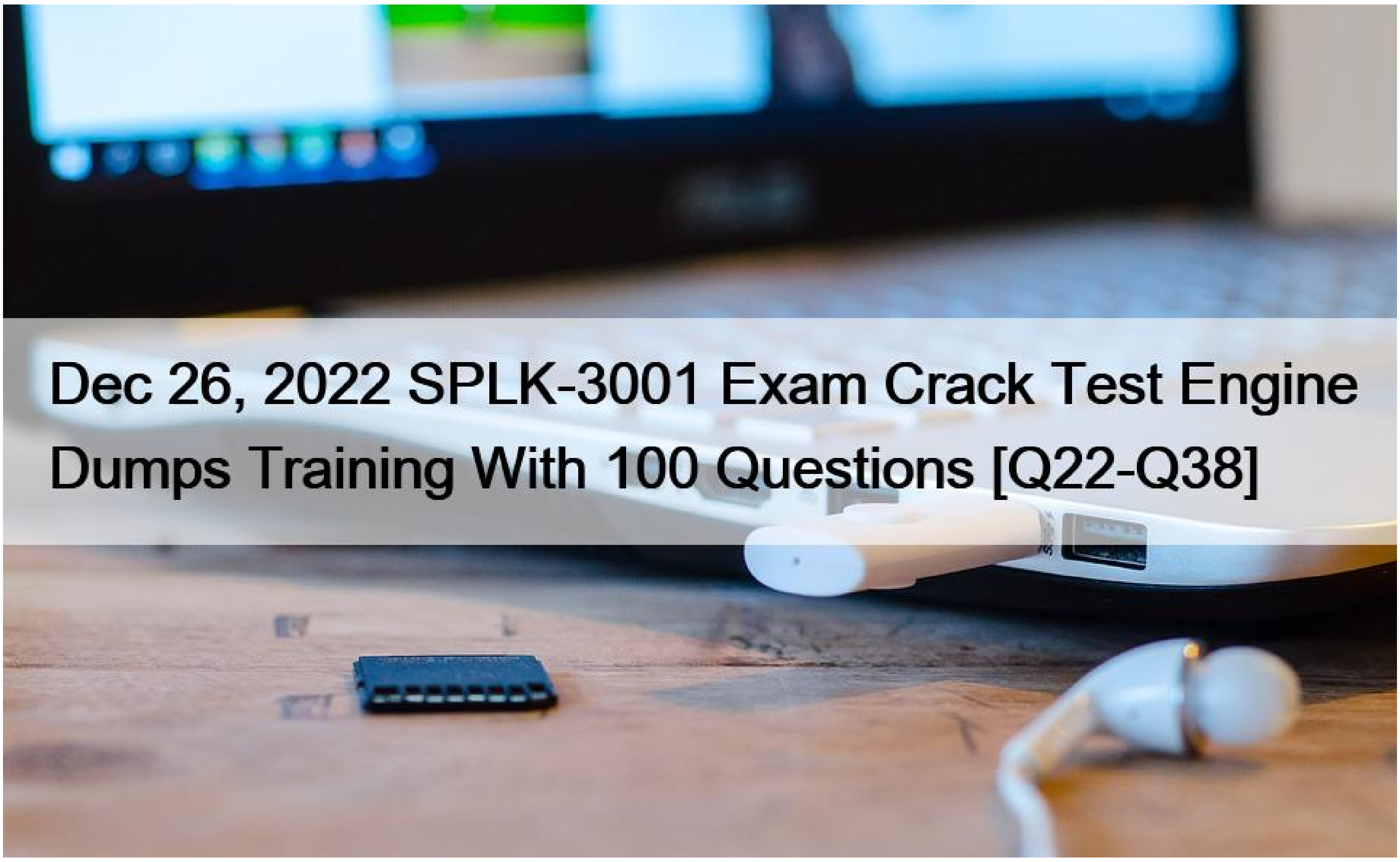
Dec 26, 2022 SPLK-3001 Exam Crack Test Engine Dumps Training With 100 Questions [Q22-Q38



Dec 26, 2022 SPLK-3001 Exam Crack Test Engine Dumps Training With 100 Questions Obtain the SPLK-3001 PDF Dumps Get 100% Outcomes Exam Questions For You To Pass Q22. Where is the Add-On Builder available from?
* GitHub
* SplunkBase
* www.splunk.com
* The ES installation package

Q23. What does the Security Posture dashboard display?
* Active investigations and their status.
* A high-level overview of notable events.
* Current threats being tracked by the SOC.
* A display of the status of security tools.
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

Q24. An administrator wants to ensure that none of the ES indexed data could be compromised through tampering.

What feature would satisfy this requirement?
* Index consistency.

* Data integrity control.
* Indexer acknowledgement.
* Index access permissions.
Explanation/Reference: https://answers.splunk.com/answers/790783/anti-tampering-features-to-protect-splunk-logs- the.html

Q25. Which indexes are searched by default for CIM data models?
* notable and default
* summary and notable
* _internal and summary
* All indexes
Explanation/Reference: https://answers.splunk.com/answers/600354/indexes-searched-by-cim-data-models.html

Q26. Adaptive response action history is stored in which index?
* cim_modactions
* modular_history
* cim_adaptiveactions
* modular_action_history

Q27. Glass tables can display static images and text, the results of ad-hoc searches, and which of the following objects?
* Lookup searches.
* Summarized data.
* Security metrics.
* Metrics store searches.
Reference:

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

Q28. The option to create a Short ID for a notable event is located where?
* The Additional Fields.
* The Event Details.
* The Contributing Events.
* The Description.

Q29. Which of the following actions may be necessary before installing ES?
* Redirect distributed search connections.
* Purge KV Store.
* Add additional indexers.
* Add additional forwarders.

Q30. An administrator is asked to configure an &#8220;Nslookup&#8221; adaptive response action, so that it appears as a selectable option in the notable event&#8217;s action menu when an analyst is working in the Incident Review dashboard. What steps would the administrator take to configure this option?
* Configure -> Content Management -> Type: Correlation Search -> Notable -> Nslookup
* Configure -> Type: Correlation Search -> Notable -> Recommended Actions -> Nslookup
* Configure -> Content Management -> Type: Correlation Search -> Notable -> Next Steps -> Nslookup
* Configure -> Content Management -> Type: Correlation Search -> Notable -> Recommended Actions -> Nslookup

Q31. Which correlation search feature is used to throttle the creation of notable events?
* Schedule priority.
* Window interval.

* Window duration.
* Schedule windows.
Reference:

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

Q32. Which of the following actions would not reduce the number of false positives from a correlation search?
* Reducing the severity.
* Removing throttling fields.
* Increasing the throttling window.
* Increasing threshold sensitivity.

Q33. What is the maximum recommended volume of indexing per day, per indexer, for a non-cloud (on-prem) ES deployment?
* 50 GB
* 100 GB
* 300 GB
* 500 MB
Reference:

https://docs.splunk.com/Documentation/ITSI/4.4.2/Install/Plan

Q34. Which of the following is a Web Intelligence dashboard?
* Network Center
* Endpoint Center
* HTTP Category Analysis
* stream :http Protocol dashboard

Q35. Both &#8220;Recommended Actions&#8221; and &#8220;Adaptive Response Actions&#8221; use adaptive response. How do they differ?
* Recommended Actions show a textual description to an analyst, Adaptive Response Actions show them encoded.
* Recommended Actions show a list of Adaptive Responses to an analyst, Adaptive Response Actions run them automatically.
* Recommended Actions show a list of Adaptive Responses that have already been run, Adaptive Response Actions run them automatically.
* Recommended Actions show a list of Adaptive Resposes to an analyst, Adaptive Response Actions run manually with analyst intervention.
Reference:

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

Q36. Which of the following is a way to test for a property normalized data model?
* Use Audit -> Normalization Audit and check the Errors panel.
* Run a | datamodelsearch, compare results to the CIM documentation for the datamodel.
* Run a | loadjobsearch, look at tag values and compare them to known tags based on the encoding.
* Run a | datamodelsearch and compare the results to the list of data models in the ES normalization guide.
Explanation/Reference: https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizedataatsearchtime

Q37. 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?
* $SPLUNK_HOME/etc/system/local/
* $SPLUNK_HOME/var/run/searchpeers/

* $SPLUNK_HOME/etc/shcluster/apps
* $SPLUNK_HOME/etc/master-apps/

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

Q38. The Remote Access panel within the User Activity dashboard is not populating with the most recent hour of data. What data model should be checked for potential errors such as skipped searches?

* Web
* Risk
* Performance
* Authentication

SPLK-3001 Exam Dumps Contains FREE Real Quesions from the Actual Exam:
https://www.topexamcollection.com/SPLK-3001-vce-collection.html]