

Exam Questions SPLK-1003

Splunk Enterprise Certified Admin

<https://www.2passeasy.com/dumps/SPLK-1003/>



NEW QUESTION 1

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 2

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 3

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 4

Where should apps be located on the deployment server that the clients pull from?

- A. \$SPLUNK_HOME/etc/apps
- B. \$SPLUNK_HOME/etc/search
- C. \$SPLUNK_HOME/etc/master-apps
- D. \$SPLUNK_HOME/etc/deployment-apps

Answer: A

Explanation:

Reference: <https://answers.splunk.com/answers/371099/how-to-configure-deployment-apps-to-push-to-client.html>

NEW QUESTION 5

This file has been manually created on a universal forwarder:

```
/opt/splunkforwarder/etc/apps/my_TA/local/inputs.conf [monitor:///var/log/messages]
```

```
sourcetype=syslog
```

```
index=syslog
```

A new Splunk admin comes in and connects the universal forwarders to a deployment server and deploys the same app with a new inputs.conf file:

```
/opt/splunk/etc/deployment-apps/my_TA/local/inputs.conf
```

```
[monitor:///var/log/maillog] sourcetype=maillog index=syslog
```

Which file is now monitored?

- A. /var/log/messages
- B. /var/log/maillog
- C. /var/log/maillog and /var/log/messages
- D. none of the above

Answer: C

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

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 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

Where can scripts for scripted inputs reside on the host file system? (Select all that apply.)

- A. \$SPLUNK_HOME/bin/scripts
- B. \$SPLUNK_HOME/etc/apps/bin
- C. \$SPLUNK_HOME/etc/system/bin
- D. \$SPLUNK_HOME/etc/apps/<your_app>/bin

Answer: ACD

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/Getdatafromscriptedinputs#Where_to_place_the_scripts_for_scripted_inputs

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 14

Which of the following are supported options when configuring optional network inputs?

- A. Metadata override, sender filtering options, network input queues (quantum queues)
- B. Metadata override, sender filtering options, network input queues (memory/persistent queues)
- C. Filename override, sender filtering options, network output queues (memory/persistent queues)
- D. Metadata override, receiver filtering options, network input queues (memory/persistent queues)

Answer: D

NEW QUESTION 17

What is the default character encoding used by Splunk during the input phase?

- A. UTF-8
- B. UTF-16
- C. EBCDIC
- D. ISO 8859

Answer: A

Explanation:

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

NEW QUESTION 21

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

NEW QUESTION 25

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 29

For single line event sourcetypes, it is most efficient to set SHOULD_LINEMERGE to what value?

- A. True
- B. False
- C. <regex string>
- D. Newline Character

Answer: B

Explanation:

Reference: <https://answers.splunk.com/answers/704533/what-are-the-best-practices-for-defining-source-ty.html>

NEW QUESTION 33

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 38

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 43

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 46

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 48

In which scenario would a Splunk Administrator want to enable data integrity check when creating an index?

- A. To ensure that hot buckets are still open for writers and have not been forced to roll to a cold state.
- B. To ensure that configuration files have not been tampered with for auditing and/or legal purposes.
- C. To ensure that user passwords have not been tampered with for auditing and/or legal purposes.
- D. To ensure that data has not been tampered with for auditing and/or legal purposes.

Answer: D

Explanation:

Reference: <https://www.splunk.com/blog/2015/10/28/data-integrity-is-back-baby.html>

NEW QUESTION 49

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 52

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 56

Which of the following apply to how distributed search works? (Select all that apply.)

- A. The search head dispatches searches to the peers.
- B. The search peers pull the data from the forwarders.
- C. Peers run searches in parallel and return their portion of results.

D. The search head consolidates the individual results and prepares reports.

Answer: A

Explanation:

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

NEW QUESTION 61

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 66

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SPLK-1003 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SPLK-1003 Product From:

<https://www.2passeasy.com/dumps/SPLK-1003/>

Money Back Guarantee

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