

SPLK-1003^{Q&As}

Splunk Enterprise Certified Admin

Pass Splunk SPLK-1003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/splk-1003.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



QUESTION 1

Which Splunk component consolidates the individual results and prepares reports in a distributed environment?

- A. Indexers
- B. Forwarder
- C. Search head
- D. Search peers

Correct Answer: C

QUESTION 2

The volume of data from collecting log files from 50 Linux servers and 200 Windows servers will require multiple indexers.

Following best practices, which types of Splunk component instances are needed?

- A. Indexers, search head, universal forwarders, license master
- B. Indexers, search head, deployment server, universal forwarders
- C. Indexers, search head, deployment server, license master, universal forwarder
- D. Indexers, search head, deployment server, license master, universal forwarder, heavy forwarder

Correct Answer: C

QUESTION 3

A new forwarder has been installed with a manually created deploymentclient.conf.

What is the next step to enable the communication between the forwarder and the deployment server?

- A. Restart Splunk on the deployment server.
- B. Enable the deployment client in Splunk Web under Forwarder Management.
- C. Restart Splunk on the deployment client.
- D. Wait for up to the time set in the phoneHomeIntervalInSecs setting.

Correct Answer: A

Reference: <https://docs.splunk.com/Documentation/Forwarder/8.2.3/Forwarder/Configuretheuniversalforwarder>

QUESTION 4

Which feature in Splunk allows Event Breaking, Timestamp extractions, and any advanced configurations found in props.conf to be validated all through the UI?

- A. Apps
- B. Search
- C. Data preview
- D. Forwarder inputs

Correct Answer: C

<http://www.splunk.com/view/SP-CAAAGPR>

QUESTION 5

Which of the following are methods for adding inputs in Splunk? (select all that apply)

- A. CLI
- B. Splunk Web
- C. Editing inputs.conf
- D. Editing monitor.conf

Correct Answer: ABC

<https://docs.splunk.com/Documentation/Splunk/8.2.2/Data/Configureyourinputs>

Add your data to Splunk Enterprise. With Splunk Enterprise, you can add data using Splunk Web or Splunk Apps. In addition to these methods, you also can use the following methods. -The Splunk Command Line Interface (CLI) -The inputs.conf configuration file. When you specify your inputs with Splunk Web or the CLI, the details are saved in a configuration file on Splunk Enterprise indexer and heavy forwarder instances.

[SPLK-1003 Practice Test](#)

[SPLK-1003 Exam
Questions](#)

[SPLK-1003 Brindumps](#)