

Exam Questions SPLK-1003

Splunk Enterprise Certified Admin

<https://www.2passeasy.com/dumps/SPLK-1003/>



NEW QUESTION 1

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: B

Explanation:

Reference: <https://docs.splunk.com/Documentation/Forwarder/7.3.1/Forwarder/Configuretheuniversalforwarder>

NEW QUESTION 2

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: C

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/HowSplunklicensingworks>

NEW QUESTION 3

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: D

Explanation:

Reference: <https://answers.splunk.com/answers/494219/need-help-with-what-should-be-a-simple-precedence.html>

NEW QUESTION 4

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: CD

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Security/Addandeditusers>

NEW QUESTION 5

Which Splunk component requires a Forwarder license?

- A. Search head
- B. Heavy forwarder
- C. Heaviest forwarder
- D. Universal forwarder

Answer: B

Explanation:

Reference: <https://answers.splunk.com/answers/70017/heavy-forwarder-costs-and-licenses.html>

NEW QUESTION 6

During search time, which directory of configuration files has the highest precedence?

- A. \$SPLUNK_HOME/etc/system/local
- B. \$SPLUNK_HOME/etc/system/default
- C. \$SPLUNK_HOME/etc/apps/app1/local
- D. \$SPLUNK_HOME/etc/users/admin/local

Answer: C

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.0/Admin/Wheretofindtheconfigurationfiles>

NEW QUESTION 7

How does the Monitoring Console monitor forwarders?

- A. By pulling internal logs from forwarders.
- B. By using the forwarder monitoring add-on.
- C. With internal logs forwarded by forwarders.
- D. With internal logs forwarder by deployment server.

Answer: A

NEW QUESTION 8

What options are available when creating custom roles? (Select all that apply.)

- A. Restrict search terms.
- B. Whitelist search terms.
- C. Limit the number of concurrent search jobs.
- D. Allow or restrict indexes that can be searched.

Answer: AD

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.2.6/Security/Aboutusersandroles>

NEW QUESTION 9

What is the default character encoding used by Splunk during the input phase?

- A. UTF-8
- B. UTF-16
- C. EBCDIC
- D. ISO 8859

Answer: A

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/Configurecharacterencoding>

NEW QUESTION 10

Which of the following enables compression for universal forwarders in outputs.conf?

- A. [udpout:mysplunk_indexer11] compression=true
- B. [tcpout] defaultGroup=my_indexers compressed=true
- C. /opt/splunkforwarder/bin/splunk enable compression
- D. [tcpout:my_indexers] server=mysplunk_indexer1:9997, mysplunk_indexer2:9997 decompression=false

Answer: B

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/Outputsconf>

NEW QUESTION 10

Which of the following statements apply to directory inputs? (Select all that apply.)

- A. All discovered text files are consumed.
- B. Compressed files are ignored by default.
- C. Splunk recursively traverses through the directory structure.
- D. When adding new log files to a monitored directory, the forwarder must be restarted to take them into account.

Answer: C

Explanation:

Reference: <https://answers.splunk.com/answers/133875/recursive-monitoring-of-directories.html>

NEW QUESTION 13

For single line event sourcetypes, it is most efficient to set SHOULD_LINEMERGE to what value?

- A. True
- B. False
- C. <regex string>
- D. Newline Character

Answer: B

Explanation:

Reference: <https://answers.splunk.com/answers/704533/what-are-the-best-practices-for-defining-source-ty.html>

NEW QUESTION 17

What is the difference between the two wildcards ... and * for the monitor stanza in inputs.conf?

- A. ... is not supported in monitor stanzas.
- B. There is no difference, they are interchangeable and match anything beyond directory boundaries.
- C. * matches anything in that specific directory path segment, whereas ... recurses through subdirectories as well.
- D. ... matches anything in that specific directory path segment, whereas * recurses through subdirectories as well.

Answer: C

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.0/Data/Specifyinputpathswithwildcards>

NEW QUESTION 21

Which valid bucket types are searchable? (Select all that apply.)

- A. Hot buckets
- B. Cold buckets
- C. Warm buckets
- D. Frozen buckets

Answer: ABC

Explanation:

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

NEW QUESTION 24

What are the required stanza attributes when configuring the transforms.conf to manipulate or remove events?

- A. REGEX, DEST, FORMAT
- B. REGEX, SRC_KEY, FORMAT
- C. REGEX, DEST_KEY, FORMAT
- D. REGEX, DEST_KEY, FORMATTING

Answer: C

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/Transformsconf>

NEW QUESTION 28

How often does Splunk recheck the LDAP server?

- A. Every 5 minutes.
- B. Each time a user logs in.
- C. Each time Splunk is restarted.
- D. Varies based on LDAP_refresh setting.

Answer: D

Explanation:

Reference: <http://docshare02.docshare.tips/files/22651/226514302.pdf>

NEW QUESTION 33

In which scenario would a Splunk Administrator want to enable data integrity check when creating an index?

- A. To ensure that hot buckets are still open for writers and have not been forced to roll to a cold state.
- B. To ensure that configuration files have not been tampered with for auditing and/or legal purposes.
- C. To ensure that user passwords have not been tampered with for auditing and/or legal purposes.
- D. To ensure that data has not been tampered with for auditing and/or legal purposes.

Answer: D

Explanation:

Reference: <https://www.splunk.com/blog/2015/10/28/data-integrity-is-back-baby.html>

NEW QUESTION 38

Which of the following apply to how distributed search works? (Select all that apply.)

- A. The search head dispatches searches to the peers.
- B. The search peers pull the data from the forwarders.
- C. Peers run searches in parallel and return their portion of results.
- D. The search head consolidates the individual results and prepares reports.

Answer: A

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/Whatisdistributedsearch>

NEW QUESTION 39

What hardware attribute would you need to be changed to increase the number of simultaneous searches (ad-hoc and scheduled) on a single search head?

- A. Disk
- B. CPUs
- C. Memory
- D. Network interface cards

Answer: B

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/SHCarchitecture>

NEW QUESTION 43

With authentication methods are natively supported within Splunk Enterprise? (Select all that apply.)

- A. LDAP
- B. SAML
- C. RADIUS
- D. Duo Multifactor Authentication

Answer: AD

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Security/SetuptoolserauthenticationwithSplunk>

NEW QUESTION 45

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SPLK-1003 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SPLK-1003 Product From:

<https://www.2passeasy.com/dumps/SPLK-1003/>

Money Back Guarantee

SPLK-1003 Practice Exam Features:

- * SPLK-1003 Questions and Answers Updated Frequently
- * SPLK-1003 Practice Questions Verified by Expert Senior Certified Staff
- * SPLK-1003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SPLK-1003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year