

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 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

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 7

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/Monitorfilesanddirectorieswithininputs.conf>

NEW QUESTION 8

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 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

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 10

Which of the following statements apply to directory inputs? (Select all that apply.)

- A. All discovered text files are consumed.
- B. Compressed files are ignored by default.
- C. Splunk recursively traverses through the directory structure.
- D. When adding new log files to a monitored directory, the forwarder must be restarted to take them into account.

Answer: C

Explanation:

Reference: <https://answers.splunk.com/answers/133875/recursive-monitoring-of-directories.html>

NEW QUESTION 15

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

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 22

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 25

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 27

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 30

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 31

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 33

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 36

.....

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