SPLK-3003Q&As

Splunk Core Certified Consultant

Pass Splunk SPLK-3003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/splk-3003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Consider the scenario where the /var/log directory contains the files secure, messages, cron, audit. A customer has created the following inputs.conf stanzas in the same Splunk app in order to attempt to monitor the files secure and messages:

```
[monitor:///var/log]
sourcetype = syslog
index = security
disabled = false
whitelist = messages

[monitor:///var/log]
sourcetype  = syslog
index = security
disabled = false
whitelist = secure
```

Which file(s) will actually be actively monitored?

A. /var/log/secure B. /var/log/messages

C. /var/log/messages, /var/log/cron, /var/log/audit, /var/log/secure

D. /var/log/secure, /var/log/messages

Correct Answer: A

QUESTION 2

The universal forwarder (UF) should be used whenever possible, as it is smaller and more efficient. In which of the following scenarios would a heavy forwarder (HF) be a more appropriate choice?

A. When a predictable version of Python is required.

B. When filtering 10% - 5% of incoming events.

C. When monitoring a log file.

D. When running a script.

Correct Answer: B

Reference: https://www.splunk.com/en_us/blog/tips-and-tricks/universal-or-heavy-that-is-the-question.html

QUESTION 3

A [script://] input sends data to a Splunk forwarder using which method?

A. UDP stream

B. TCP stream

C. Temporary file

D. STDOUT/STDERR

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/latest/Admin/inputsconf

QUESTION 4

Where does the bloomfilter reside?

A. $SPLUNK_HOME/var/lib/splunk/indexfoo/db/db_1553504858_1553504507_8

B. $SPLUNK_HOME/var/lib/splunk/indexfoo/db/db_1553504858_1553504507_8/*.tsidx

C. $SPLUNK_HOME/var/lib/splunk/fishbucket

D. $SPLUNK_HOME/var/lib/splunk/indexfoo/db/db_1553504858_1553504507_8/rawdata

Correct Answer: C

QUESTION 5

What is the Splunk PS recommendation when using the deployment server and building deployment apps?

A. Carefully design smaller apps with specific configuration that can be reused.

B. Only deploy Splunk PS base configurations via the deployment server.

C. Use $SPLUNK_HOME/etc/system/local configurations on forwarders and only deploy TAs via the deployment server.

D. Carefully design bigger apps containing multiple configs.

Correct Answer: B

Reference: https://www.splunk.com/en_us/blog/platform/adding-a-deployment-server-forwardermanagement-to-a-new-or-existing-splunk-cloud-or-splunk-enterprise-deployment.html