

Exam Questions SPLK-1003

Splunk Enterprise Certified Admin

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



NEW QUESTION 1

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 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 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 4

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 5

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 6

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 7

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 8

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 9

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 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 10

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 15

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 16

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 17

Which of the following indexes come pre-configured with Splunk Enterprise? (Select all that apply.)

- A. _licence
- B. _internal
- C. _external
- D. _thebucket

Answer: B

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Howindexingworks>

NEW QUESTION 19

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 23

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 26

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 27

.....

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