Advanced Splunk Enterprise Admin - 30 MCQs

1. What is the primary purpose of the `inputs.conf` file in Splunk?

A) Manage indexing rules

B) Define search constraints

C) Configure data inputs

D) Set role-based access control

Answer: C

2. Which command lists the current status of indexer cluster peers?

A) splunk show cluster-status

B) splunk show peers

C) splunk list cluster-peers

D) splunk show cluster-status -status

Answer: C

3. In an indexer cluster, what is the default replication factor?

A) 1

B) 2

C) 3

D) 4

Answer: C

4. Which file is used to set the search factor in an indexer cluster?

A) indexes.conf

B) server.conf

C) clustering.conf

D) inputs.conf

Answer: B

5. What does setting `frozenTimePeriodInSecs` in `indexes.conf` do?

A) Sets the indexer's restart time

B) Specifies how long data is searchable

C) Sets the archive timeout

D) Defines when data moves to frozen stage

Answer: D

6. What is the role of the Cluster Master Node?

A) Indexes data from forwarders

B) Serves search requests

C) Orchestrates bucket replication and peer coordination

D) Manages indexer licensing

Answer: C

7. When would you use a Heavy Forwarder instead of a Universal Forwarder?

A) For data collection only

B) When no parsing is needed

C) When filtering or routing data

D) For faster data throughput

Answer: C

8. Which file governs the throttling settings of data inputs?

A) limits.conf

B) inputs.conf

C) props.conf

D) throttle.conf

Answer: A

9. What configuration file would you use to define index settings?

A) indexes.conf

B) inputs.conf

C) props.conf

D) transforms.conf

Answer: A

10. To encrypt the data at rest in Splunk, you need to use:

A) SSL certs

B) Encrypted search heads

C) Volume-level encryption

D) Built-in Splunk Encryption API

Answer: C

11. What is the maximum number of Search Heads in a Search Head Cluster (SHC)?

A) 3

B) 5

C) 10

D) No hard limit (but ~50 recommended)

Answer: D

12. What is used to synchronize knowledge objects across SHC members?

A) KV Store

B) Captain node

C) Deployer

D) License Master

Answer: C

13. The `bundle` in Search Head clustering refers to:

A) A compressed backup of logs

B) A configuration snapshot pushed to indexers

C) A UI theme

D) A collection of Splunk dashboards

Answer: B

14. What mechanism ensures search head members work together in SHC?

A) Captain election

B) Rolling deployment

C) Search forwarding

D) License pooling

Answer: A

15. Which file holds information on indexer clustering roles?

A) clustering.conf

B) indexes.conf

C) server.conf

D) outputs.conf

Answer: A

16. Which feature helps reduce indexer storage by keeping only important logs?

A) Data aging

B) Summary indexing

C) Event sampling

D) Data model acceleration

Answer: B

17. What is the purpose of `btool` in Splunk?

A) Managing license pools

B) Viewing merged configuration settings

C) Scheduling reports

D) Restarting Splunk services

Answer: B

18. What does the `coldPath` parameter in `indexes.conf` define?

A) Location for newly indexed data

B) Storage for archived data

C) Path for rolled hot buckets

D) Path for search results

Answer: C

19. Which file would you edit to define a transform for event routing?

A) props.conf

B) transforms.conf

C) outputs.conf

D) limits.conf

Answer: B

20. What is `thawedPath` used for?

A) Cache for summary indexes

B) Backup of configuration files

C) Storage for restored frozen data

D) Path for incomplete buckets

Answer: C

21. How does the Search Head Captain manage jobs?

A) Distributes searches evenly

B) Randomly assigns jobs

C) Only handles KV Store replication

D) Controls UI interactions

Answer: A

22. What is the function of the License Master?

A) Collect logs from forwarders

B) Serve dashboards

C) Track indexing volume and compliance

D) Route data to indexers

Answer: C

23. What type of cluster replication ensures data is highly available?

A) Single-site

B) Multi-site with site-aware replication

C) Local-mode

D) Stateless mode

Answer: B

24. What is the typical retention period for hot buckets?

A) Until full

B) Fixed to 30 days

C) As defined in frozenTimePeriodInSecs

D) Until they roll to warm buckets

Answer: D

25. The `fishbucket` in Splunk tracks:

A) Failed forwarders

B) Indexed file pointers (CRC and seek)

C) Bucket transitions

D) Search job status

Answer: B

26. How does Splunk determine whether a file has already been indexed?

A) File name hash

B) Timestamps

C) File size

D) CRC and seek position stored in fishbucket

Answer: D

27. What would you use `mcatalog` command for?

A) Searching across all indexes

B) Metadata search across large deployments

C) License reporting

D) App configuration lookup

Answer: B

28. What does `splunk clean kvstore` do?

A) Deletes dashboards

B) Resets indexers

C) Removes KV Store collections

D) Deletes configuration files

Answer: C

29. Which port is typically used for receiving data from forwarders?

A) 9997

B) 8089

C) 8000

D) 443

Answer: A

30. What is used to control concurrent search limits?

A) limits.conf

B) server.conf

C) authorize.conf

D) web.conf

Answer: A