Splunk Certified Admin - Multiple Choice Questions

1. 1. What is the default location for Splunk indexes?

* A) /opt/splunk/etc
* B) /opt/splunk/var/log
* C) /opt/splunk/var/lib/splunk
* D) /opt/splunk/etc/apps

Answer: C

1. 2. Which file is used to define user roles and capabilities?

* A) users.conf
* B) authorize.conf
* C) authentication.conf
* D) server.conf

Answer: B

1. 3. What is the main purpose of inputs.conf?

* A) To configure indexing settings
* B) To define data inputs
* C) To control user access
* D) To set search time extraction

Answer: B

1. 4. What is the purpose of a deployment server in Splunk?

* A) To act as a search head
* B) To send alerts
* C) To manage forwarder configurations
* D) To store indexed data

Answer: C

1. 5. Which component is responsible for parsing and indexing data in Splunk?

* A) Forwarder
* B) Indexer
* C) Search Head
* D) Cluster Master

Answer: B

1. 6. What is the default management port of Splunk Web?

* A) 9997
* B) 8000
* C) 8089
* D) 514

Answer: B

1. 7. What are the three stages of data processing in Splunk?

* A) Input, parsing, indexing
* B) Collection, filtering, alerting
* C) Collection, transformation, search
* D) Input, transformation, visualization

Answer: A

1. 8. What kind of data does a Universal Forwarder send?

* A) Parsed data
* B) Indexed data
* C) Raw data
* D) Metadata

Answer: C

1. 9. Which command is used to restart Splunk from CLI?

* A) splunk restart
* B) splunk reload
* C) restart splunk
* D) splunkctl restart

Answer: A

1. 10. What file controls search time field extractions?

* A) inputs.conf
* B) outputs.conf
* C) props.conf
* D) indexes.conf

Answer: C

1. 11. How do you apply changes in configuration files without restarting Splunk?

* A) splunk apply config
* B) splunk refresh
* C) splunk btool reload
* D) splunk reload deploy-server

Answer: D

1. 12. What capability allows a user to edit knowledge objects?

* A) admin\_all\_objects
* B) edit\_knowledge
* C) write\_kv\_store
* D) edit\_roles

Answer: A

1. 13. What is a sourcetype in Splunk?

* A) A field that defines the host name
* B) A type of user-defined dashboard
* C) A classification of data input format
* D) A kind of saved search

Answer: C

1. 14. Which file is used to configure indexing parameters like retention and data size?

* A) props.conf
* B) indexes.conf
* C) inputs.conf
* D) limits.conf

Answer: B

1. 15. What is the function of btool in Splunk?

* A) To backup configuration files
* B) To list all available commands
* C) To debug configuration file issues
* D) To browse indexed data

Answer: C

1. 16. What does the 'fishbucket' in Splunk store?

* A) Search history
* B) User credentials
* C) Checkpoint information for file monitoring
* D) Dashboard configurations

Answer: C

1. 17. Which Splunk component handles distributed search requests?

* A) Search Head
* B) Indexer
* C) Deployment Server
* D) License Master

Answer: A

1. 18. What is the purpose of the outputs.conf file?

* A) Configure dashboard outputs
* B) Send data to indexers
* C) Manage alerts
* D) Create lookup outputs

Answer: B

1. 19. How can you back up Splunk indexes safely?

* A) While Splunk is running
* B) Using the Splunk Web UI
* C) By copying hot buckets directly
* D) By copying cold and warm buckets only

Answer: D

1. 20. What is the maximum retention period defined in indexes.conf measured in?

* A) Minutes
* B) Hours
* C) Days
* D) Seconds

Answer: D