

## Exam Questions SPLK-1003

Splunk Enterprise Certified Admin

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



#### NEW QUESTION 1

Which forwarder type can parse data prior to forwarding?

- A. Universal forwarder
- B. Heaviest forwarder
- C. Hyper forwarder
- D. Heavy forwarder

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 2

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:** A

**Explanation:**

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

#### 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

Where can scripts for scripted inputs reside on the host file system? (Select all that apply.)

- A. \$SPLUNK\_HOME/bin/scripts
- B. \$SPLUNK\_HOME/etc/apps/bin
- C. \$SPLUNK\_HOME/etc/system/bin
- D. \$SPLUNK\_HOME/etc/apps/<your\_app>/bin

**Answer:** ACD

**Explanation:**

Reference: [https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/Getdatafromscriptedinputs#Where\\_to\\_place\\_the\\_scripts\\_for\\_scripted\\_inputs](https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/Getdatafromscriptedinputs#Where_to_place_the_scripts_for_scripted_inputs)

#### NEW QUESTION 5

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 6

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 7**

Which of the following authentication types requires scripting in Splunk?

- A. ADFS
- B. LDAP
- C. SAML
- D. RADIUS

**Answer: D**

**Explanation:**

Reference: <https://answers.splunk.com/answers/131127/scripted-authentication.html>

**NEW QUESTION 8**

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 9**

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 10**

Which of the following indexes come pre-configured with Splunk Enterprise? (Select all that apply.)

- A. \_licence
- B. \_internal
- C. \_external
- D. \_thefishbucket

**Answer: B**

**Explanation:**

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

**NEW QUESTION 10**

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 14**

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 19

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/SetuptoolsauthenticationwithSplunk>

#### NEW QUESTION 22

.....

## 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