Monitoring from a another POV

projects/tasks @ Hack4Glarus Winter-2019

Philipp Bühler <pb@sysfive.com> @pb_double

sysfive.com portfolio

- Continous system and application operation
- Collaborations with Providers, Developers, Services and QA
- Hybrid cloud provisioning
- cost efficient scaling on commodity HW
- scale out to AWS/RS/GCE
- Incident, problem, disaster response

- Service availability independent of solution scenario
- migrate from or to private/public cloud or own HW
- robust, scalable technology portfolio
- continuous improvements in security and server architecture
- coherent provisioning across platforms (dev/stage/live)
- vendor/provider independence, OSS focus

Projects

- Rookie Guide Updates - see Redmine-Wiki
- packer/VMM - finalize ports(7)
    - see h4g-summer presentation for details
    - go dep / vendoring - painful, reposize
    - Possible with Makefile "trickery"
- Monitoring (haproxy/prometheus/suricata/VAST/grafana/...)
-
- https://github.com/double-p --- code & presentations

What’s monitoring anyway?

Stoneage approach (pull)

- "GET / HTTP/1.0" - every 5 minutes. What about the other 4.99 minutes?
- parse logfiles "later", storage waste. Latency.
- "static" dashboards/graphs. No drill down; realtime?

Push monitoring (nowadays)

- "App" is generating events (riemann)
- or exporting (prometheus)
- serverless might be tricky (overhead, cost)

In overall way less latency, no additional logfile parsing.

Good enough?

Ask the network!

Picture: see https://twitter/pb_double

- Observe live traffic (opt: store PCAP for DPI)
- works w/o logging (if supported anyway)
- all details at your fingertips (even retrospective)
- agnostic to VM/microsvc/lambda
- different sort of complexity

Egress!!

application connects outbound

- No (HTTP) logging
- TLS1.3?
- trust/keystore (JVM restart if PKIX)
- outbound URL manipulation (api1 -> api2 at Sun midnight)
- detect malicious outbound (bitcoin!)
- IPv6!