Splunk Enterprise Certified Architect

1. Which of the following will cause the greatest reduction in disk size requirements for a cluster of N indexers running Splunk Enterprise Security?

A. Setting the cluster search factor to N-1.

B. Increasing the number of buckets per index.

C. Decreasing the data model acceleration range.

D. Setting the cluster replication factor to N-1.

Answer(s): D

---

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

A. Increasing the search factor in the cluster.

B. Increasing the replication factor in the cluster.

C. Increasing the number of search heads in the cluster.

D. Increasing the number of CPUs on the indexers in the cluster.

Answer(s): B

---

3. 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?

A. Replace the indexer storage to solid state drives (SSD).

B. Add more search heads and redistribute users based on the search type.

C. Look for slow searches and reschedule them to run during an off-peak time.

D. Add more search peers and make sure forwarders distribute data evenly across all indexers.

Answer(s): C

---

4. A Splunk architect has inherited the Splunk deployment at Buttercup Games and end users are complaining that the events are inconsistently formatted for a web sourcetype. Further investigation reveals that not all web logs flow through the same infrastructure: some of the data goes through heavy forwarders and some of the forwarders are managed by another department. Which of the following items might be the cause for this issue?

A. The search head may have different configurations than the indexers.

B. The data inputs are not properly configured across all the forwarders.

C. The indexers may have different configurations than the heavy forwarders.

D. The forwarders managed by the other department are an older version than the rest.

Answer(s): D

---

5. A customer has installed a 500GB Enterprise license. They also purchased and installed a 300GB, no enforcement license on the same license master. How much data can the customer ingest before search is locked out?

A. 300GB. After this limit, search is locked out.

B. 500G After this limit, search is locked out.

C. 800GB. After this limit, search is locked out.

D. Search is not locked out. Violations are still recorded.

Answer(s): D

6. What does the deployer do in a Search Head Cluster (SHC)? (Select all that apply.)

A. Distributes apps to SHC members.

B. Bootstraps a clean Splunk install for a SHC.

C. Distributes non-search related and manual configuration file changes.

D. Distributes runtime knowledge object changes made by users across the SHC.

Answer(s): A

---

7. 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(s): C

---

8. 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(s): D

9. A multi-site indexer cluster can be configured using which of the following? (Select all that apply.)

- [ ] A. Via Splunk Web.
- [ ] B. Directly edit SPLUNK_HOME/etc/system/local/server.conf
- [ ] C. Run a splunk edit cluster-config command from the CLI.
- [ ] D. Directly edit SPLUNK_HOME/etc/system/default/server.conf

Answer(s): A B

---

10. Which index-time props.conf attributes impact indexing performance? (Select all that apply.)

- [ ] A. REPORT
- [ ] B. LINE_BREAKER
- [ ] C. ANNOTATE_PUNCT
- [ ] D. SHOULD_LINEMERGE

Answer(s): B D

---

11. Which of the following are client filters available in serverclass.conf? (Select all that apply.)

- [ ] A. DNS name.
- [ ] B. IP address.
- [ ] C. Splunk server role.
- [ ] D. Platform (machine type).

Answer(s): A B

---

12. What log file would you search to verify if you suspect there is a problem interpreting a regular expression in a monitor stanza?

A. btool.log

B. metrics.log

C. splunkd.log

D. tailing_processor.log

Answer(s): C

---

13. Which Splunk tool offers a health check for administrators to evaluate the health of their Splunk deployment?

A. btool

B. DiagGen

C. SPL Clinic

D. Monitoring Console

Answer(s): D

---

14. 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(s): D

---

15. Which of the following is true regarding Splunk Enterprise performance? (Select all that apply.)

- ☐ A. Adding search peers increases the maximum size of search results.
- ☐ B. Adding RAM to an existing search heads provides additional search capacity.
- ☐ C. Adding search peers increases the search throughput as search load increases.
- ☐ D. Adding search heads provides additional CPU cores to run more concurrent searches.

Answer(s): B D

---

16. Which Splunk Enterprise offering has its own license?

A. Splunk Cloud Forwarder

B. Splunk Heavy Forwarder

C. Splunk Universal Forwarder

D. Splunk Forwarder Management

Answer(s): C

---

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

A. Audittrail

B. EventBreaking

C. IndexingPipeline

D. AggregatorMiningProcessor

Answer(s): D

---

18. Which Splunk server role regulates the functioning of indexer cluster?

A. Indexer

B. Deployer

C. Master Node

D. Monitoring Console

Answer(s): C

---

19. When adding or rejoining a member to a search head cluster, the following error is displayed:
Error pulling configurations from the search head cluster captain; consider performing a destructive configuration resync on this search head cluster member.
What corrective action should be taken?

A. Restart the search head.

B. Run the splunk apply shcluster-bundle command from the deployer.

C. Run the clean raft command on all members of the search head cluster.

D. Run the splunk resync shcluster-replicated-config command on this member.

Answer(s): B

---

20. Which of the following commands is used to clear the KV store?

A. splunk clean kvstore

B. splunk clear kvstore

C. splunk delete kvstore

D. splunk reinitialize kvstore

Answer(s): A
