

Exam Questions SPLK-1003

Splunk Enterprise Certified Admin

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



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

The universal forwarder has which capabilities when sending data? (Select all that apply.)

- A. Sending alerts
- B. Compressing data
- C. Obfuscating/hiding data
- D. Indexer acknowledgement

Answer: D

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Forwarding/Typesofforwarders>

NEW QUESTION 3

Which of the following are supported configuration methods to add inputs on a forwarder? (Select all that apply.)

- A. CLI
- B. Edit inputs.conf
- C. Edit forwarder.conf
- D. Forwarder Management

Answer: B

Explanation:

Reference: <https://docs.splunk.com/Documentation/Forwarder/7.3.1/Forwarder/Configuretheuniversalforwarder>

NEW QUESTION 4

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 5

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 6

When configuring monitor inputs with whitelists or blacklists, what is the supported method of filtering the lists?

- A. Slash notation
- B. Regular expression
- C. Irregular expression
- D. Wildcard-only expression

Answer: B

Explanation:

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

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 of the following statements describe deployment management? (Select all that apply.)

- A. Requires an Enterprise license.
- B. Is responsible for sending apps to forwarders.
- C. Once used, is the only way to manage forwarders.
- D. Can automatically restart the host OS running the forwarder.

Answer: A

NEW QUESTION 9

During search time, which directory of configuration files has the highest precedence?

- A. \$SPLUNK_HOME/etc/system/local
- B. \$SPLUNK_HOME/etc/system/default
- C. \$SPLUNK_HOME/etc/apps/app1/local
- D. \$SPLUNK_HOME/etc/users/admin/local

Answer: C

Explanation:

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

NEW QUESTION 10

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

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 12

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 16

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 21

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 25

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 27

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 32

Which Splunk component does a search head primarily communicate with?

- A. Indexer
- B. Forwarder
- C. Cluster master
- D. Deployment server

Answer: A

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/InheritedDeployment/Deploymenttopology>

NEW QUESTION 36

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 41

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 46

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 49

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 52

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 54

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 58

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 59

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 64

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 69

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 72

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 77

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 82

.....

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