SPLK-3003 Q&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.passapply.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
indox - socrutiy
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

Which of the following statements is true, as it pertains to search head clustering (SHC)?

A. SHC is supported on AIX, Linux, and Windows operating systems.

B. Maximum number of nodes for a SHC is 10.

C. SHC members must run on the same hardware specifications.

D. Minimum number of nodes for a SHC is 5.

Correct Answer: B

QUESTION 3

A customer would like Splunk to delete files after they\\'ve been ingested. The Universal Forwarder has read/write access to the directory structure. Which input type would be most appropriate to use in order to ensure files are ingested

and then deleted afterwards?

A. Script

B. Batch

C. Monitor

D. Fschange

Correct Answer: B

Reference: https://community.splunk.com/t5/Getting-Data-In/Is-it-possible-to-have-a-Splunk-universalforwarder-read-a/td-p/172752

QUESTION 4

A customer is using both internal Splunk authentication and LDAP for user management.

If a username exists in both $SPLUNK_HOME/etc/passwd and LDAP, which of the following statements is

accurate?

A. The internal Splunk authentication will take precedence.

B. Authentication will only succeed if the password is the same in both systems.

C. The LDAP user account will take precedence.

D. Splunk will error as it does not support overlapping usernames

Correct Answer: A

QUESTION 5

A site from a multi-site indexer cluster needs to be decommissioned. Which of the following actions must be taken?

A. Nothing. Decommissioning a site is not possible.

B. Create an alias for where the new data should be sent.

C. Remove the site from the list of available sites.

D. Remove the site from the list of available sites and create an alias for where the new data should be sent.

Correct Answer: D