Beats for splunk

There is no problem using the PacketBeat and TopBeat inteded for the ELK - ElasticSearch, LogStash, Kibana stack with splunk, as these can log to file:

First, install theam as described in ELK - ElasticSearch, LogStash, Kibana

Then, set the output to file in the Beat's yml file (in either /etc/packetbeat/packetbeat.yml or /etc/topbeat/topbeat.yml):

/etc/packetbeat/packetbeat.yml

```
# Configure what outputs to use when sending the data collected by the beat.
# Multiple outputs may be used.
output:
...
...
### File as output
  file:
    # Path to the directory where to save the generated files. The option is mandatory.
    path: "/tmp/packetbeat"
    # Name of the generated files. The default is `packetbeat` and it generates files: `packetbeat`,
`packetbeat.1`, `packetbeat.2`, etc.
    filename: packetbeat
    # Maximum size in kilobytes of each file. When this size is reached, the files are
    # rotated. The default value is 10 MB.
    rotate_every_kb: 10000
    # Maximum number of files under path. When this number of files is reached, the
    # oldest file is deleted and the rest are shifted from last to first. The default
    # is 7 files.
    number_of_files: 7
```

/etc/topbeat/topbeat.yml

```
# Configure what outputs to use when sending the data collected by the beat.
# Multiple outputs may be used.
output:
...
...
### File as output
  file:
    # Path to the directory where to save the generated files. The option is mandatory.
    path: "/tmp/topbeat"
    # Name of the generated files. The default is `topbeat` and it generates files: `topbeat`, `topbeat.1`,
`topbeat.2`, etc.
    filename: topbeat
    # Maximum size in kilobytes of each file. When this size is reached, the files are
    # rotated. The default value is 10 MB.
    rotate_every_kb: 10000
    # Maximum number of files under path. When this number of files is reached, the
    # oldest file is deleted and the rest are shifted from last to first. The default
    # is 7 files.
    number_of_files: 7
```

Then add, the file to splunk input.conf:

input.conf

```
[monitor:///tmp/packetbeat/packetbeat]
host=moserver
index=packetbeat
sourcetype=packetbeat-output
[monitor:///tmp/topbeat/topbeat]
host=moserver
index=topbeat
sourcetype=topbeat-output
```

These baby's log a lot of data... so I configure the sample rate for topbeat (can be done for packetbeat), and change it from 10 to 60 seconds:

/etc/topbeat/topbeat.yml

```
input:
  # In seconds, defines how often to read server statistics
  period: 10
```