USING PUPPET TO STAND UP CENTRALIZED LOGGING AND METRICS

Presented by Charles Dunbar

WHO I AM

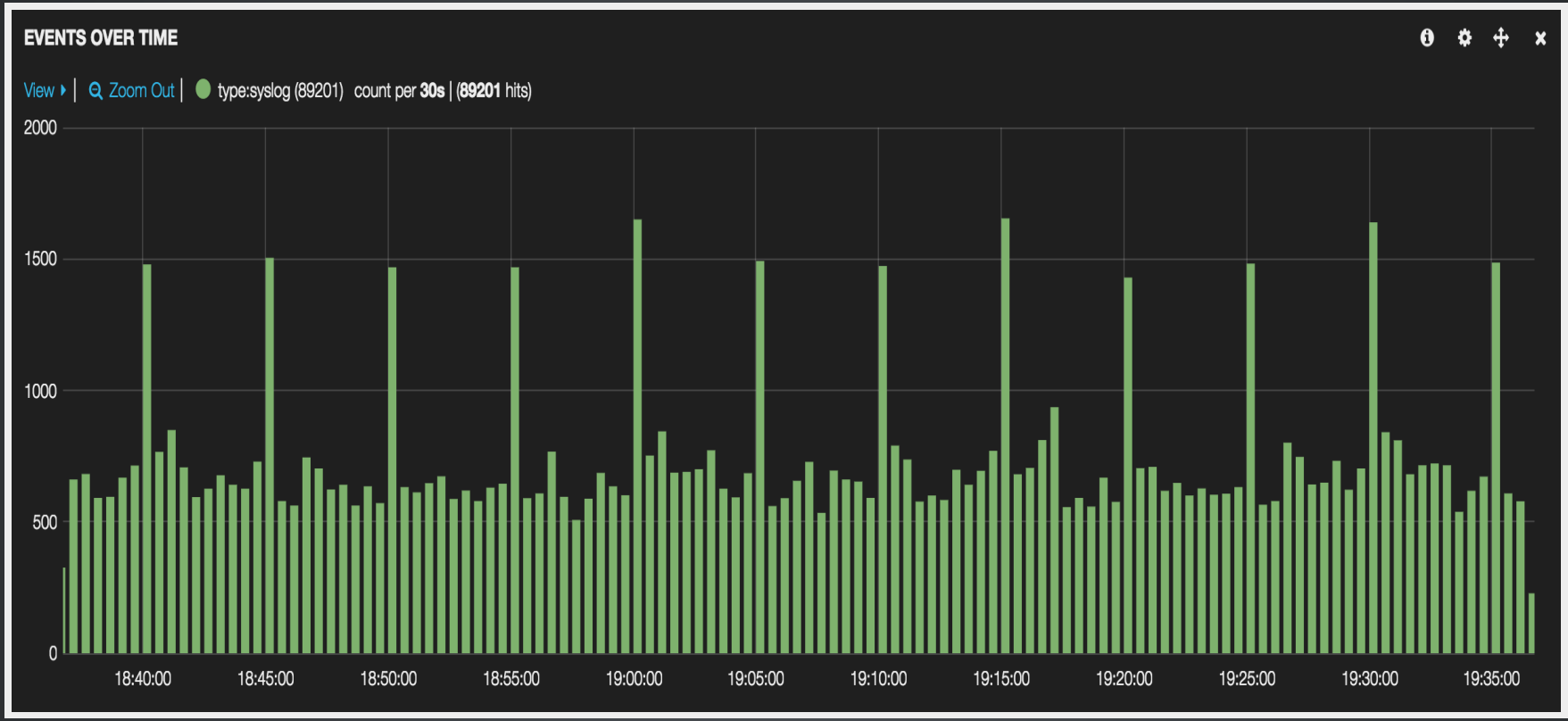
charles@puppetlabs.com

chuck_d - IRC

WHY CENTRALIZED LOGGING

- Easy to grep
- Able to delete local logs
  - Save space
  - Harder for attackers to hide tracks
- Compliance

VISUALIZING LOGS



Easier to find patterns and trends

TOOLS USED

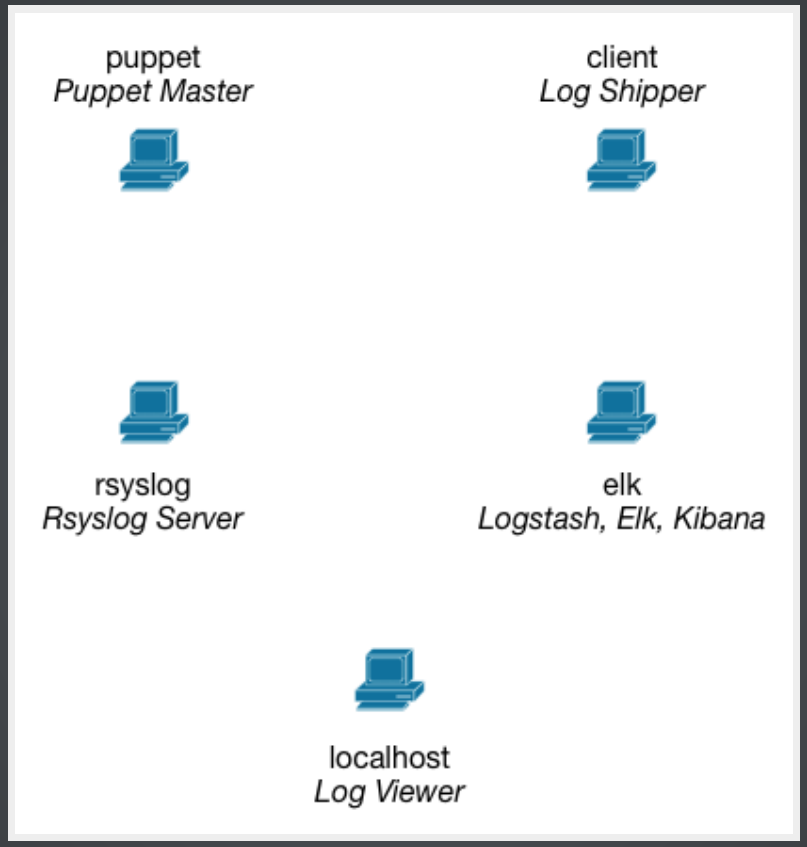
- Rsyslog + SSL
- Logstash, Elasticsearch, Kibana (ELK)
- Logstash-forwarder
- Puppet

DEMO

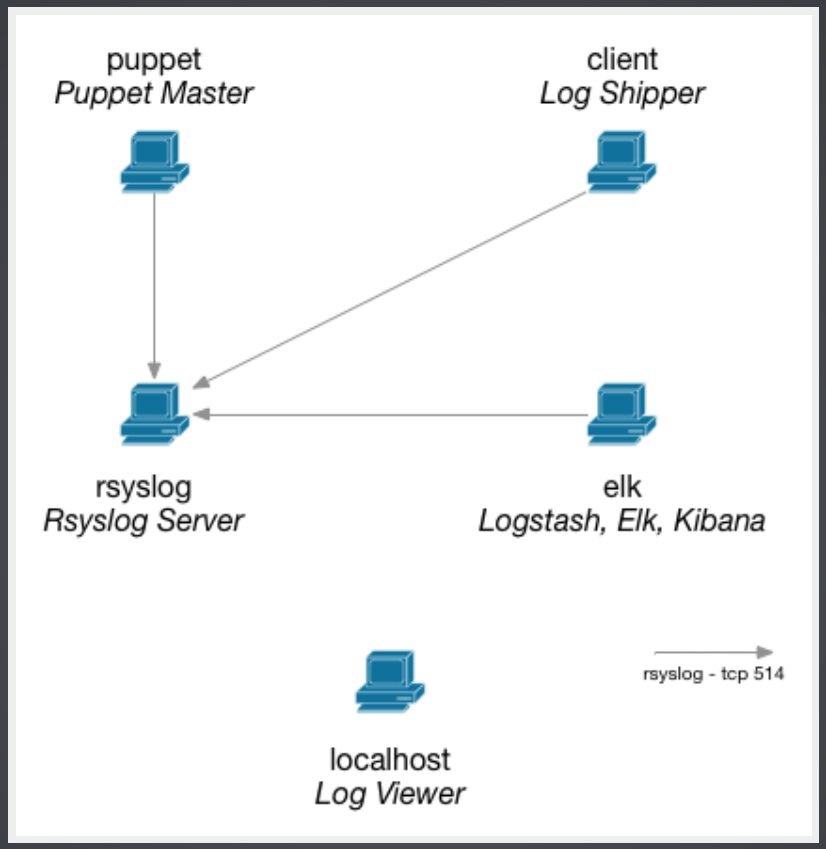
Using Vagrant with Debian VMs

Find all the files at
https://github.com/charlesdunbar/PuppetConf2014

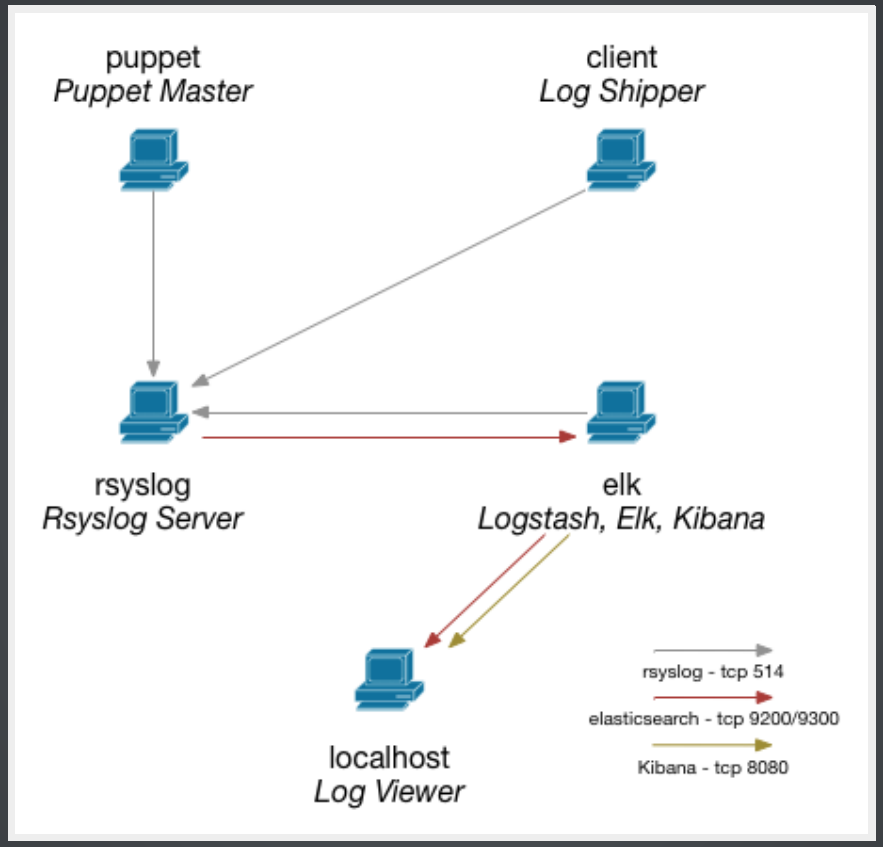
INITIAL SETUP



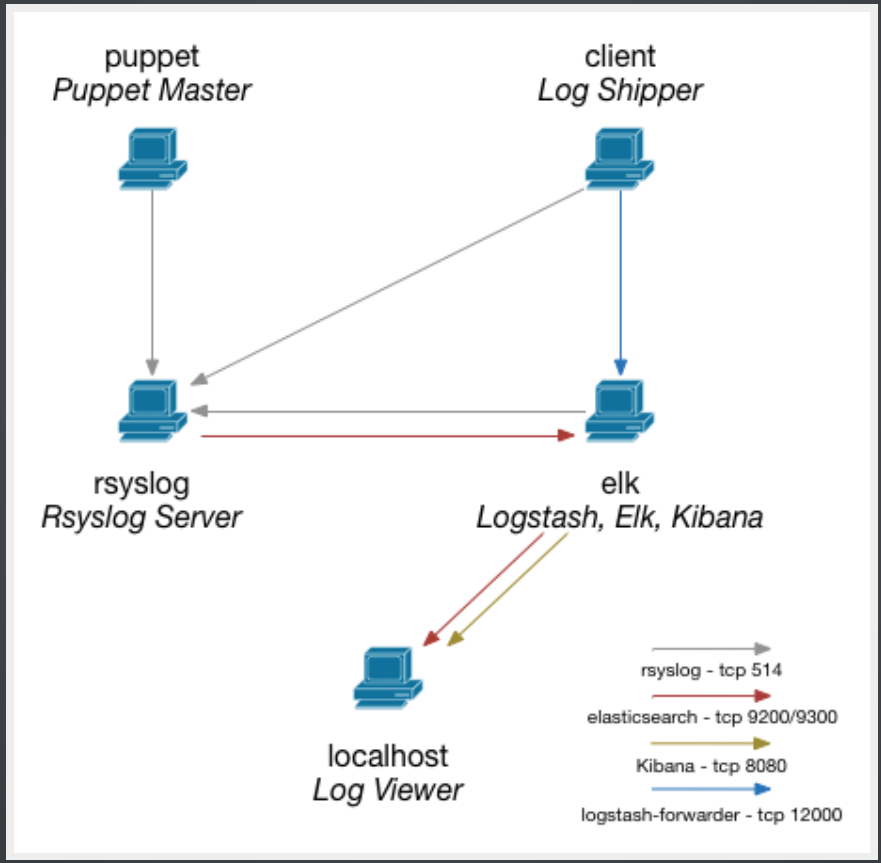
CONFIGURE RSYSLOG



CONFIGURE ELK



EXTRA LOGGING WITH LOGSTASH-FORWARDER



QUESTIONS?