

Latest Version: 12.0

Question: 1

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

- A. maxDaysToKeep
- B. moveToFrozenAfter
- C. maxDataRetentionTime
- D. frozenTimePeriodInSecs

Answer: D

<https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Setaretirementandarchivingpolicy>

Question: 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: BD

<https://docs.splunk.com/Documentation/Splunk/8.0.1/Forwarding/Aboutforwardingandreceivingdata>

Question: 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: A

<https://docs.splunk.com/Documentation/Splunk/8.0.4/Data/Whitelistorblacklistspecificincomingdata>

Question: 4

In which Splunk configuration is the SEDCMD used?

- A. props.conf
- B. inputs.conf
- C. indexes.conf
- D. transforms.conf

Answer: A

<https://docs.splunk.com/Documentation/Splunk/8.0.5/Forwarding/Forwarddatatothird-partysystems>

Question: 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: ABD