splunk> turn data into doing™

Splunk Data On-Boarding Checklist

Have data you want to see in Splunk? Answering these questions will help your Splunk administrator help you.

What we'll need for each distinct data set:

Name/Owner: ______________________________

Title/Role: ______________________________

Team: ______________________________

Data sample

Description of the data

Sourcetype suggestion: ______________________________

How are events broken? ● single-line ○ multi-line (events start with: ______________________)

Is there a date/timestamp? ● yes ○ no ○ >1 (pick one: ______________________)

What time zone is in use? ______________________________

What fields are interesting? ______________________________

Uses for the data

Searches

□ I want to search using keywords for troubleshooting.

□ I want real-time searches.

□ I want to compute statistics over the last _____ weeks

□ I want to know the top *n* of something over the last _____ months

□ I want to create and save my own searches.

Reports

□ I want to create charts / tables / gauges (circle one) over the last _____ hours

□ I want real-time reports.

□ I want a dashboard.

□ I want to create and save my own reports.

□ I am building reports over long periods of time and want data summarized.

Alerts

□ I want Splunk to send me alerts via email every ___ seconds

Information about data collection

Where is it located? Server(s) ______________________________ Path ______________________________________

How should it be collected? ● Splunk Universal Forwarder ○ Syslog ○ Other: __________________________

Information about retention policy

Keep it for this long: ___ minutes

Store this much of it: ___ GB

Who should have access to the data

Team / LDAP Group: ____

Apply the Common Information Model: ____

Is there a TA available (look on Splunkbase)? ● yes (which: ______________________________________) ○ no