



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

What does the risk framework add to an object (user, server or other type) to indicate increased risk?

- A. An urgency.
- B. A risk profile.
- C. An aggregation.
- D. A numeric score.

Answer: C

Explanation:

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

NEW QUESTION 2

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 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.

Answer: D

Explanation:

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

NEW QUESTION 4

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 5

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 6

An administrator is asked to configure an "Nslookup" adaptive response action, so that it appears as a selectable option in the notable event's action menu when an analyst is working in the Incident Review dashboard. What steps would the administrator take to configure this option?

- A. Configure -> Content Management -> Type: Correlation Search -> Notable -> Nslookup
- B. Configure -> Type: Correlation Search -> Notable -> Recommended Actions -> Nslookup
- C. Configure -> Content Management -> Type: Correlation Search -> Notable -> Next Steps -> Nslookup

D. Configure -> Content Management -> Type: Correlation Search -> Notable -> Recommended Actions -> Nslookup

Answer: D

NEW QUESTION 7

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

Answer: C

Explanation:

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

NEW QUESTION 8

Adaptive response action history is stored in which index?

- A. cim_modactions
- B. modular_history
- C. cim_adaptiveactions
- D. modular_action_history

Answer: A

Explanation:

Reference: <https://docs.splunk.com/Documentation/ES/6.1.0/Install/Indexes>

NEW QUESTION 9

Where is it possible to export content, such as correlation searches, from ES?

- A. Content exporter
- B. Configure -> Content Management
- C. Export content dashboard
- D. Settings Menu -> ES -> Export

Answer: B

Explanation:

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

NEW QUESTION 10

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 10

ES needs to be installed on a search head with which of the following options?

- A. No other apps.
- B. Any other apps installed.
- C. All apps removed except for TA-*
- D. Only default built-in and CIM-compliant apps.

Answer: A

Explanation:

Reference: <https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallEnterpriseSecurity>

NEW QUESTION 11

How is it possible to navigate to the ES graphical Navigation Bar editor?

- A. Configure -> Navigation Menu
- B. Configure -> General -> Navigation
- C. Settings -> User Interface -> Navigation -> Click on "Enterprise Security"
- D. Settings -> User Interface -> Navigation Menus -> Click on "default" next to SplunkEnterpriseSecuritySuite

Answer: B

Explanation:

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Customizemenubar#Restore_the_default_navigation

NEW QUESTION 14

What tools does the Risk Analysis dashboard provide?

- A. High risk threats.
- B. Notable event domains displayed by risk score.
- C. A display of the highest risk assets and identities.
- D. Key indicators showing the highest probability correlation searches in the environment.

Answer: C

Explanation:

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

NEW QUESTION 18

Which of the following actions can improve overall search performance?

- A. Disable indexed real-time search.
- B. Increase priority of all correlation searches.
- C. Reduce the frequency (schedule) of lower-priority correlation searches.
- D. Add notable event suppressions for correlation searches with high numbers of false positives.

Answer: A

NEW QUESTION 23

An administrator wants to ensure that none of the ES indexed data could be compromised through tampering. What feature would satisfy this requirement?

- A. Index consistency.
- B. Data integrity control.
- C. Indexer acknowledgement.
- D. Index access permissions.

Answer: B

Explanation:

Reference: <https://answers.splunk.com/answers/790783/anti-tampering-features-to-protect-splunk-logs-the.html>

NEW QUESTION 27

.....

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/>