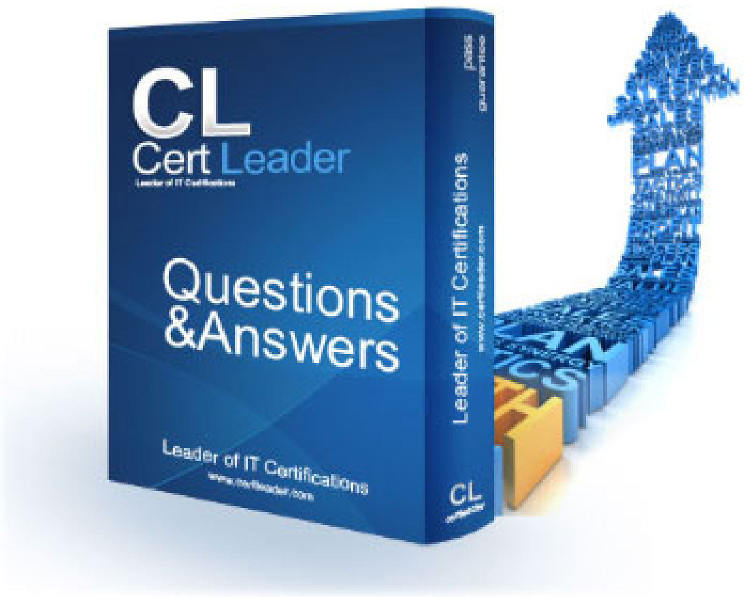
SPLK-3001 Dumps

Splunk Enterprise Security Certified Admin Exam

https://www.certleader.com/SPLK-3001-dumps.html



NEW 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

Answer: D

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

NEW QUESTION 2
Which setting is used in indexes.conf to specify alternate locations for accelerated storage?

A. thawedPath
B. tstatsHomePath
C. summaryHomePath
D. warmToColdScript

Answer: B

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

NEW QUESTION 3
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 4
Which argument to the | tstats command restricts the search to summarized data only?

A. summaries=t
B. summaries=all
C. summariesonly=t
D. summariesonly=all

Answer: C

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

NEW QUESTION 5
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 6
Where is the Add-On Builder available from?

A. GitHub
B. SplunkBase
C. www.splunk.com
D. The ES installation package

Answer: B

Explanation:
Reference: https://docs.splunk.com/Documentation/AddonBuilder/3.0.1/UserGuide/Installation

NEW QUESTION 7
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 8
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 9
A site has a single existing search head which hosts a mix of both CIM and non-CIM compliant applications. All of the applications are mission-critical. The customer wants to carefully control cost, but wants good ES performance. What is the best practice for installing ES?

A. Install ES on the existing search head.
B. Add a new search head and install ES on it.
C. Increase the number of CPUs and amount of memory on the search head, then install ES.
D. Delete the non-CIM-compliant apps from the search head, then install ES.

Answer: B

Explanation:
Reference: https://www.splunk.com/pdfs/technical-briefs/splunk-validated-architectures.pdf

NEW QUESTION 10
Where are attachments to investigations stored?

A. KV Store
B. notable index
C. attachments.csv lookup
D. <splunk_home>/etc/apps/SA-Investigations/default/ui/views/attachments

Answer: A

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

NEW QUESTION 10
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 12
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 17
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 18
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 19
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 22
What is the first step when preparing to install ES?

A. Install ES.
B. Determine the data sources used.
C. Determine the hardware required.
D. Determine the size and scope of installation.

Answer: D

NEW QUESTION 25
......