

## SPLK-1003 Dumps

### Splunk Enterprise Certified Admin

<https://www.certleader.com/SPLK-1003-dumps.html>



#### NEW QUESTION 1

Which setting in indexes.conf allows data retention to be controlled by time?

- A. maxDaysToKeep
- B. moveToFrozenAfter
- C. maxDataRetentionTime
- D. frozenTimePeriodInSecs

**Answer:** D

#### Explanation:

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

#### 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

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 4

When running the command shown below, what is the default path in which deploymentserver.conf is created?

```
splunk set deploy-poll deployServer:port
```

- A. SPLUNK\_HOME/etc/deployment
- B. SPLUNK\_HOME/etc/system/local
- C. SPLUNK\_HOME/etc/system/default
- D. SPLUNK\_HOME/etc/apps/deployment

**Answer:** B

#### Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Updating/Configureddeploymentclients>

#### 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

Which optional configuration setting in inputs.conf allows you to selectively forward the data to specific indexer(s)?

- A. \_TCP\_ROUTING
- B. \_INDEXER\_LIST
- C. \_INDEXER\_GROUP
- D. \_INDEXER\_ROUTING

**Answer:** A

**Explanation:**

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

**NEW QUESTION 7**

To set up a network input in Splunk, what needs to be specified?

- A. File path.
- B. Username and password.
- C. Network protocol and port number.
- D. Network protocol and MAC address.

**Answer:** A

**Explanation:**

Reference: <http://dev.splunk.com/view/dev-guide/SP-CAAAE3A>

**NEW QUESTION 8**

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 9**

What is the correct order of steps in Duo Multifactor Authentication?

- A. \* 1. Request Login\* 2. Connect to SAML server\* 3. Duo MFA\* 4. Create User session\* 5. Authentication Granted\* 6. Log into Splunk
- B. \* 1. Request Login\* 2. Duo MFA\* 3. Authentication Granted\* 4. Connect to SAML server\* 5. Log into Splunk\* 6. Create User session
- C. \* 1. Request Login\* 2. Check authentication / group mapping\* 3. Authentication Granted\* 4. Duo MFA\* 5. Create User session\* 6. Log into Splunk
- D. \* 1. Request Login\* 2. Duo MFA\* 3. Check authentication / group mapping\* 4. Create User session\* 5. Authentication Granted\* 6. Log into Splunk

**Answer:** C

**Explanation:**

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

**NEW QUESTION 10**

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 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 15**

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](https://docs.splunk.com/Documentation/Splunk/7.3.1/Security/Aboutusersandroles#How_users_inherit_capabilities)

**NEW QUESTION 18**

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 21**

Which layers are involved in Splunk configuration file layering? (Select all that apply.)

- A. App context
- B. User context
- C. Global context
- D. Forwarder context

**Answer:** AC

**Explanation:**

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

**NEW QUESTION 24**

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

**Answer:** AB

**Explanation:**

Reference: <http://dev.splunk.com/view/dev-guide/SP-CAAAE3A>

**NEW QUESTION 25**

Which option accurately describes the purpose of the HTTP Event Collector (HEC)?

- A. A token-based HTTP input that is secure and scalable and that requires the use of forwarders.
- B. A token-based HTTP input that is secure and scalable and that does not require the use of forwarders.
- C. An agent-based HTTP input that is secure and scalable and that does not require the use of forwarders.
- D. A token-based HTTP input that is insecure and non-scalable and that does not require the use of forwarders.

**Answer:** B

**Explanation:**

Reference: <http://dev.splunk.com/view/event-collector/SP-CAAAE6M>

**NEW QUESTION 27**

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 31**

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 34**

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 37**

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 39**

Where are license files stored?

- A. \$SPLUNK\_HOME/etc/secure
- B. \$SPLUNK\_HOME/etc/system
- C. \$SPLUNK\_HOME/etc/licenses
- D. \$SPLUNK\_HOME/etc/apps/licenses

**Answer:** C

**Explanation:**

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

**NEW QUESTION 43**

Which Splunk component performs indexing and responds to search requests from the search head?

- A. Forwarder
- B. Search peer
- C. License master
- D. Search head cluster

**Answer:** B

**Explanation:**

Reference: <https://www.edureka.co/blog/splunk-architecture/>

**NEW QUESTION 46**

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](https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/Indexesconf#PER_INDEX_OPTIONS)

**NEW QUESTION 51**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your SPLK-1003 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/SPLK-1003-dumps.html>