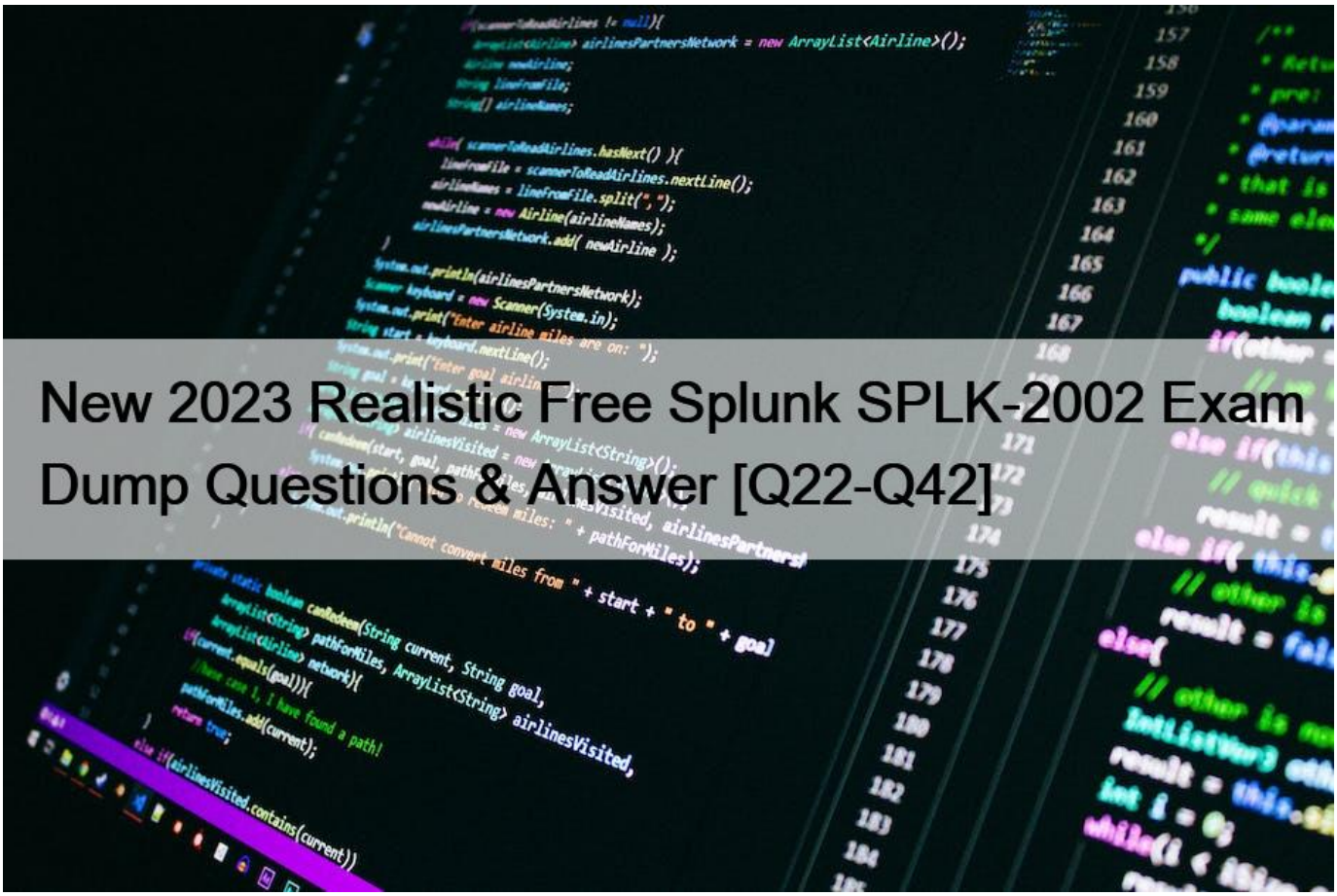
# New 2023 Realistic Free Splunk SPLK-2002 Exam Dump Questions & Answer [Q22-Q42




New 2023 Realistic Free Splunk SPLK-2002 Exam Dump Questions and Answer
SPLK-2002 Practice Test Engine: Try These 92 Exam Questions

**NEW QUESTION 22**

Which of the following are true statements about Splunk indexer clustering?
* All peer nodes must run exactly the same Splunk version.
* The master node must run the same or a later Splunk version than search heads.
* The peer nodes must run the same or a later Splunk version than the master node.
* The search head must run the same or a later Splunk version than the peer nodes.
Explanation/Reference: https://answers.splunk.com/answers/760348/search-head-version-compatibility.html

**NEW QUESTION 23**

Splunk Enterprise platform instrumentation refers to data that the Splunk Enterprise deployment logs in the

_introspectionindex. Which of the following logs are included in this index? (Select all that apply.)

* audit.log
* metrics.log
* disk_objects.log
* resource_usage.log

Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Troubleshooting/

Abouttheplatforminstrumentationframework

**NEW QUESTION 24**

Which of the following are true statements about Splunk indexer clustering?
* All peer nodes must run exactly the same Splunk version.
* The master node must run the same or a later Splunk version than search heads.
* The peer nodes must run the same or a later Splunk version than the master node.
* The search head must run the same or a later Splunk version than the peer nodes.

**NEW QUESTION 25**

To reduce the captain’s work load in a search head cluster, what setting will prevent scheduled searches from running on the captain?
* adhoc_searchhead = true(on all members)
* adhoc_searchhead = true(on the current captain)
* captain_is_adhoc_searchhead = true(on all members)
* captain_is_adhoc_searchhead = true(on the current captain)

Explanation/Reference:

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/Adhocclustermember

**NEW QUESTION 26**

When using the props.conf LINE_BREAKER attribute to delimit multi-line events, the SHOULD_LINEMERGE attribute should be set to what?
* Auto
* None
* True
* False

**NEW QUESTION 27**

When adding or decommissioning a member from a Search Head Cluster (SHC), what is the proper order of operations?
* 1. Delete Splunk Enterprise, if it exists.

2. Install and initialize the instance.

3. Join the SHC.
* 1. Install and initialize the instance.

2. Delete Splunk Enterprise, if it exists.

3. Join the SHC.

* 1. Initialize cluster rebalance operation.

2. Remove master node from cluster.

3. Trigger replication.
* 1. Trigger replication.

2. Remove master node from cluster.

3. Initialize cluster rebalance operation.
Explanation

**NEW QUESTION 28**

When troubleshooting monitor inputs, which command checks the status of the tailed files?

splunk cmd btool inputs list | tail
* splunk cmd btool check inputs layer
* curl https://serverhost:8089/services/admin/inputstatus/
* TailingProcessor:FileStatus

curl https://serverhost:8089/services/admin/inputstatus/
* TailingProcessor:Tailstatus
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/
Troubleshoottheinputprocess#Troubleshoot_your_tailed_files

**NEW QUESTION 29**

Which tool(s) can be leveraged to diagnose connection problems between an indexer and forwarder? (Select all that apply.)
* telnet
* tcpdump
* splunk btool
* splunk btprobe

**NEW QUESTION 30**

In search head clustering, which of the following methods can you use to transfer captaincy to a different member? (Select all that apply.)
* Use the Monitoring Console.
* Use the Search Head Clustering settings menu from Splunk Web on any member.
* Run the splunk transfer shcluster-captaincommand from the current captain.
* Run the splunk transfer shcluster-captaincommand from the member you would like to become the captain.
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/Transfercaptain

**NEW QUESTION 31**

To reduce the captain’s work load in a search head cluster, what setting will prevent scheduled searches from running on the captain?
* adhoc_searchhead = true (on all members)
* adhoc_searchhead = true (on the current captain)

* captain_is_adhoc_searchhead = true (on all members)
* captain_is_adhoc_searchhead = true (on the current captain)

**NEW QUESTION 32**

What log file would you search to verify if you suspect there is a problem interpreting a regular expression in a

monitor stanza?
* btool.log
* metrics.log
* splunkd.log
* tailing_processor.log

Explanation/Reference: https://answers.splunk.com/answers/479312/how-to-edit-inputsconf-to-monitor-multiple-files-w-

1.html

**NEW QUESTION 33**

Which Splunk tool offers a health check for administrators to evaluate the health of their Splunk deployment?
* btool
* DiagGen
* SPL Clinic
* Monitoring Console

**NEW QUESTION 34**

Configurations from the deployer are merged into which location on the search head cluster member?
* SPLUNK_HOME/etc/system/local
* SPLUNK_HOME/etc/apps/APP_HOME/local
* SPLUNK_HOME/etc/apps/search/default
* SPLUNK_HOME/etc/apps/APP_HOME/default

Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/DistSearch/ PropagateSHCconfigurationchanges

**NEW QUESTION 35**

The frequency in which a deployment client contacts the deployment server is controlled by what?
* polling_interval attribute in outputs.conf
* phoneHomeIntervalInSecs attribute in outputs.conf
* polling_interval attribute in deploymentclient.conf
* phoneHomeIntervalInSecs attribute in deploymentclient.conf

**NEW QUESTION 36**

Which of the following can a Splunk diag contain?
* Search history, Splunk users and their roles, running processes, indexed data
* Server specs, current open connections, internal Splunk log files, index listings
* KV store listings, internal Splunk log files, search peer bundles listings, indexed data
* Splunk platform configuration details, Splunk users and their roles, current open connections, index listings

**NEW QUESTION 37**

Which of the following will cause the greatest reduction in disk size requirements for a cluster of N indexers running Splunk Enterprise Security?
* Setting the cluster search factor to N-1.
* Increasing the number of buckets per index.
* Decreasing the data model acceleration range.
* Setting the cluster replication factor to N-1.

**NEW QUESTION 38**

Search dashboards in the Monitoring Console indicate that the distributed deployment is approaching its

capacity. Which of the following options will provide the most search performance improvement?
* Replace the indexer storage to solid state drives (SSD).
* Add more search heads and redistribute users based on the search type.
* Look for slow searches and reschedule them to run during an off-peak time.
* Add more search peers and make sure forwarders distribute data evenly across all indexers.

**NEW QUESTION 39**

Which of the following clarification steps should be taken if apps are not appearing on a deployment client?

(Select all that apply.)
* Check serverclass.confof the deployment server.
* Check deploymentclient.confof the deployment client.
* Check the content of SPLUNK_HOME/etc/appsof the deployment server.
* Search for relevant events in splunkd.logof the deployment server.

Explanation/Reference: https://answers.splunk.com/answers/177021/why-is-deployment-client-not-picking-up-changes-

to.html

**NEW QUESTION 40**

A new Splunk customer is using syslog to collect data from their network devices on port 514. What is the best practice for ingesting this data into Splunk?
* Configure syslog to send the data to multiple Splunk indexers.
* Use a Splunk indexer to collect a network input on port 514 directly.
* Use a Splunk forwarder to collect the input on port 514 and forward the data.
* Configure syslog to write logs and use a Splunk forwarder to collect the logs.

Explanation/Reference: https://docs.splunk.com/Documentation/SplunkCloud/8.0.0/Data/Monitornetworkports

**NEW QUESTION 41**

Splunk Enterprise platform instrumentation refers to data that the Splunk Enterprise deployment logs in the

_introspection index. Which of the following logs are included in this index? (Select all that apply.)
* audit.log
* metrics.log
* disk_objects.log
* resource_usage.log

**NEW QUESTION 42**

Which of the following is true regarding Splunk Enterprise performance? (Select all that apply.)
* Adding search peers increases the maximum size of search results.
* Adding RAM to an existing search heads provides additional search capacity.
* Adding search peers increases the search throughput as search load increases.
* Adding search heads provides additional CPU cores to run more concurrent searches.

Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Capacity/HowsavedsearchesaffectSplunkEnterpriseperformance