Splunk Enterprise Certified Admin

1. Which setting in indexes.conf allows data retention to be controlled by time?

A. maxDaysToKeep

B. moveToFrozenAfter

C. maxDataRetentionTime

D. frozenTimePeriodInSecs

Answer(s): D

---

2. The universal forwarder has which capabilities when sending data? (Select all that apply.)

A. Sending alerts

B. Compressing data

C. Obfuscating/hiding data

D. Indexer acknowledgement

Answer(s): D

---

3. In case of a conflict between a whitelist and a blacklist input setting, which one is used?

A. Blacklist

B. Whitelist

C. They cancel each other out.

D. Whichever is entered into the configuration first.

Answer(s): A

---

4. In which Splunk configuration is the SEDCMD used?

A. props.conf

B. inputs.conf

C. indexes.conf

D. transforms.conf

Answer(s): A

---

5. Which of the following are supported configuration methods to add inputs on a forwarder? (Select all that apply.)

□ A. CLI

□ B. Edit inputs.conf

□ C. Edit forwarder.conf

□ D. Forwarder Management

Answer(s): A B

---

6. Which parent directory contains the configuration files in Splunk?

A. $SPLUNK_HOME/etc

B. $SPLUNK_HOME/var

C. $SPLUNK_HOME/conf

D. $SPLUNK_HOME/default

Answer(s): A

---

7. Which forwarder type can parse data prior to forwarding?

A. Universal forwarder

B. Heaviest forwarder

C. Hyper forwarder

D. Heavy forwarder

Answer(s): D

---

8. Which Splunk component consolidates the individual results and prepares reports in a distributed environment?

A. Indexers

B. Forwarder

C. Search head

D. Search peers

Answer(s): A

---

9. Which Splunk component distributes apps and certain other configuration updates to search head cluster members?

A. Deployer

B. Cluster master

C. Deployment server

D. Search head cluster master

Answer(s): A

---

10. Where should apps be located on the deployment server that the clients pull from?

A. $SPLUNK_HOME/etc/apps

B. $SPLUNK_HOME/etc/search

C. $SPLUNK_HOME/etc/master-apps

D. $SPLUNK_HOME/etc/deployment-apps

Answer(s): A

---

11. This file has been manually created on a universal forwarder:
/opt/splunkforwarder/etc/apps/my_TA/local/inputs.conf
[monitor:///var/log/messages]
sourcetype=syslog
index=syslog
A new Splunk admin comes in and connects the universal forwarders to a deployment server and deploys the same app with a new inputs.conf file:
/opt/splunk/etc/deployment-apps/my_TA/local/inputs.conf
[monitor:///var/log/maillog]
sourcetype=maillog
index=syslog
Which file is now monitored?

A. /var/log/messages

B. /var/log/maillog

C. /var/log/maillog and /var/log/messages

D. none of the above

Answer(s): A

---

12. In which phase of the index time process does the license metering occur?

A. Input phase

B. Parsing phase

C. Indexing phase

D. Licensing phase

Answer(s): C

---

13. You update a props.conf file while Splunk is running. You do not restart Splunk and you run this command: splunk btool props list –- debug. What will the output be?

A. A list of all the configurations on-disk that Splunk contains.

B. A verbose list of all configurations as they were when splunkd started.

C. A list of props.conf configurations as they are on-disk along with a file path from which the configuration is located.

D. A list of the current running props.conf configurations along with a file path from which the configuration was made.

Answer(s): D

---

14. When running the command shown below, what is the default path in which deploymentserver.conf is created?
splunk set deploy-poll deployServer:port

A. SPLUNK_HOME/etc/deployment

B. SPLUNK_HOME/etc/system/local

C. SPLUNK_HOME/etc/system/default

D. SPLUNK_HOME/etc/apps/deployment

Answer(s): B

---

15. The priority of layered Splunk configuration files depends on the file's:

A. Owner

B. Weight

C. Context

D. Creation time

Answer(s): C

---

16. When configuring monitor inputs with whitelists or blacklists, what is the supported method of filtering the lists?

A. Slash notation

B. Regular expression

C. Irregular expression

D. Wildcard-only expression

Answer(s): B

---

17. What is required when adding a native user to Splunk? (Select all that apply.)

□ A. Password

□ B. Username

□ C. Full Name

□ D. Default app

Answer(s): C D

---

18. What are the minimum required settings when creating a network input in Splunk?

A. Protocol, port number

B. Protocol, port, location

C. Protocol, username, port

D. Protocol, IP, port number

Answer(s): A

---

19. Which Splunk component requires a Forwarder license?

A. Search head

B. Heavy forwarder

C. Heaviest forwarder

D. Universal forwarder

Answer(s): B

---

20. Which optional configuration setting in inputs.conf allows you to selectively forward the data to specific indexer(s)?

A. _TCP_ROUTING

B. _INDEXER_LIST

C. _INDEXER_GROUP

D. _INDEXER_ROUTING

Answer(s): A
