SPLK-1003$^{Q\&As}$

Splunk Enterprise Certified Admin

Pass Splunk SPLK-1003 Exam with 100% Guarantee

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

QUESTION 1

Which file will be matched for the following monitor stanza in inputs. conf?

[monitor: ///var/log/*/bar/*. txt]

A. /var/log/host_460352847/temp/bar/file/csv/foo.txt

B. /var/log/host_460352847/bar/foo.txt

C. /var/log/host_460352847/bar/file/foo.txt

D. /var/ log/ host_460352847/temp/bar/file/foo.txt

Correct Answer: C

The correct answer is C. /var/log/host_460352847/bar/file/foo.txt. The monitor stanza in inputs.conf is used to configure Splunk to monitor files and directories for new data.The monitor stanza has the following syntax1:

[monitor://]

The input path can be a file or a directory, and it can include wildcards (*) and regular expressions. The wildcards match any number of characters, including none, while the regular expressions match patterns of characters.The input path is

case-sensitive and must be enclosed in double quotes if it contains spaces1. In this case, the input path is /var/log//bar/.txt, which means Splunk will monitor any file with the .txt extension that is located in a subdirectory named bar under the /

var/log directory.The subdirectory bar can be at any level under the /var/log directory, and the * wildcard will match any characters before or after the bar and .txt parts1. Therefore, the file /var/log/host_460352847/bar/file/foo.txt will be

matched by the monitor stanza, as it meets the criteria. The other files will not be matched, because:

A. /var/log/host_460352847/temp/bar/file/csv/foo.txt has a .csv extension, not a .txt extension.

B. /var/log/host_460352847/bar/foo.txt is not located in a subdirectory under the bar directory, but directly in the bar directory. D. /var/log/host_460352847/temp/bar/file/foo.txt is located in a subdirectory named file under the bar directory, not directly in the bar directory.

QUESTION 2

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 writes 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

Correct Answer: D

QUESTION 3

In inputs. conf, which stanza would mean Splunk was only reading one local file?

A. [read://opt/log/crashlog/Jan27crash.txt]

B. [monitor::/ opt/log/crashlog/Jan27crash.txt]

C. [monitor:/// opt/log/]

D. [monitor:/// opt/log/ crashlog/Jan27crash.txt]

Correct Answer: B

[monitor::/opt/log/crashlog/Jan27crash.txt]. This stanza means that Splunk is monitoring a single local file named Jan27crash.txt in the /opt/log/crashlog/ directory1. The monitor input type is used to monitor files and directories for changes and index any new data that is added2.

QUESTION 4

A security team needs to ingest a static file for a specific incident. The log file has not been collected previously and future updates to the file must not be indexed.

Which command would meet these needs?

A. splunk add one shot / opt/ incident [data .log --index incident

B. splunk edit monitor /opt/incident/data.* --index incident

C. splunk add monitor /opt/incident/data.log --index incident

D. splunk edit oneshot [opt/ incident/data.* --index incident

Correct Answer: A

The correct answer is A. splunk add one shot / opt/ incident [data . log --index incident According to the Splunk documentation1, the splunk add one shot command adds a single file or directory to the Splunk index and then stops monitoring it.

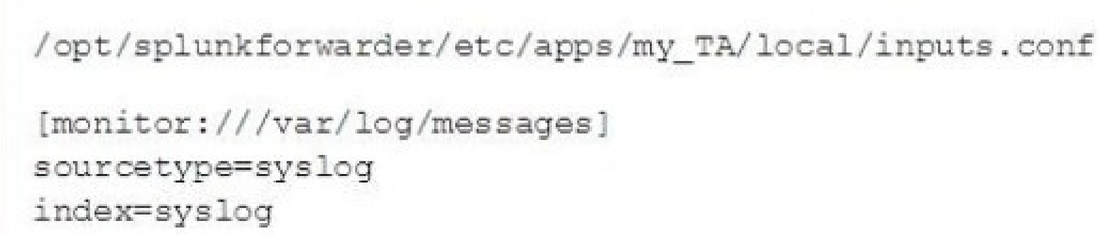
This is useful for ingesting static files that do not change or update. The command takes the following syntax:

splunk add one shot -index

The file parameter specifies the path to the file or directory to be indexed. The index parameter specifies the name of the index where the data will be stored. If the index does not exist, Splunk will create it automatically. Option B is incorrect because the splunk edit monitor command modifies an existing monitor input, which is used for ingesting files or directories that change or update over time. This command does not create a new monitor input, nor does it stop monitoring after indexing. Option C is incorrect because the splunk add monitor command creates a new monitor input, which is also used for ingesting files or directories that change or update over time. This command does not stop monitoring after indexing. Option D is incorrect because the splunk edit oneshot command does not exist. There is no such command in the Splunk CLI. References:1:Monitor files and directories with inputs.conf - Splunk Documentation

QUESTION 5

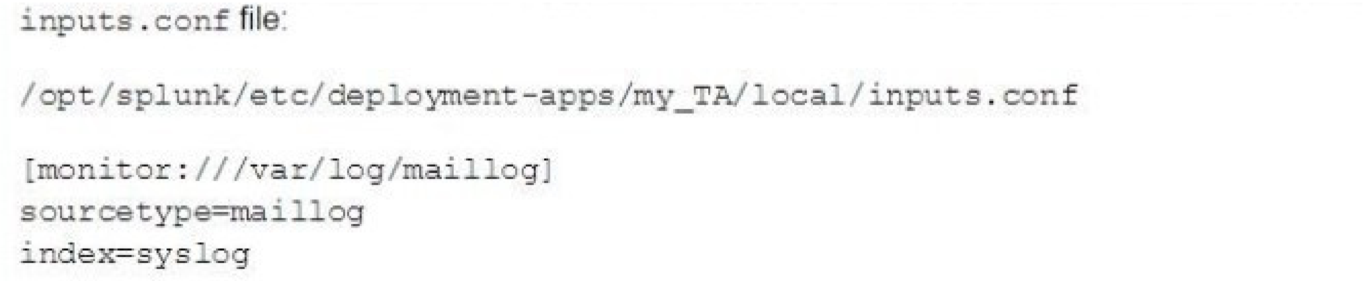
This file has been manually created on a universal forwarder



```
/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

Correct Answer: B

Latest SPLK-1003 Dumps   SPLK-1003 PDF Dumps   SPLK-1003 Study Guide