



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.geekcert.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

The CLI command `splunk add forward-server indexer:` will create stanza(s) in which configuration file?

- A. `inputs.conf`
- B. `indexes.conf`
- C. `outputs.conf`
- D. `servers.conf`

Correct Answer: C

The CLI command "Splunk add forward-server indexer:" is used to define the indexer and the listening port on forwards. The command creates this kind of entry "[tcpout-server://:]" in the `outputs.conf` file.

Reference: <https://docs.splunk.com/Documentation/Forwarder/8.2.2/Forwarder/Configureforwardingwithoutoutputs.conf>
<https://docs.splunk.com/Documentation/Forwarder/8.0.5/Forwarder/Enableareceiver>

QUESTION 2

Which option on the Add Data menu is most useful for testing data ingestion without creating `inputs.conf`?

- A. Upload option
- B. Forward option
- C. Monitor option
- D. Download option

Correct Answer: A

QUESTION 3

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

Correct Answer: A



QUESTION 4

Which of the following is a benefit of distributed search?

- A. Peers run search in sequence.
- B. Peers run search in parallel.
- C. Resilience from indexer failure.
- D. Resilience from search head failure.

Correct Answer: B

<https://docs.splunk.com/Documentation/Splunk/8.2.2/DistSearch/Whatisdistributedsearch>

Parallel reduce search processing If you struggle with extremely large high-cardinality searches, you might be able to apply parallel reduce processing to them to help them complete faster. You must have a distributed search environment to use parallel reduce search processing.

QUESTION 5

In addition to single, non-clustered Splunk instances, what else can the deployment server push apps to?

- A. Universal forwarders
- B. Splunk Cloud
- C. Linux package managers
- D. Windows using WMI

Correct Answer: A

Reference: <https://community.splunk.com/t5/Deployment-Architecture/Push-apps-from-deployment-server-automatically-to-universal/m-p/328191>

[Latest SPLK-1003 Dumps](#)

[SPLK-1003 VCE Dumps](#)

[SPLK-1003 Exam Questions](#)