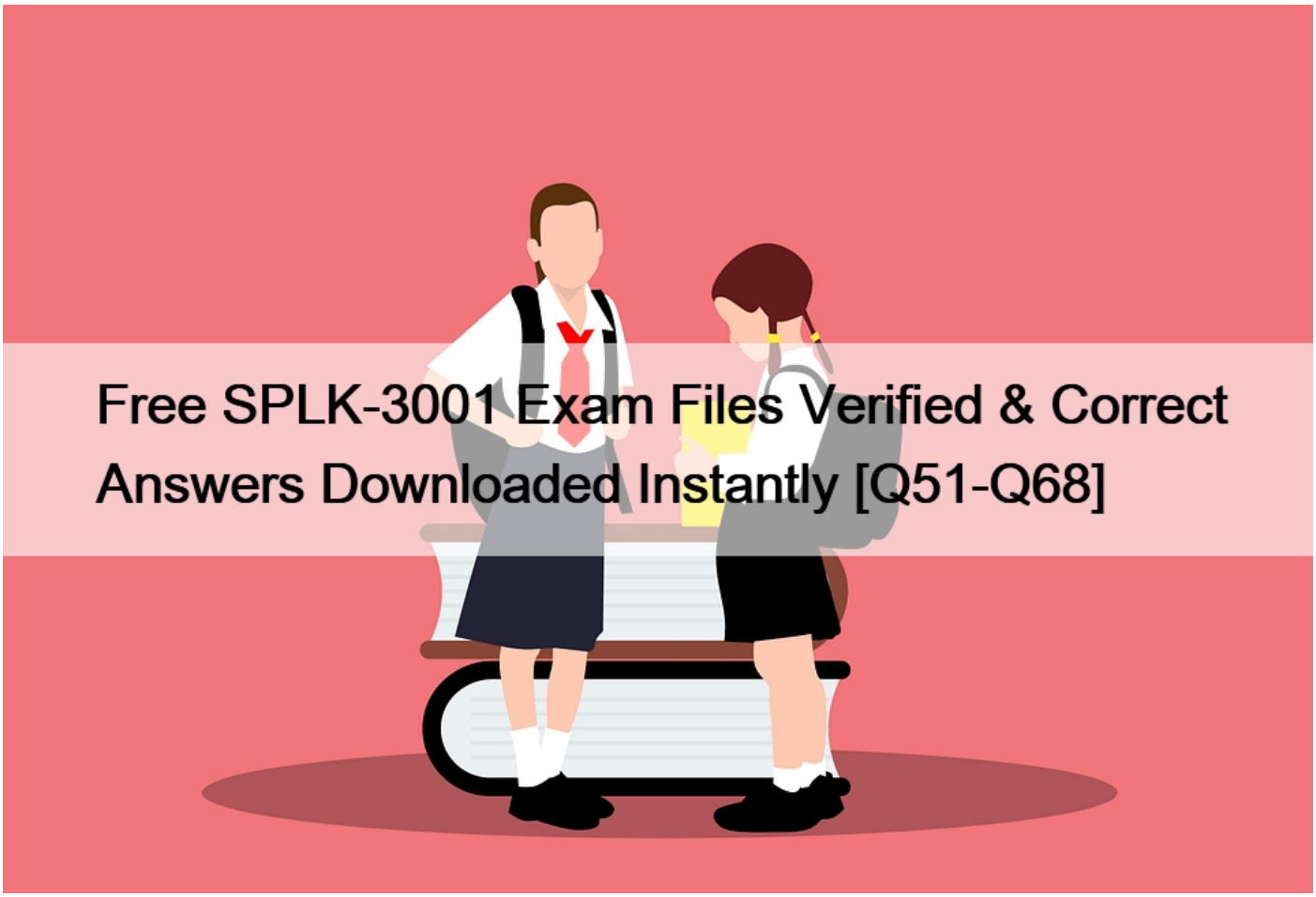
Free SPLK-3001 Exam Files Verified & Correct Answers Downloaded Instantly [Q51-Q68



Free SPLK-3001 Exam Files Verified & Correct Answers Downloaded Instantly Instant Download SPLK-3001 Dumps Q&As Provide PDF&Test Engine

What are the Prerequisites for SPLK-3001?

You should have a thorough knowledge of data engineering and analysis.You should have at least 4 years of experience working with Splunk. These years have to be consecutive.You should be a graduate of an accredited university (with a computer science undergraduate degree or higher)The experienced candidate must have worked on multiple solutions in Splunk, Hadoop, Storm and Big Data.Should be a certified software engineer (for experience only).

NO.51 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 Reference:

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

NO.52 Which two fields combine to create the Urgency of a notable event?
* Priority and Severity.
* Priority and Criticality.
* Criticality and Severity.
* Precedence and Time.

NO.53 Where should an ES search head be installed?
* On a Splunk server with top level visibility.
* On any Splunk server.
* On a server with a new install of Splunk.
* On a Splunk server running Splunk DB Connect.

NO.54 What role should be assigned to a security team member who will be taking ownership of notable events in the incident review dashboard?
* ess_user
* ess_admin
* ess_analyst
* ess_reviewer

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

NO.55 Which of the following actions can improve overall search performance?
* Disable indexed real-time search.
* Increase priority of all correlation searches.
* Reduce the frequency (schedule) of lower-priority correlation searches.
* Add notable event suppressions for correlation searches with high numbers of false positives.

NO.56 Which of the following are the default ports that must be configured for Splunk Enterprise Security to function?
* SplunkWeb (8000), Splunk Management (8089), KV Store (8191)
* SplunkWeb (8068), Splunk Management (8089), KV Store (8000)
* SplunkWeb (8390), Splunk Management (8323), KV Store (8672)
* SplunkWeb (8043), Splunk Management (8088), KV Store (8191)

https://docs.splunk.com/Documentation/Splunk/8.1.2/Security/SecureSplunkonyournetwork

NO.57 Which of the following actions may be necessary before installing ES?
* Redirect distributed search connections.
* Purge KV Store.
* Add additional indexers.
* Add additional forwarders.

NO.58 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 | datamodel search, compare results to the CIM documentation for the datamodel.
* Run a | loadjob search, look at tag values and compare them to known tags based on the encoding.
* Run a | datamodel search and compare the results to the list of data models in the ES normalization guide.

NO.59 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?
* Install ES on the existing search head.
* Add a new search head and install ES on it.
* Increase the number of CPUs and amount of memory on the search head, then install ES.
* Delete the non-CIM-compliant apps from the search head, then install ES.

NO.60 Enterprise Security’s dashboards primarily pull data from what type of knowledge object?
* Tstats
* KV Store
* Data models
* Dynamic lookups

NO.61 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?
* Install ES on the existing search head.
* Add a new search head and install ES on it.
* Increase the number of CPUs and amount of memory on the search head, then install ES.
* Delete the non-CIM-compliant apps from the search head, then install ES.

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

NO.62 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.
* Index access permissions.
* Data integrity control.
* Indexer acknowledgement.

NO.63 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

NO.64 A security manager has been working with the executive team en long-range security goals. A primary goal for the team Is to Improve managing user risk in the organization. Which of the following ES features can help identify users accessing inappropriate web sites?
* Configuring the identities lookup with user details to enrich notable event Information for forensic analysis.
* Make sure the Authentication data model contains up-to-date events and is properly accelerated.
* Configuring user and website watchlists so the User Activity dashboard will highlight unwanted user actions.
* Use the Access Anomalies dashboard to identify unusual protocols being used to access corporate sites.

NO.65 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.

Reference:

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

NO.66 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

NO.67 Which correlation search feature is used to throttle the creation of notable events?

* Schedule priority.
* Window interval.
* Window duration.
* Schedule windows.

NO.68 Which settings indicated that the correlation search will be executed as new events are indexed?

* Always-On
* Real-Time
* Scheduled
* Continuous

Reference:

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

How can you achieve a Splunk SPLK-3001?

It won't be difficult to achieve Splunk SPLK-3001 certification now that the test has been revised and is less lengthy than before. However, there are still certain preparations that need to be made before attempting to take the test. To qualify for this qualification, you should first be a certified Splunk administrator. If a candidate has knowledge and skills that are required to pass Splunk SPLK-3001 Exam and fully prepared with **Splunk SPLK-3001 Dumps** then he should take this Splunk SPLK-3001 exam.
Then, you must prepare yourself to pass the tests by practicing and preparing for all the questions and scenarios. Reading various

reviews will give you a better understanding of what is expected from you in the test. Moreover, experience counts too, so it will be beneficial to have worked with Splunk previously for a period of time.

There you can get information about the Difficulty in writing the Splunk SPLK-3001 Exam

There are great deals of problems a Possibility faced when Potential consumers begin preparing yourself for the Splunk SPLK-3001 Exam. If a possibility plans to prepare his for the Splunk SPLK-3001 Examination with no issue along with in a similar means obtain superior premium quality in the. After that they call for to select the best Splunk SPLK-3001 unloads real issues approach. There are lots of web net sites that are supplying one of the most existing Splunk SPLK-3001 Examination problems together with responses yet these concerns are not validated by Microsoft identified professionals which's why various are fallen short in their simply preliminary effort. ValidBraindumps is the straight-out outstanding platform which uses the possibility with the essential Splunk SPLK-3001 concerns that will most absolutely help him to pass the Splunk SPLK-3001 on the very truly very first time. The possibility will certainly most absolutely not need to take the Splunk SPLK-3001 exam 2 times as a result of the reality that with the help of the **Splunk SPLK-3001 Dumps** Possibility will definitely have every important item called for to pass the Splunk SPLK-3001 Test. We are supplying among the most about day together with authentic questions which is the variable that this is the one that he requires to profit from in addition to there are no chances to stop working when a prospect will most definitely have reputable mind tosses out from ValidBraindumps. We have the assurance that the problems that we have will definitely be the ones that will definitely pass possibility in the Splunk SPLK-3001 Examination in the as a matter of fact incredibly initial campaign.

Exam Valid Dumps with Instant Download Free Updates: https://www.validbraindumps.com/SPLK-3001-exam-prep.html]