated storage?

A. thawedPath

B. tstatsHomePath

C. summaryHomePath

D. warmToColdScript

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Acceleratedatamodels

QUESTION 7

Which data model populated the panels on the Risk Analysis dashboard?

A. Risk

B. Audit

C. Domain analysis

D. Threat intelligence

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/RiskAnalysis#Dashboard_panels

QUESTION 8

Which correlation search feature is used to throttle the creation of notable events?

A. Schedule priority.

B. Window interval.

C. Window duration.

D. Schedule windows.

Correct Answer: C

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

QUESTION 9

ES apps and add-ons from $SPLUNK_HOME/etc/apps should be copied from the staging instance to what location on the cluster deployer instance?

A. $SPLUNK_HOME/etc/master-apps/

B. $SPLUNK_HOME/etc/system/local/

C. $SPLUNK_HOME/etc/shcluster/apps

D. $SPLUNK_HOME/var/run/searchpeers/

Correct Answer: C

The upgraded contents of the staging instance will be migrated back to the deployer and deployed to the search head cluster members. On the staging instance, copy $SPLUNK_HOME/etc/apps to $SPLUNK_HOME/etc/shcluster/apps on the deployer. 1. On the deployer, remove any deprecated apps or add-ons in $SPLUNK_HOME/etc/shcluster/apps that were removed during the upgrade on staging. Confirm by reviewing the ES upgrade report generated on staging, or by examining the apps moved into $SPLUNK_HOME/etc/disabled-apps on staging

QUESTION 10

How is notable event urgency calculated?

A. Asset priority and threat weight.

B. Alert severity found by the correlation search.

C. Asset or identity risk and severity found by the correlation search.

D. Severity set by the correlation search and priority assigned to the associated asset or identity.

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned

QUESTION 11

Where are attachments to investigations stored?

A. KV Store

B. notable index

C. attachments.csv lookup D. /etc/apps/SA-Investigations/default/ui/views/attachments

Correct Answer: A

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

QUESTION 12

Which column in the Asset or Identity list is combined with event security to make a notable event\\'s urgency?

A. VIP

B. Priority

C. Importance

D. Criticality

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned

QUESTION 13

Which of the following ES features would a security analyst use while investigating a network anomaly notable?

A. Correlation editor.

B. Key indicator search.

C. Threat download dashboard.

D. Protocol intelligence dashboard.

Correct Answer: D

Reference: https://www.splunk.com/en_us/products/premium-solutions/splunk-enterprise-security/ features.html

QUESTION 14

After installing Enterprise Security, the distributed configuration management tool can be used to create which app to configure indexers?

A. Splunk_DS_ForIndexers.spl

B. Splunk_ES_ForIndexers.spl

C. Splunk_SA_ForIndexers.spl

D. Splunk_TA_ForIndexers.spl

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallTechnologyAdd-ons

QUESTION 15

At what point in the ES installation process should Splunk_TA_ForIndexes.spl be deployed to the indexers?

A. When adding apps to the deployment server.

B. Splunk_TA_ForIndexers.spl is installed first.

C. After installing ES on the search head(s) and running the distributed configuration management tool.

D. Splunk_TA_ForIndexers.spl is only installed on indexer cluster sites using the cluster master and the splunk apply cluster-bundle command.

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallTechnologyAdd-ons