

Splunk

Exam Questions SPLK-1003

Splunk Enterprise Certified Admin



NEW QUESTION 1

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 2

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 3

You update a props.conf file while Splunk is running. You do not restart Splunk and you run this command: splunk btool props list --debug. What will the output be?

- A. A list of all the configurations on-disk that Splunk contains.
- B. A verbose list of all configurations as they were when splunkd started.
- C. A list of props.conf configurations as they are on-disk along with a file path from which the configuration is located.
- D. A list of the current running props.conf configurations along with a file path from which the configuration was made.

Answer: D

Explanation:

Reference: <https://answers.splunk.com/answers/494219/need-help-with-what-should-be-a-simple-precedence.html>

NEW QUESTION 4

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 5

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 6

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 7

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 8

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 9

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 10

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 10

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 14

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 18

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 19

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 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 24

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 28

How do you remove missing forwarders from the Monitoring Console?

- A. By restarting Splunk.
- B. By rescanning active forwarders.
- C. By reloading the deployment server.
- D. By rebuilding the forwarder asset table.

Answer: D

Explanation:

Reference: <https://answers.splunk.com/answers/447096/how-to-remove-missing-forwarders-from-the-distribu.html>

NEW QUESTION 33

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 34

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

In this sourcetype definition the MAX_TIMESTAMP_LOOKAHEAD is missing. Which value would fit best?

```
[sshd_syslog] TIME_PREFIX = ^
```

```
TIME_FORMAT = %Y-%m-%d %H:%M:%S.%3N %z
```

```
LINE_BREAKER = ([\r\n]+)\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2} SHOULD_LINEMERGE = false
```

```
TRUNCATE = 0
```

Event example: 2018-04-13 13:42:41.214 -0500 server sshd[26219]: Connection from 172.0.2.60 port 47366

- A. MAX_TIMESTAMP_LOOKAHEAD = 5
- B. MAX_TIMESTAMP_LOOKAHEAD = 10
- C. MAX_TIMESTAMP_LOOKAHEAD = 20
- D. MAX_TIMESTAMP_LOOKAHEAD = 30

Answer: B

NEW QUESTION 37

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

NEW QUESTION 39

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 40

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/SetupuserauthenticationwithSplunk>

NEW QUESTION 42

.....

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](#)