

# Splunk

## Exam Questions SPLK-1003

Splunk Enterprise Certified Admin



#### 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

In which Splunk configuration is the SEDCMD used?

- A. props.conf
- B. inputs.conf
- C. indexes.conf
- D. transforms.conf

**Answer:** A

**Explanation:**

Reference: <https://answers.splunk.com/answers/212128/why-sedcmd-configured-in-propsconf-is-working-duri.html>

#### NEW QUESTION 3

Which parent directory contains the configuration files in Splunk?

- A. \$SPLUNK\_HOME/etc
- B. \$SPLUNK\_HOME/var
- C. \$SPLUNK\_HOME/conf
- D. \$SPLUNK\_HOME/default

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 4

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 5

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 6

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 7**

The priority of layered Splunk configuration files depends on the file's:

- A. Owner
- B. Weight
- C. Context
- D. Creation time

**Answer: C**

**Explanation:**

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.0/Admin/Wheretofindtheconfigurationfiles>

**NEW QUESTION 8**

What is required when adding a native user to Splunk? (Select all that apply.)

- A. Password
- B. Username
- C. Full Name
- D. Default app

**Answer: CD**

**Explanation:**

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

**NEW QUESTION 9**

Within props.conf, which stanzas are valid for data modification? (Select all that apply.)

- A. Host
- B. Server
- C. Source
- D. Sourcetype

**Answer: CD**

**Explanation:**

Reference: <https://answers.splunk.com/answers/3687/host-stanza-in-props-conf-not-being-honored-for-udp-514-data-sources.html>

**NEW QUESTION 10**

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**

How does the Monitoring Console monitor forwarders?

- A. By pulling internal logs from forwarders.
- B. By using the forwarder monitoring add-on.
- C. With internal logs forwarded by forwarders.
- D. With internal logs forwarder by deployment server.

**Answer: A**

**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 19

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 20

Which of the following is a valid distributed search group?

- A. [distributedSearch:Paris] default = false servers = server1, server2
- B. [searchGroup:Paris] default = false servers = server1:8089, server2:8089
- C. [searchGroup:Paris] default = false servers = server1:9997, server2:9997
- D. [distributedSearch:Paris] default = false servers = server1:8089; server2:8089

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 21

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 23

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 25

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 28

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 32**

When deploying apps, which attribute in the forwarder management interface determines the apps that clients install?

- A. App Class
- B. Client Class
- C. Server Class
- D. Forwarder Class

**Answer:** C

**Explanation:**

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

**NEW QUESTION 36**

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 39**

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions 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](#)**