

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

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 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

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 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

What are the minimum required settings when creating a network input in Splunk?

- A. Protocol, port number
- B. Protocol, port, location
- C. Protocol, username, port
- D. Protocol, IP, port number

Answer: A

Explanation:

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

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

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

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

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 15

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 17

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 19

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 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 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 26

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 28

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 29

.....

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