

Exam Questions SPLK-1003

Splunk Enterprise Certified Admin

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



NEW QUESTION 1

In case of a conflict between a whitelist and a blacklist input setting, which one is used?

- A. Blacklist
- B. Whitelist
- C. They cancel each other out.
- D. Whichever is entered into the configuration first.

Answer: A

Explanation:

Reference: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=8&ved=2ahUKEwj0r6Lso6bkAhUqxYUKHbWIDz4QFjAHegQIAxAC&url=http%3A%2F%2Fsplunk.training%2Fshowpdf.asp%3Fdata%3D789BB6B10C1B4376B548D711B4377F3F4B511B437805A8EC11B437742EA8F11B43779B6FA211B4376EA657C11B4376FC19B311B4377E2407E11B43730AF97411B4377F3F4B511B437742EA8F11B43779B6FA211B43771F822111B437731365811B43730AF97411B437789BB6B11B4376B548D711B4377F3F4B511B437805A8EC11B437742EA8F11B43779B6FA211B4376EA657C11B4376FC19B311B4377E2407E11B43732E61E211B4377F3F4B511B437742EA8F11B43779B6FA211B43771F822111B437731365811B43746D0DC011B4377549EC611B4377BED81011B437789BB6B11B4376D8B14511B437731365811B4376B548D711B4377F3F4B511B4376FC19B311B43732E61E211B4376D8B14511B4377AD23D911B437789BB6B11B43730AF97411B4373989B2C11B437386E6F511B437386E6F511B4373DF6C0811B43737532BE11B4373BC039A11B437351CA5011B43737532BE11B43730AF97411B4375BD6DD511B43730AF97411B437564E8C211B43730AF97411B437%257C2318D1%257C11649A&usg=AOvVaw2e9s-JweivuCkqTb4-Y9uW>

NEW QUESTION 2

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 3

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 4

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/Monitorfilesanddirectorieswithinputs.conf>

NEW QUESTION 5

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 6

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 7

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 8

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 9

Which of the following are methods for adding inputs in Splunk? (Select all that apply.)

- A. CLI
- B. Splunk Web
- C. Editing inpits.conf
- D. Editing monitor.conf

Answer: AB

Explanation:

Reference: <http://dev.splunk.com/view/dev-guide/SP-CAAAE3A>

NEW QUESTION 10

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 10

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 11

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 16

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 19

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 23

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 26

.....

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