



Splunk

Exam Questions SPLK-3001

Splunk Enterprise Security Certified Admin Exam

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

The Add-On Builder creates Splunk Apps that start with what?

- A. DA-
- B. SA-
- C. TA-
- D. App-

Answer: C

Explanation:

Reference: <https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/abouttheessolution/>

NEW QUESTION 2

Which of the following is a way to test for a property normalized data model?

- A. Use Audit -> Normalization Audit and check the Errors panel.
- B. Run a | datamodel search, compare results to the CIM documentation for the datamodel.
- C. Run a | loadjob search, look at tag values and compare them to known tags based on the encoding.
- D. Run a | datamodel search and compare the results to the list of data models in the ES normalization guide.

Answer: B

Explanation:

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

NEW QUESTION 3

When investigating, what is the best way to store a newly-found IOC?

- A. Paste it into Notepad.
- B. Click the “Add IOC” button.
- C. Click the “Add Artifact” button.
- D. Add it in a text note to the investigation.

Answer: B

NEW QUESTION 4

Which of the following are data models used by ES? (Choose all that apply)

- A. Web
- B. Anomalies
- C. Authentication
- D. Network Traffic

Answer: B

Explanation:

Reference: <https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/datamodelsusedbyes/>

NEW QUESTION 5

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.

Answer: B

Explanation:

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

NEW QUESTION 6

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.

Answer: C

Explanation:

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

NEW QUESTION 7

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.

Answer: D

Explanation:

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

NEW QUESTION 8

What does the Security Posture dashboard display?

- A. Active investigations and their status.
- B. A high-level overview of notable events.
- C. Current threats being tracked by the SOC.
- D. A display of the status of security tools.

Answer: B

Explanation:

The Security Posture dashboard is designed to provide high-level insight into the notable events across all domains of your deployment, suitable for display in a Security Operations Center (SOC). This dashboard shows all events from the past 24 hours, along with the trends over the past 24 hours, and provides real-time event information and updates.

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

NEW QUESTION 9

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.

Answer: C

Explanation:

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

NEW QUESTION 10

Which of the following is a key feature of a glass table?

- A. Rigidity.
- B. Customization.
- C. Interactive investigations.
- D. Strong data for later retrieval.

Answer: B

NEW QUESTION 10

To observe what network services are in use in a network’s activity overall, which of the following dashboards in Enterprise Security will contain the most relevant data?

- A. Intrusion Center
- B. Protocol Analysis
- C. User Intelligence
- D. Threat Intelligence

Answer: A

Explanation:

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

NEW QUESTION 11

Which of the following would allow an add-on to be automatically imported into Splunk Enterprise Security?

- A. A prefix of CIM_
- B. A suffix of .spl
- C. A prefix of TECH_
- D. A prefix of Splunk_TA_

Answer: D

Explanation:

Reference: <https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/planintegrationes/>

NEW QUESTION 16

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/

Answer: C

Explanation:

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

NEW QUESTION 20

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.

Answer: D

Explanation:

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

NEW QUESTION 21

Which of the following threat intelligence types can ES download? (Choose all that apply)

- A. Text
- B. STIX/TAXII
- C. VulnScanSPL
- D. SplunkEnterpriseThreatGenerator

Answer: B

Explanation:

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

NEW QUESTION 22

If a username does not match the 'identity' column in the identities list, which column is checked next?

- A. Email.
- B. Nickname
- C. IP address.
- D. Combination of Last Name, First Name.

Answer: C

NEW QUESTION 27

Which of the following features can the Add-on Builder configure in a new add-on?

- A. Expire data.
- B. Normalize data.
- C. Summarize data.
- D. Translate data.

Answer: B

Explanation:

Reference: <https://docs.splunk.com/Documentation/AddonBuilder/3.0.1/UserGuide/Overview>

NEW QUESTION 29

The Brute Force Access Behavior Detected correlation search is enabled, and is generating many false positives. Assuming the input data has already been validated. How can the correlation search be made less sensitive?

- A. Edit the search and modify the notable event status field to make the notable events less urgent.
- B. Edit the search, look for where or xswhere statements, and after the threshold value being compared to make it less common match.
- C. Edit the search, look for where or xswhere statements, and alter the threshold value being compared to make it a more common match.
- D. Modify the urgency table for this correlation search and add a new severity level to make notable events from this search less urgent.

Answer: B

Explanation:

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

NEW QUESTION 30

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.

Answer: D

Explanation:

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

NEW QUESTION 32

What is the default schedule for accelerating ES Datamodels?

- A. 1 minute
- B. 5 minutes
- C. 15 minutes
- D. 1 hour

Answer: B

Explanation:

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

NEW QUESTION 34

.....

Relate Links

100% Pass Your SPLK-3001 Exam with Exambible Prep Materials

<https://www.exambible.com/SPLK-3001-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>