SPLK-1003 Q&As

Splunk Enterprise Certified Admin

Pass Splunk SPLK-1003 Exam with 100% Guarantee

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

https://www.geekcert.com/splk-1003.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

Which Splunk component does a search head primarily communicate with?

A. Indexer

B. Forwarder

C. Cluster master

D. Deployment server

Correct Answer: A

QUESTION 2

In which Splunk configuration is the SEDCMD used?

A. props, conf

B. inputs.conf

C. indexes.conf

D. transforms.conf

Correct Answer: A

https://docs.splunk.com/Documentation/Splunk/8.0.5/Forwarding/Forwarddatatothird-partysystemsd

"You can specify a SEDCMD configuration in props.conf to address data that contains characters that the third-party server cannot process. "

QUESTION 3

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 4

How is a remote monitor input distributed to forwarders?

A. As an app.

B. As a forward.conf file.

C. As a monitor.conf file.

D. As a forwarder monitor profile.

Correct Answer: A

https://docs.splunk.com/Documentation/Splunk/8.0.5/Data/Usingforwardingagents Scroll down to the section Titled, How to configure forwarder inputs, and subsection Here are the main ways that you can configure data inputs on a forwarder Install the app or add- on that contains the inputs you wants

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.5/Data/Usingforwardingagents

---

QUESTION 5

Where should apps be located on the deployment server that the clients pull from?

A. $SFLUNK_KOME/etc/apps

B. $SPLUNK_HCME/etc/sear:ch

C. $SPLUNK_HCME/etc/master-apps

D. $SPLUNK HCME/etc/deployment-apps

Correct Answer: D

After an app is downloaded, it resides under $SPLUNK_HOME/etc/apps on the deployment clients. But it resided in the $SPLUNK_HOME/etc/deployment-apps location in the deployment server.