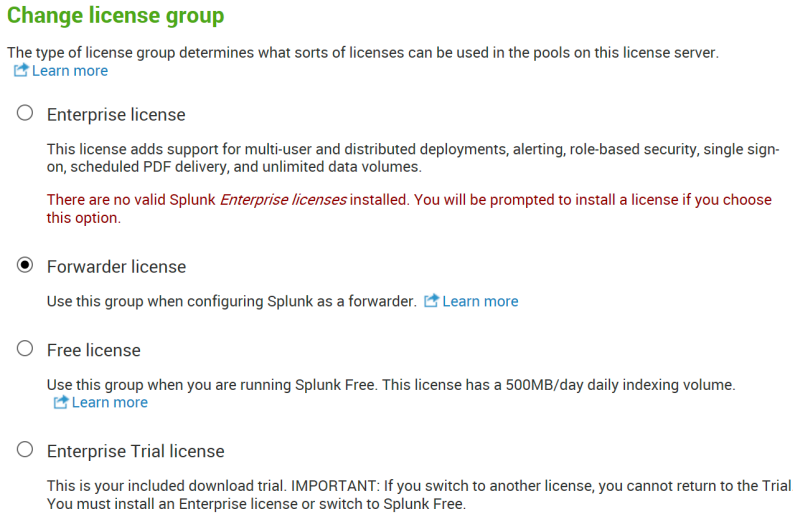
Heavy Forwarders >

Why?

- Index and parse data locally
- Load balance
- Specific data routing rules

Heavy Forwarders >

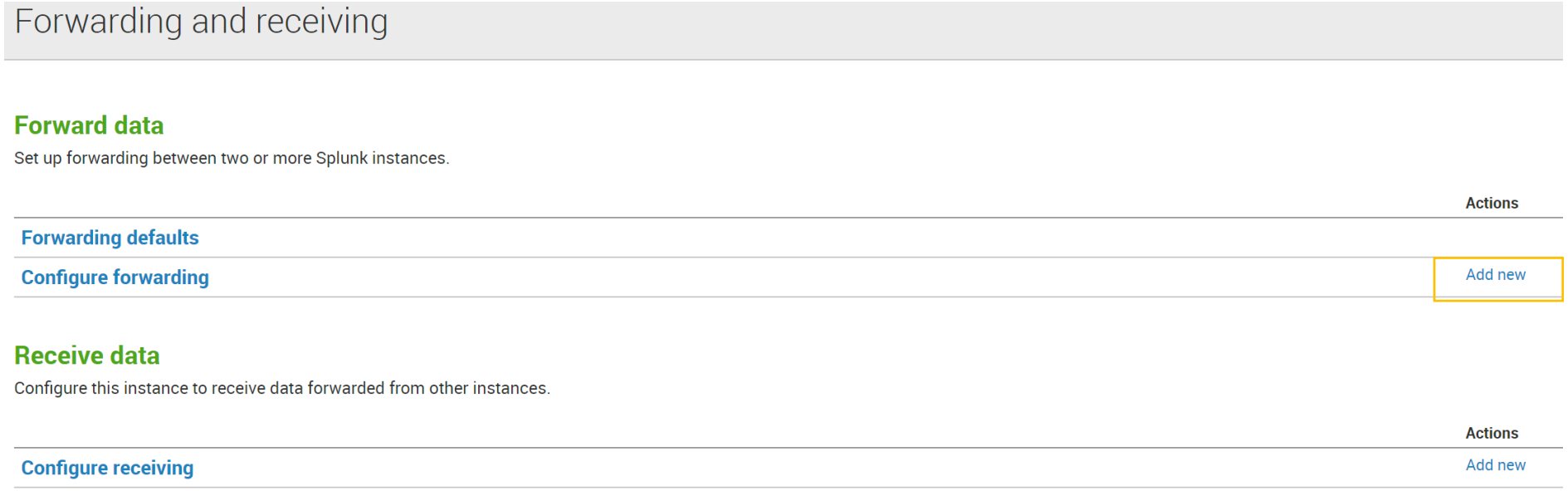
- A complete installation of Splunk
  - The same installation you would use for an indexer or search head
- Apply a forwarding license
  - Settings > Licensing > Change license group >



Heavy Forwarders >

Configuration

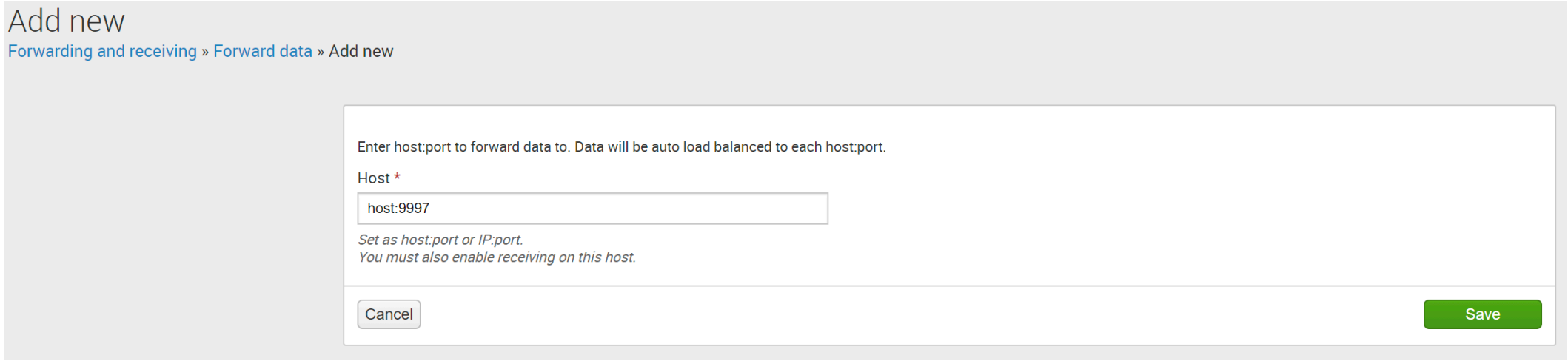
- Settings > Forwarding and Receiving > Add new (under Forward data)



Heavy Forwarders >

Configuration

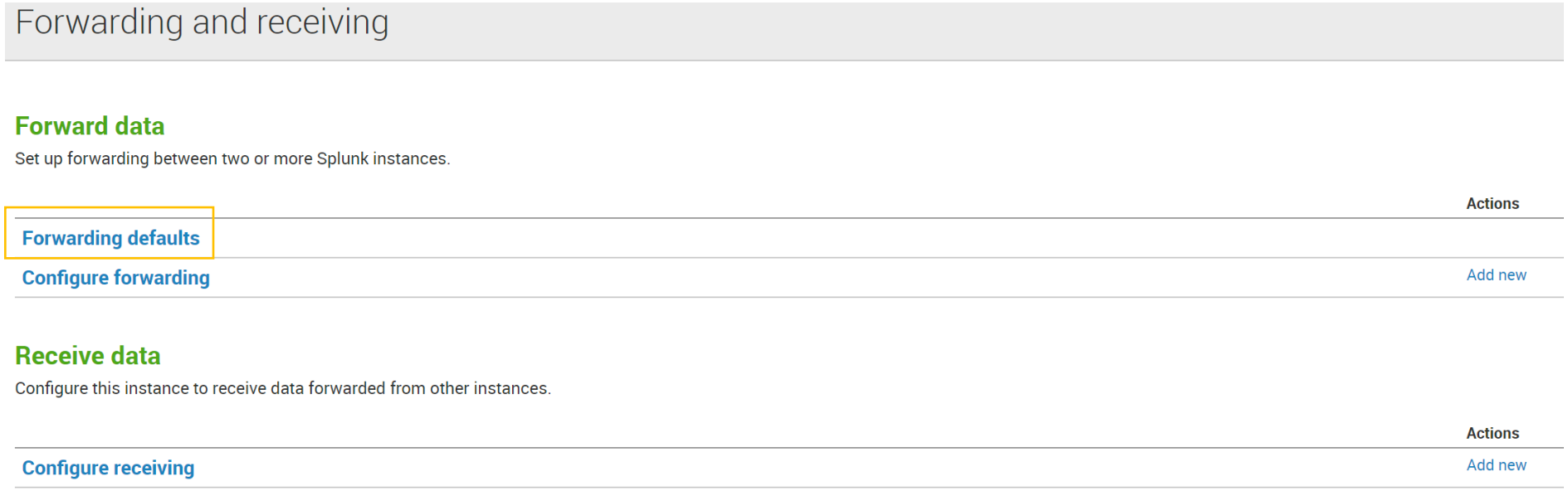
- Enter new hostname:port number, or IP:port number
- Separate multiples with commas



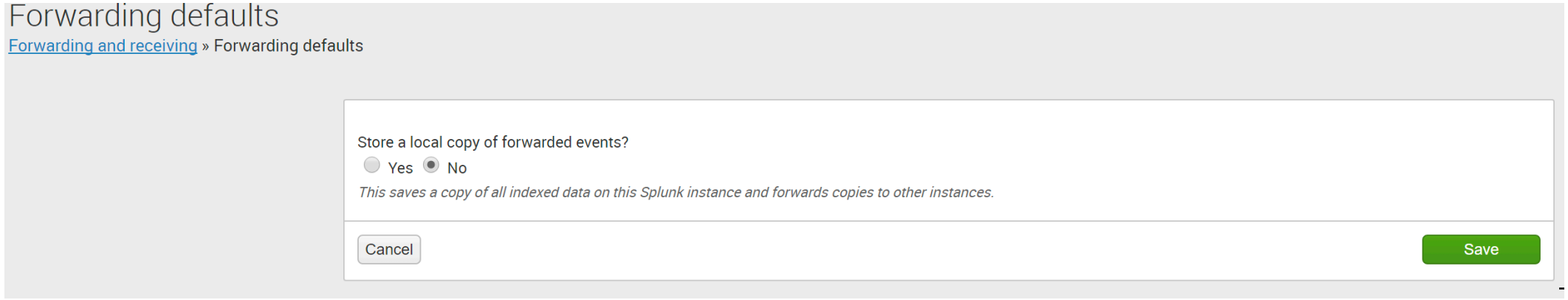
Heavy Forwarders >

Configuration

- To save a copy of the data locally, select Forwarding defaults



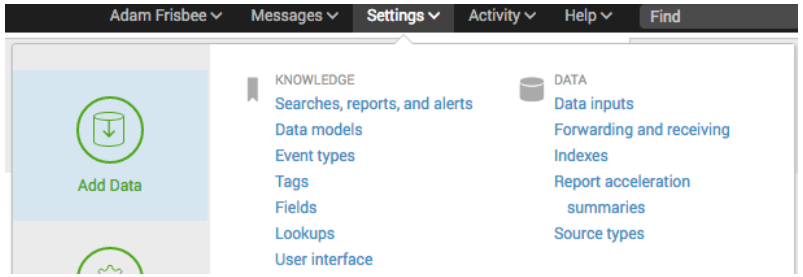
Heavy Forwarders >



Heavy Forwarders >

Universal	Heavy
“Light” agent	Full Splunk Enterprise instance
Event parsing available in some cases	Event parsing available
No event routing	Event routing available

Monitoring Files & Folders >



upload

files from my computer

Local log files
Local structured files (e.g. CSV)
Tutorial for adding data

monitor

files and ports on this Splunk indexer

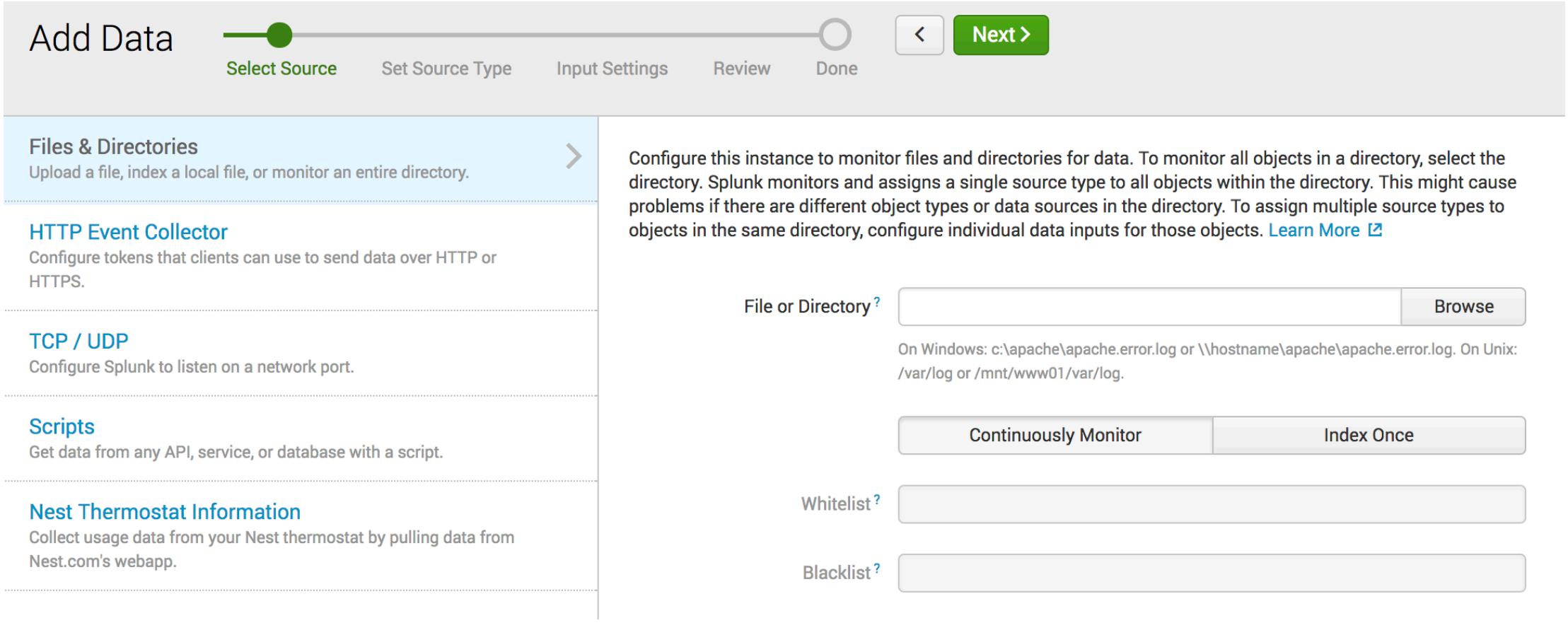
Files - WMI - TCP/UDP - Scripts
Modular inputs for external data sources

forward

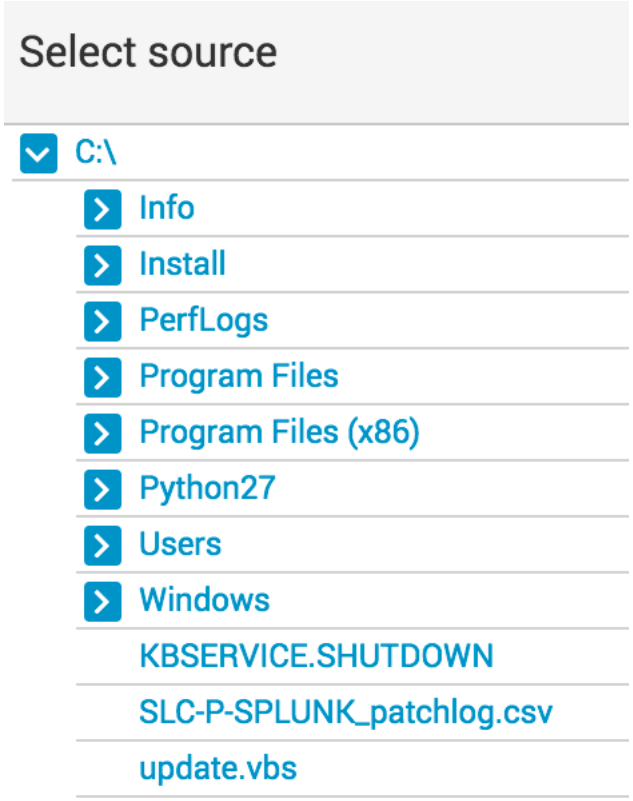
data from Splunk forwarder

Files - TCP/UDP - Scripts

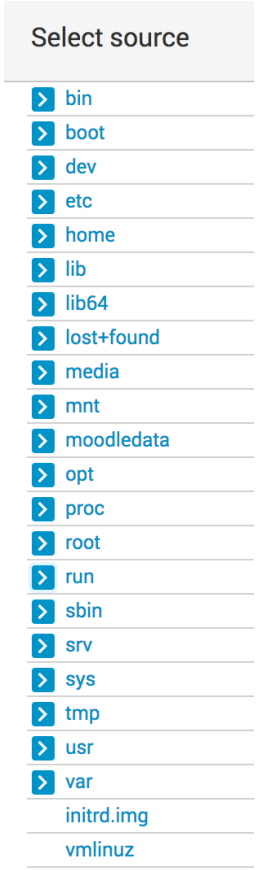
Monitoring Files & Folders >



Monitoring Files & Folders >

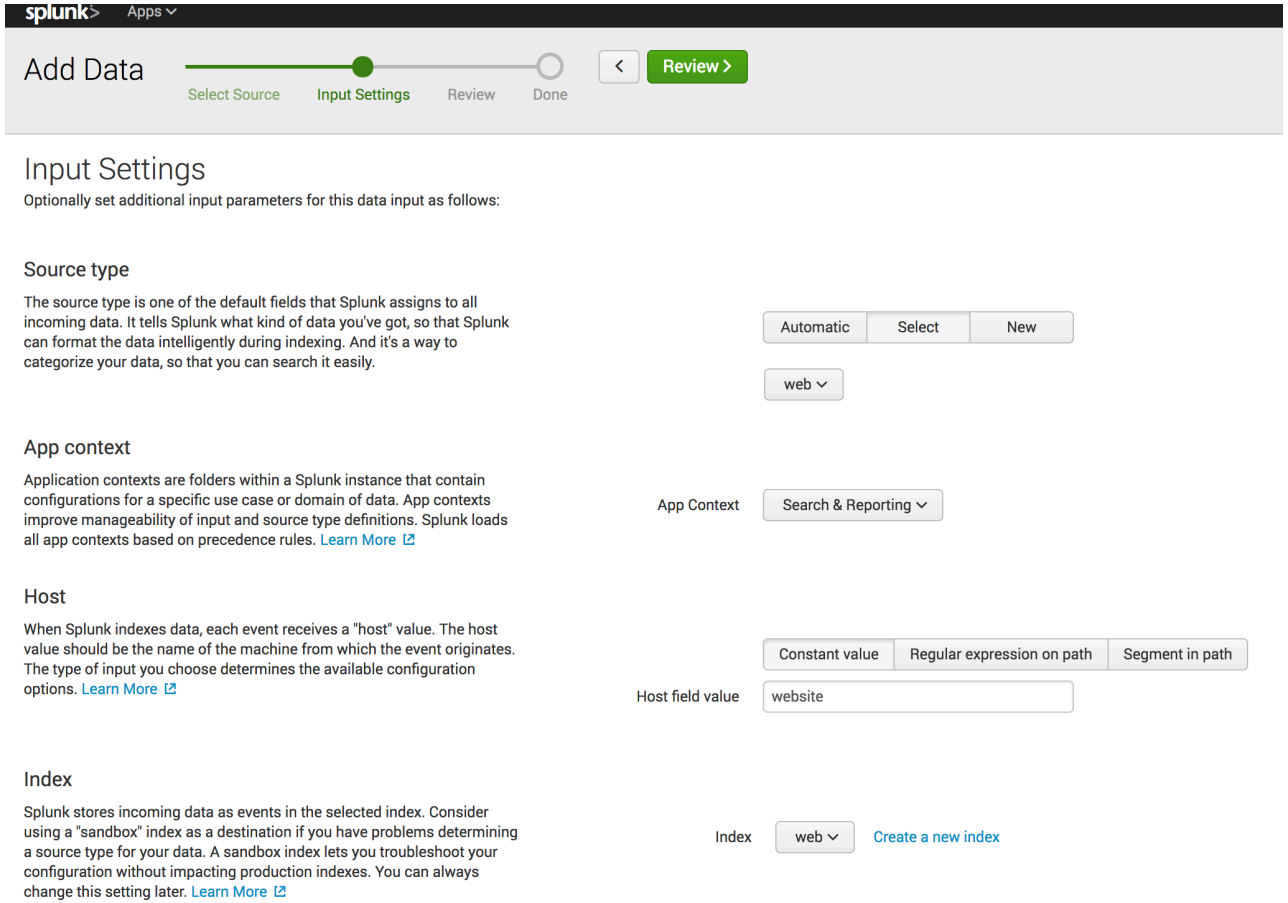


Windows



Linux

Monitoring Files & Folders >



Thanks, Splunkers!