# Splunk Certified Enterprise Admin - Advanced MCQs

1. In an indexer cluster, what is the purpose of a search head?

A. To collect logs from forwarders

B. To index and store data

C. To coordinate replication across peers

D. To run searches and display results

Answer: D

2. Which configuration file manages index settings like frozenTimePeriodInSecs?

A. inputs.conf

B. props.conf

C. indexes.conf

D. outputs.conf

Answer: C

3. What happens when a bucket transitions to the frozen state?

A. It is searchable

B. It is compressed

C. It is deleted or archived

D. It is replicated

Answer: C

4. Which command enables you to decommission an indexer from a cluster?

A. splunk offline --enforce-counts

B. splunk remove indexer

C. splunk offline

D. splunk stop

Answer: A

5. In a clustered deployment, which of the following roles should the master node NOT perform?

A. Cluster management

B. Search head

C. Configuration distribution

D. License master

Answer: B

6. How is app configuration deployed in a distributed environment using deployment server?

A. Via cluster manager

B. With configuration bundles

C. Through forwarder management

D. Via REST API

Answer: C

7. What file determines whether a search head is part of a search head cluster?

A. server.conf

B. clustering.conf

C. shcluster.conf

D. inputs.conf

Answer: C

8. How can you reduce license usage in Splunk?

A. Disable indexing

B. Increase frozenTimePeriodInSecs

C. Filter unwanted data at the forwarder

D. Reduce replication factor

Answer: C

9. What is the default replication factor in an indexer cluster?

A. 1

B. 2

C. 3

D. 0

Answer: C

10. How do you perform a rolling restart in an indexer cluster?

A. Restart all indexers simultaneously

B. Use splunk rolling-restart on cluster master

C. Restart the deployment server

D. Use splunk offline on each peer

Answer: B

11. Which port is used by the Deployment Server by default?

A. 8089

B. 9997

C. 8065

D. 8080

Answer: A

12. In SmartStore, what happens to warm buckets?

A. They remain on hot tier

B. They are deleted immediately

C. They are moved to remote object storage

D. They are compressed and archived

Answer: C

13. Which stanza is used in inputs.conf for monitoring a file?

A. [monitor://]

B. [file://]

C. [source://]

D. [logfile://]

Answer: A

14. What does the fschangemanager process do?

A. Tracks file system changes

B. Monitors CPU usage

C. Manages frozen buckets

D. Handles forwarder-to-indexer communication

Answer: A

15. What is the function of the btool command?

A. Re-index data

B. View effective configuration

C. Restart Splunk

D. Update indexes

Answer: B

16. What action does splunk clean eventdata perform?

A. Deletes all data and metadata

B. Archives buckets

C. Cleans frozen buckets only

D. Re-indexes raw data

Answer: A

17. When configuring LDAP authentication, which file is used?

A. authentication.conf

B. server.conf

C. users.conf

D. web.conf

Answer: A

18. What are the valid search affinity modes in a search head cluster?

A. strict, relaxed, balanced

B. preferred, random, strict

C. strict, relaxed

D. fair, distributed

Answer: C

19. How can you ensure high availability for the license master?

A. Enable indexer clustering

B. Configure license pooling

C. Implement a backup license master

D. Deploy on a forwarder

Answer: C

20. Which of the following roles can perform a bundle replication in a SHC?

A. Any member

B. Only deployer

C. Captain

D. Cluster manager

Answer: C

21. What happens when the indexing queue fills up?

A. Data is dropped

B. Data is cached to disk

C. Indexing stops

D. A restart is triggered

Answer: B

22. What does the thawed directory contain?

A. Compressed frozen data

B. Rehydrated data from archive

C. Data that failed to index

D. SmartStore metadata

Answer: B

23. How do you manually promote a new captain in a SHC?

A. Use splunk promote captain

B. Restart deployer

C. Use REST API call to captain

D. Use splunk bootstrap shcluster-captain

Answer: D

24. In indexer clustering, what is the role of the cluster manager?

A. License enforcement

B. Data parsing

C. Bucket replication coordination

D. Search head management

Answer: C

25. What does the maxHotBuckets setting control in indexes.conf?

A. Number of hot buckets allowed per index

B. Size of cold buckets

C. Maximum age of a hot bucket

D. Total number of buckets per peer

Answer: A