

Splunk

Exam Questions SPLK-1003

Splunk Enterprise Certified Admin



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 parent directory contains the configuration files in Splunk?

- A. \$SPLUNK_HOME/etc
- B. \$SPLUNK_HOME/var
- C. \$SPLUNK_HOME/conf
- D. \$SPLUNK_HOME/default

Answer: A

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/Configurationfiledirectories>

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

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 5

What is required when adding a native user to Splunk? (Select all that apply.)

- A. Password
- B. Username
- C. Full Name
- D. Default app

Answer: CD

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Security/Addandeditusers>

NEW QUESTION 6

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 7

Which Splunk forwarder type allows parsing of data before forwarding to an indexer?

- A. Universal forwarder
- B. Parsing forwarder
- C. Heavy forwarder
- D. Advanced forwarder

Answer: C

Explanation:

Reference: <https://docs.splunk.com/Documentation/SplunkCloud/7.2.6/Forwarding/Typesofforwarders>

NEW QUESTION 8

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 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

What is the default character encoding used by Splunk during the input phase?

- A. UTF-8
- B. UTF-16
- C. EBCDIC
- D. ISO 8859

Answer: A

Explanation:

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

NEW QUESTION 10

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 12

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 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 20

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 23

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 24

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
[Order The SPLK-1003 Practice Test Here](#)