



QUESTION & ANSWER

HIGHER QUALITY, BETTER SERVICE

Provide One Year Free Update!

<https://www.passquestion.com>

Exam : **SPLK-1003**

Title : Splunk Enterprise Certified
Admin

Version : DEMO

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

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

Answer: D

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/SmartStoredataretention>

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

- A. Sending alerts
- B. Compressing data
- C. Obfuscating/hiding data
- D. Indexer acknowledgement

Answer: D

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Forwarding/Typesofforwarders>

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

Explanation:

Reference:

<https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=8&ved=2ahUKEwj0r6Lso6bkAhUqxYUKHbWIDz4QFjAHegQIAxAC&url=http%3A%2F%2Fsplunk.training%2Fshowpdf.asp%3Fdata%3D789BB6B10C1B4376B548D711B4377F3F4B511B437805A8EC11B437742EA8F11B43779B6FA211B4376EA657C11B4376FC19B311B4377E2407E11B43730AF97411B4377F3F4B511B437742EA8F11B43779B6FA211B43771F822111B437731365811B43730AF97411B437789BB6B11B4376B548D711B4377F3F4B511B437805A8EC11B437742EA8F11B43779B6FA211B4376EA657C11B4376FC19B311B4377E2407E11B43732E61E211B4377F3F4B511B437742EA8F11B43779B6FA211B43771F822111B437731365811B43746D0DC011B4377549EC611B4377BED81011B437789BB6B11B4376D8B14511B437731365811B4376B548D711B4377F3F4B511B4376FC19B311B43732E61E211B4376D8B14511B4377AD23D911B437789BB6B11B43730AF97411B4373989B2C11B437386E6F511B437386E6F511B4373DF6C0811B43737532BE11B4373BC039A11B437351CA5011B43737532BE11B43730AF97411B4375BD6DD511B43730AF97411B437564E8C211B43730AF97411B437%257C2318D1%257C11649A&usg=AOvVaw2e9s-JweivuCkqTb4-Y9uW>

4.In which Splunk configuration is the SEDCMDused?

- A. props.conf
- B. inputs.conf

- C. indexes.conf
- D. transforms.conf

Answer: A

Explanation:

Reference:

<https://answers.splunk.com/answers/212128/why-sedcmd-configured-in-propsconf-is-workingduri.html>

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

- A. CLI
- B. Edit inputs.conf
- C. Edit forwarder.conf
- D. Forwarder Management

Answer: AB

Explanation:

Reference:

https://docs.splunk.com/Documentation/Forwarder/7.3.1/Forwarder/HowtoforwarddatatoSplunkEnterprise#Define_inputs_on_the_universal_forwarder_with_configuration_files