

Updated Apr-2023 Exam SPLK-2002 Dumps - Pass Your Certification Exam [Q30-Q45]



Updated Apr-2023 Exam SPLK-2002 Dumps - Pass Your Certification Exam
Latest Real Splunk SPLK-2002 Exam Dumps Questions

Splunk SPLK-2002 : Splunk Enterprise Certified Architect Exam Certified Professional salary
The average salary of a Splunk SPLK-2002 : Splunk Enterprise Certified Architect expert in:
- England - 65,632 POUND- India - 15,42,327 INR- United State - 100,247 USD- Europe - 60,347 EURO **NEW**
QUESTION 30

Which server.confattribute should be added to the master node's server.conf file when

decommissioning a site in an indexer cluster?

- * site_mappings
- * available_sites
- * site_search_factor
- * site_replication_factor

Explanation/Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.2/Indexer/Decommissionasite>

NEW QUESTION 31

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

Explanation/Reference: <https://answers.splunk.com/answers/6926/how-to-keep-data-together-as-one-event.html>

NEW QUESTION 32

What is the logical first step when starting a deployment plan?

- * Inventory the currently deployed logging infrastructure.
- * Determine what apps and use cases will be implemented.
- * Gather statistics on the expected adoption of Splunk for sizing.
- * Collect the initial requirements for the deployment from all stakeholders.

NEW QUESTION 33

Which search will show all deployment client messages from the client (UF)?

- * `index=_audit component=DC* host=<ds> | stats count by message`
- * `index=_audit component=DC* host=<uf> | stats count by message`
- * `index=_internal component= DC* host=<uf> | stats count by message`
- * `index=_internal component=DS* host=<ds> | stats count by message`

NEW QUESTION 34

Of the following types of files within an index bucket, which file type may consume the most disk?

- * Inverted index (.tsidx)
- * Metadata (.data)
- * Bloom filter
- * Rawdata

NEW QUESTION 35

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

(Select all that apply.)

- * Check serverclass.conf of the deployment server.
- * Check deploymentclient.conf of the deployment client.
- * Check the content of SPLUNK_HOME/etc/apps of the deployment server.
- * Search for relevant events in splunkd.log of the deployment server.

NEW QUESTION 36

What does setting site=site0 on all Search Head Cluster members do in a multi-site indexer cluster?

- * Disables search site affinity.
- * Sets all members to dynamic captaincy.
- * Enables multisite search artifact replication.

- * Enables automatic search site affinity discovery.

NEW QUESTION 37

A customer plans to ingest 600 GB of data per day into Splunk. They will have six concurrent users, and they also want high data availability and high search performance. The customer is concerned about cost and wants to spend the minimum amount on the hardware for Splunk. How many indexers are recommended for this deployment?

- * Two indexers not in a cluster, assuming users run many long searches.
- * Three indexers not in a cluster, assuming a long data retention period.
- * Two indexers clustered, assuming high availability is the greatest priority.
- * Two indexers clustered, assuming a high volume of saved/scheduled searches.

Explanation/Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.2/Capacity/Summaryofperformancerecommendations>

NEW QUESTION 38

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 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.conf` of the deployment server.
- * Check `deploymentclient.conf` of the deployment client.
- * Check the content of `SPLUNK_HOME/etc/apps` of the deployment server.
- * Search for relevant events in `splunkd.log` of the deployment server.

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

NEW QUESTION 40

Which of the following describe migration from single-site to multisite index replication?

- * A master node is required at each site.
- * Multisite policies apply to new data only.
- * Single-site buckets instantly receive the multisite policies.
- * Multisite total values should not exceed any single-site factors.

Explanation/Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.2/Indexer/Migratetomultisite>

NEW QUESTION 41

Stakeholders have identified high availability for searchable data as their top priority. Which of the following best addresses this

requirement?

- * Increasing the search factor in the cluster.
- * Increasing the replication factor in the cluster.
- * Increasing the number of search heads in the cluster.
- * Increasing the number of CPUs on the indexers in the cluster.

Explanation

<https://docs.splunk.com/Documentation/Splunk/7.3.2/DistSearch/SHCArchitecture>

NEW QUESTION 42

Stakeholders have identified high availability for searchable data as their top priority. Which of the following best addresses this requirement?

- * Increasing the search factor in the cluster.
- * Increasing the replication factor in the cluster.
- * Increasing the number of search heads in the cluster.
- * Increasing the number of CPUs on the indexers in the cluster.

Explanation/Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.2/DistSearch/SHCArchitecture>

NEW QUESTION 43

Which command is used for thawing the archive bucket?

- * Splunk collect
- * Splunk convert
- * Splunk rebuild
- * Splunk dbinspect

Explanation/Reference: <https://answers.splunk.com/answers/337025/after-frozen-data-restore-thawed-data-not-working.html>

NEW QUESTION 44

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.

NEW QUESTION 45

When Splunk indexes data in a non clustered environment, what kind of files does it create by default?

- * Index and .tsidx files.
- * Rawdata and index files.
- * Compressed and .tsidx files.
- * Compressed and meta data files.

SPLK-2002 Dumps To Pass Splunk Enterprise Certified Architect Exam in One Day:

<https://www.examslabs.com/Splunk/Splunk-Enterprise-Certified-Architect/best-SPLK-2002-exam-dumps.html>