

SPLK-2002 Dumps

Splunk Enterprise Certified Architect

<https://www.certleader.com/SPLK-2002-dumps.html>



NEW QUESTION 1

When using the props.conf LINE_BREAKER attribute to delimit multi-line events, the SHOULD_LINEMERGE attribute should be set to what?

- A. Auto
- B. None
- C. True
- D. False

Answer: C

NEW QUESTION 2

Which of the following should be included in a deployment plan?

- A. Business continuity and disaster recovery plans.
- B. Current logging details and data source inventory.
- C. Current and future topology diagrams of the IT environment.
- D. A comprehensive list of stakeholders, either direct or indirect.

Answer: D

NEW QUESTION 3

In a four site indexer cluster, which configuration stores two searchable copies at the origin site, one searchable copy at site2, and a total of four searchable copies?

- A. site_search_factor = origin:2, site1:2, total:4
- B. site_search_factor = origin:2, site2:1, total:4
- C. site_replication_factor = origin:2, site1:2, total:4
- D. site_replication_factor = origin:2, site2:1, total:4

Answer: D

NEW QUESTION 4

Which component in the splunkd.log will log information related to bad event breaking?

- A. Audittrail
- B. EventBreaking
- C. IndexingPipeline
- D. AggregatorMiningProcessor

Answer: D

NEW QUESTION 5

The frequency in which a deployment client contacts the deployment server is controlled by what?

- A. polling_interval attribute in outputs.conf
- B. phoneHomeIntervalInSecs attribute in outputs.conf
- C. polling_interval attribute in deploymentclient.conf
- D. phoneHomeIntervalInSecs attribute in deploymentclient.conf

Answer: D

NEW QUESTION 6

To activate replication for an index in an indexer cluster, what attribute must be configured in indexes.conf on all peer nodes?

- A. repFactor = 0
- B. replicate = 0
- C. repFactor = auto
- D. replicate = auto

Answer: C

NEW QUESTION 7

Which of the following are true statements about Splunk indexer clustering?

- A. All peer nodes must run exactly the same Splunk version.
- B. The master node must run the same or a later Splunk version than search heads.
- C. The peer nodes must run the same or a later Splunk version than the master node.
- D. The search head must run the same or a later Splunk version than the peer nodes.

Answer: B

NEW QUESTION 8

Which of the following is a good practice for a search head cluster deployer?

- A. The deployer only distributes configurations to search head cluster members when they “phone home”.
- B. The deployer must be used to distribute non-replicable configurations to search head cluster members.
- C. The deployer must distribute configurations to search head cluster members to be valid configurations.
- D. The deployer only distributes configurations to search head cluster members with splunk apply shcluster-bundle.

Answer: A

NEW QUESTION 9

Which search head cluster component is responsible for pushing knowledge bundles to search peers, replicating configuration changes to search head cluster members, and scheduling jobs across the search head cluster?

- A. Master
- B. Captain
- C. Deployer
- D. Deployment server

Answer: B

NEW QUESTION 10

In the deployment planning process, when should a person identify who gets to see network data?

- A. Deployment schedule
- B. Topology diagramming
- C. Data source inventory
- D. Data policy definition

Answer: C

NEW QUESTION 10

A Splunk instance has the following settings in SPLUNK_HOME/etc/system/local/server.conf:

```
[clustering] mode = master
replication_factor = 2
pass4SymmKey = password123
```

Which of the following statements describe this Splunk instance?
(Select all that apply.)

- A. This is a multi-site cluster.
- B. This cluster's search factor is 2.
- C. This Splunk instance needs to be restarted.
- D. This instance is missing the master_uri attribute.

Answer: AC

NEW QUESTION 15

Which of the following is a way to exclude search artifacts when creating a diag?

- A. SPLUNK_HOME/bin/splunk diag --exclude
- B. SPLUNK_HOME/bin/splunk diag --debug --refresh
- C. SPLUNK_HOME/bin/splunk diag --disable=dispatch
- D. SPLUNK_HOME/bin/splunk diag --filter-searchstrings

Answer: A

NEW QUESTION 20

Which of the following statements describe licensing in a clustered Splunk deployment? (Select all that apply.)

- A. Free licenses do not support clustering.
- B. Replicated data does not count against licensing.
- C. Each cluster member requires its own clustering license.
- D. Cluster members must share the same license pool and license master.

Answer: BD

NEW QUESTION 21

Which server.conf attribute should be added to the master node's server.conf file when decommissioning a site in an indexer cluster?

- A. site_mappings
- B. available_sites
- C. site_search_factor
- D. site_replication_factor

Answer: A

NEW QUESTION 23

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

- A. splunk cmd btool inputs list | tail
- B. splunk cmd btool check inputs layer
- C. curl https://serverhost:8089/services/admin/inputstatus/TailingProcessor:FileStatus
- D. curl https://serverhost:8089/services/admin/inputstatus/TailingProcessor:Tailstatus

Answer: C

NEW QUESTION 27

Splunk configuration parameter settings can differ between multiple .conf files of the same name contained within different apps. Which of the following directories has the highest precedence?

- A. System local directory.
- B. System default directory.
- C. App local directories, in ASCII order.
- D. App default directories, in ASCII order.

Answer: A

NEW QUESTION 29

Which of the following is an indexer clustering requirement?

- A. Must use shared storage.
- B. Must reside on a dedicated rack.
- C. Must have at least three members.
- D. Must share the same license pool.

Answer: D

NEW QUESTION 30

What is the algorithm used to determine captaincy in a Splunk search head cluster?

- A. Raft distributed consensus.
- B. Rapt distributed consensus.
- C. Rift distributed consensus.
- D. Round-robin distribution consensus.

Answer: A

NEW QUESTION 32

When Splunk is installed, where are the internal indexes stored by default?

- A. SPLUNK_HOME/bin
- B. SPLUNK_HOME/var/lib
- C. SPLUNK_HOME/var/run
- D. SPLUNK_HOME/etc/system/default

Answer: B

NEW QUESTION 36

Which of the following tasks should the architect perform when building a deployment plan? (Select all that apply.)

- A. Use case checklist.
- B. Install Splunk apps.
- C. Inventory data sources.
- D. Review network topology.

Answer: D

NEW QUESTION 37

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SPLK-2002 Exam with Our Prep Materials Via below:

<https://www.certleader.com/SPLK-2002-dumps.html>