

Splunk

Exam Questions SPLK-1003

Splunk Enterprise Certified Admin



NEW QUESTION 1

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=AOVaw2e9s-JweivuCkqTb4-Y9uW>

NEW QUESTION 2

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: A

Explanation:

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

NEW QUESTION 3

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 4

Which Splunk forwarder type allows parsing of data before forwarding to an indexer?

- A. Universal forwarder
- B. Parsing forwarder
- C. Heavy forwarder
- D. Advanced forwarder

Answer: C

Explanation:

Reference: <https://docs.splunk.com/Documentation/SplunkCloud/7.2.6/Forwarding/Typesofforwarders>

NEW QUESTION 5

Which of the following statements describe deployment management? (Select all that apply.)

- A. Requires an Enterprise license.
- B. Is responsible for sending apps to forwarders.
- C. Once used, is the only way to manage forwarders.
- D. Can automatically restart the host OS running the forwarder.

Answer: A

NEW QUESTION 6

User role inheritance allows what to be inherited from the parent role? (Select all that apply.)

- A. Parents
- B. Capabilities
- C. Index access

D. Search history

Answer: B

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Security/Aboutusersandroles#How_users_inherit_capabilities

NEW QUESTION 7

How would you configure your distsearch.conf to allow you to run the search below?

sourcetype=access_combined status=200 action=purchase splunk_server_group=HOUSTON

- A. [distributedSearch:NYC] default = false servers = nyc1:8089, nyc2:8089 [distributedSearch:HOUSTON] default = false servers = houston1:8089, houston2:8089
- B. [distributedSearch] servers =nyc1, nyc2, houston1, houston2 [distributedSearch:NYC] default = false servers = nyc1, nyc2 [distributedSearch:HOUSTON]default = false servers = houston1, houston2
- C. [distributedSearch] servers =nyc1:8089, nyc2:8089, houston1:8089, houston2:8089[distributedSearch:NYC] default= false servers = nyc1:8089, nyc2:8089 [distributedSearch:HOUSTON]default = false servers = houston1:8089, houston2:8089
- D. [distributedSearch] servers =nyc1:8089; nyc2:8089; houston1:8089; houston2:8089[distributedSearch:NYC]default = false servers = nyc1:8089; nyc2:8089 [distributedSearch:HOUSTON] default = false servers = houston1:8089; houston2:8089

Answer: D

NEW QUESTION 8

Local user accounts created in Splunk store passwords in which file?

- A. \$SPLUNK_HOME/etc/passwd
- B. \$SPLUNK_HOME/etc/authentication
- C. \$SPLUNK_HOME/etc/users/passwd.conf
- D. \$SPLUNK_HOME/etc/users/authentication.conf

Answer: A

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/User-seedconf>

NEW QUESTION 9

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 10

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 10

What type of data is counted against the Enterprise license at a fixed 150 bytes per event?

- A. License data
- B. Metrics data
- C. Internal Splunk data
- D. Internal Windows logs

Answer: B

Explanation:

Reference: <https://answers.splunk.com/answers/581441/how-is-the-splunk-license-measured.html>

NEW QUESTION 15

How do you remove missing forwarders from the Monitoring Console?

- A. By restarting Splunk.
- B. By rescanning active forwarders.
- C. By reloading the deployment server.
- D. By rebuilding the forwarder asset table.

Answer: D

Explanation:

Reference: <https://answers.splunk.com/answers/447096/how-to-remove-missing-forwarders-from-the-distribu.html>

NEW QUESTION 17

Which Splunk indexer operating system platform is supported when sending logs from a Windows universal forwarder?

- A. Any OS platform.
- B. Linux platform only.
- C. Windows platform only.
- D. None of the above.

Answer: C

NEW QUESTION 18

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 19

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 22

Which of the following are required when defining an index in indexes.conf? (Select all that apply.)

- A. coldPath
- B. homePath
- C. frozenPath
- D. thawedPath

Answer: D

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/Indexesconf#PER_INDEX_OPTIONS

NEW QUESTION 23

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 27

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
[Order The SPLK-1003 Practice Test Here](#)