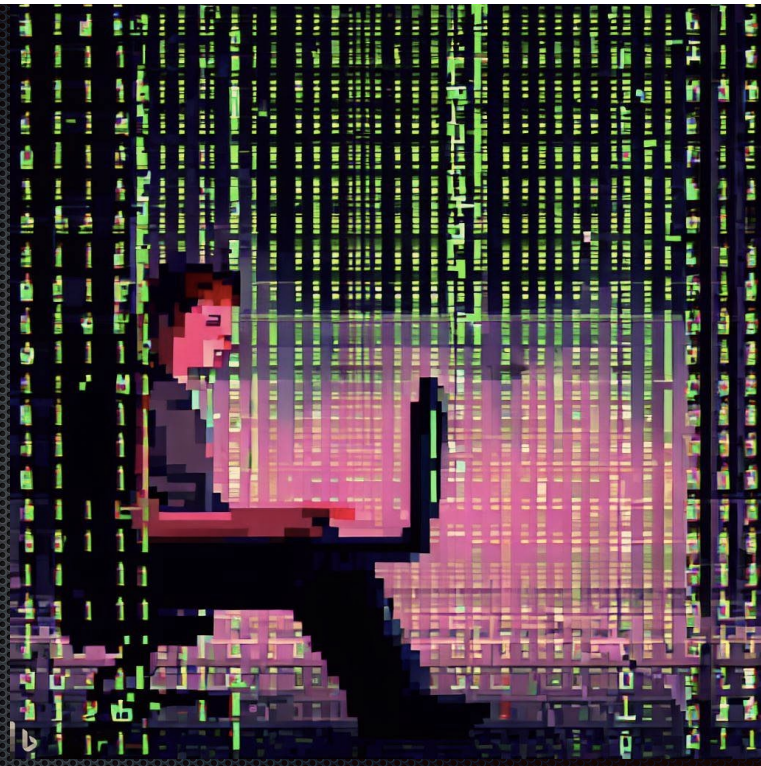
Syslog for fun (and profit?)

Warren Myers

OLF 2023



Little background about me

- Lead architect for analytics and automation for Alchemy Global Networks
- 16+ years in professional services enterprise software suites and platforms
- Been programming/admin'ing computers since I was 10
- First used Red Hat Linux 3.something in ~1996 off the CD that came with "Red Hat Linux Unleashed" by SAMS Publishing

First Question

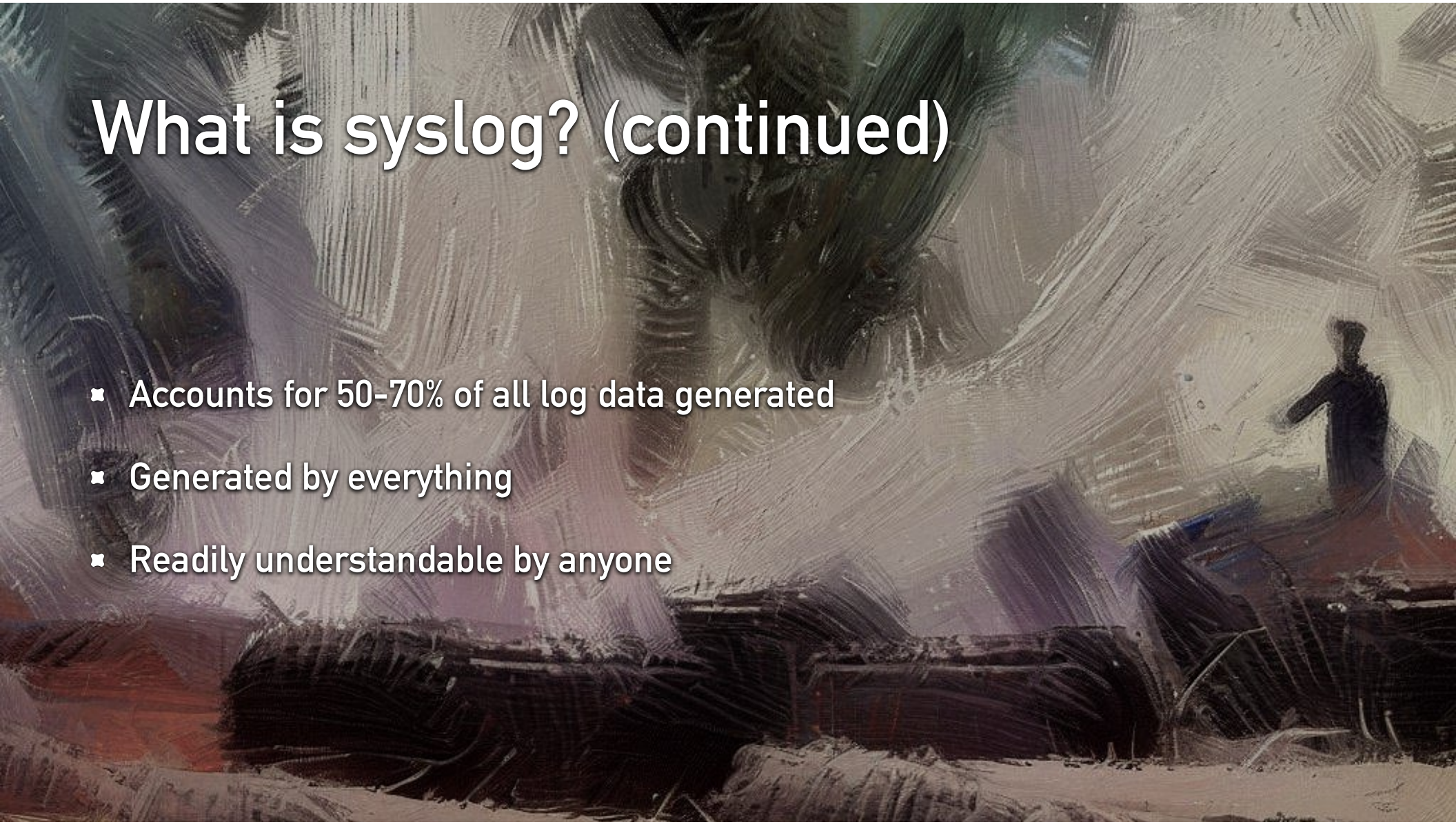
How are you managing device and application logging today?

Second Question

What insights are you gathering / wish you could gather from the plethora of logging data available in your environment?

What is syslog?

- An old, very basic, and very text-y protocol
  - A message might look like this:
    - Aug 31 17:25:40 sng-demo kernel: signal: max sigframe size: 3632
  - Or this:
    - Aug 31 17:50:57 sng-demo sshd[742]: error: kex_exchange_identification: banner line contains invalid characters



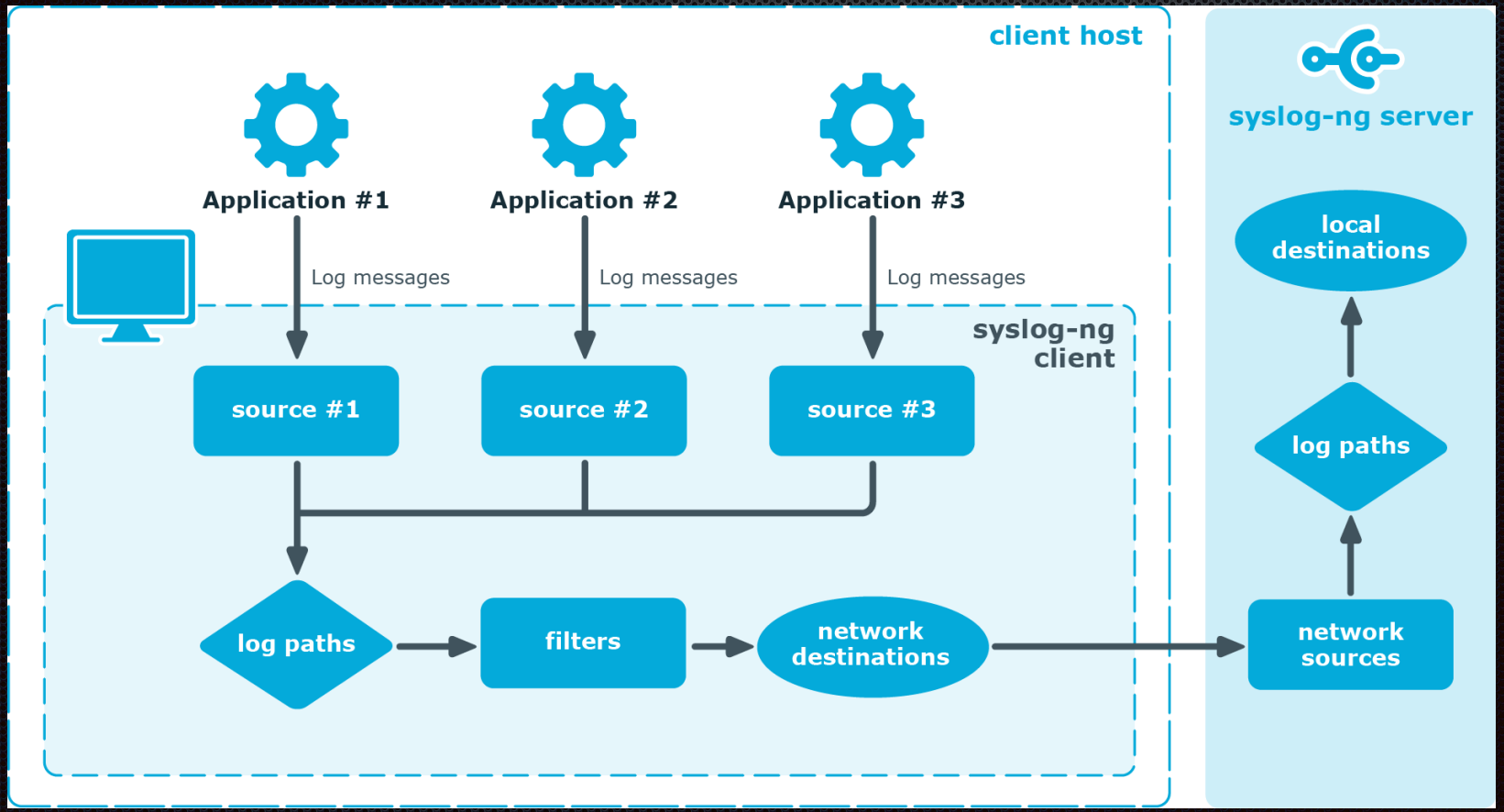
What is syslog? (continued)

- Accounts for 50-70% of all log data generated
- Generated by everything
- Readily understandable by anyone

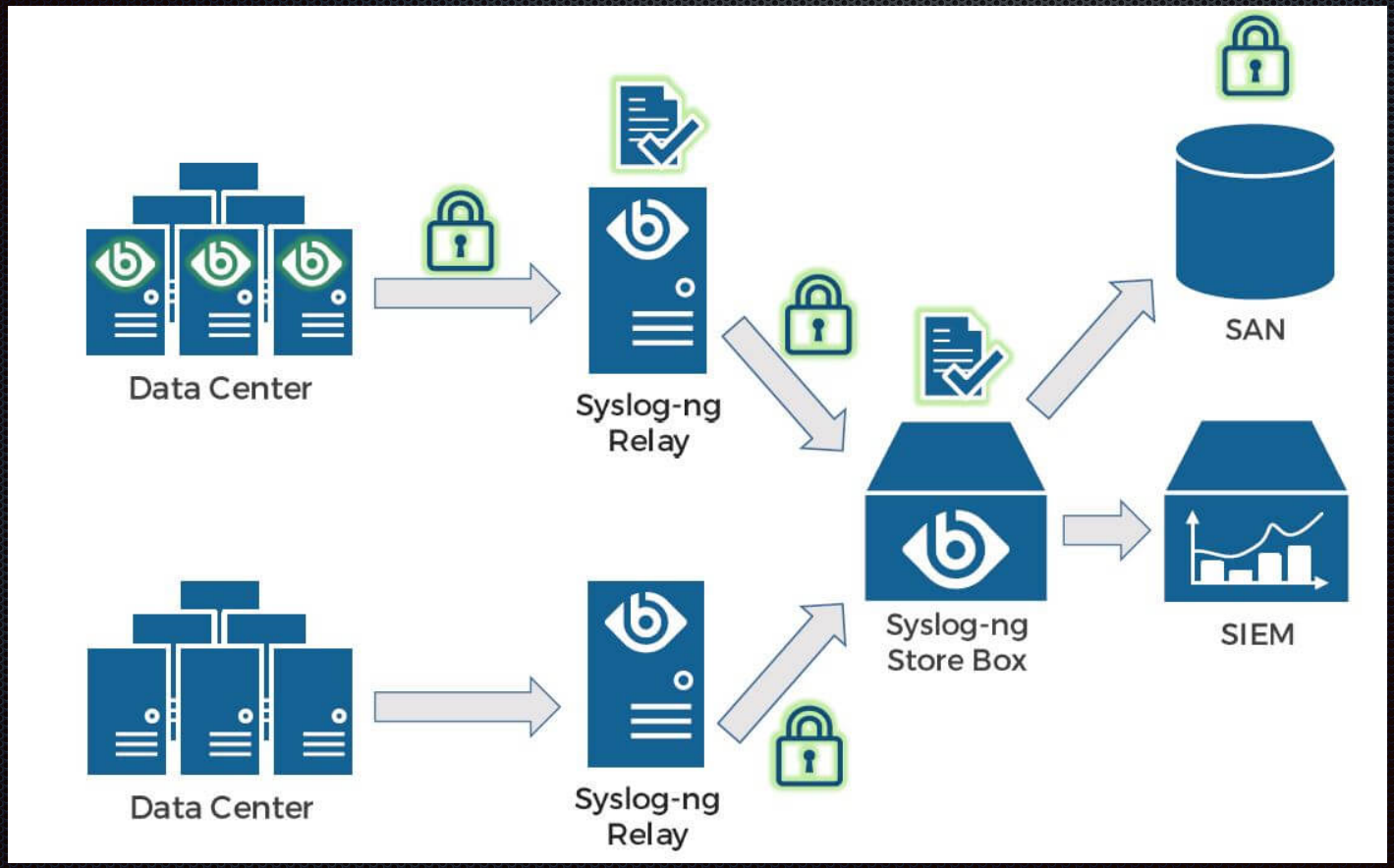
How to collect syslog

- Need a syslog collector
- Several exist - commercial, free, open-source, proprietary
  - Main OSS options
    - rsyslog - rocket-fast system for log processing; also has commercial support
    - Syslog-ng - older than rsyslog; also has a commercial option
    - GrayLog - commercial for >5GB/day
  - Proprietary options
    - Splunk; Kiwi; PRTG

Syslog-ng message path



Syslog[-ng] collection architecture

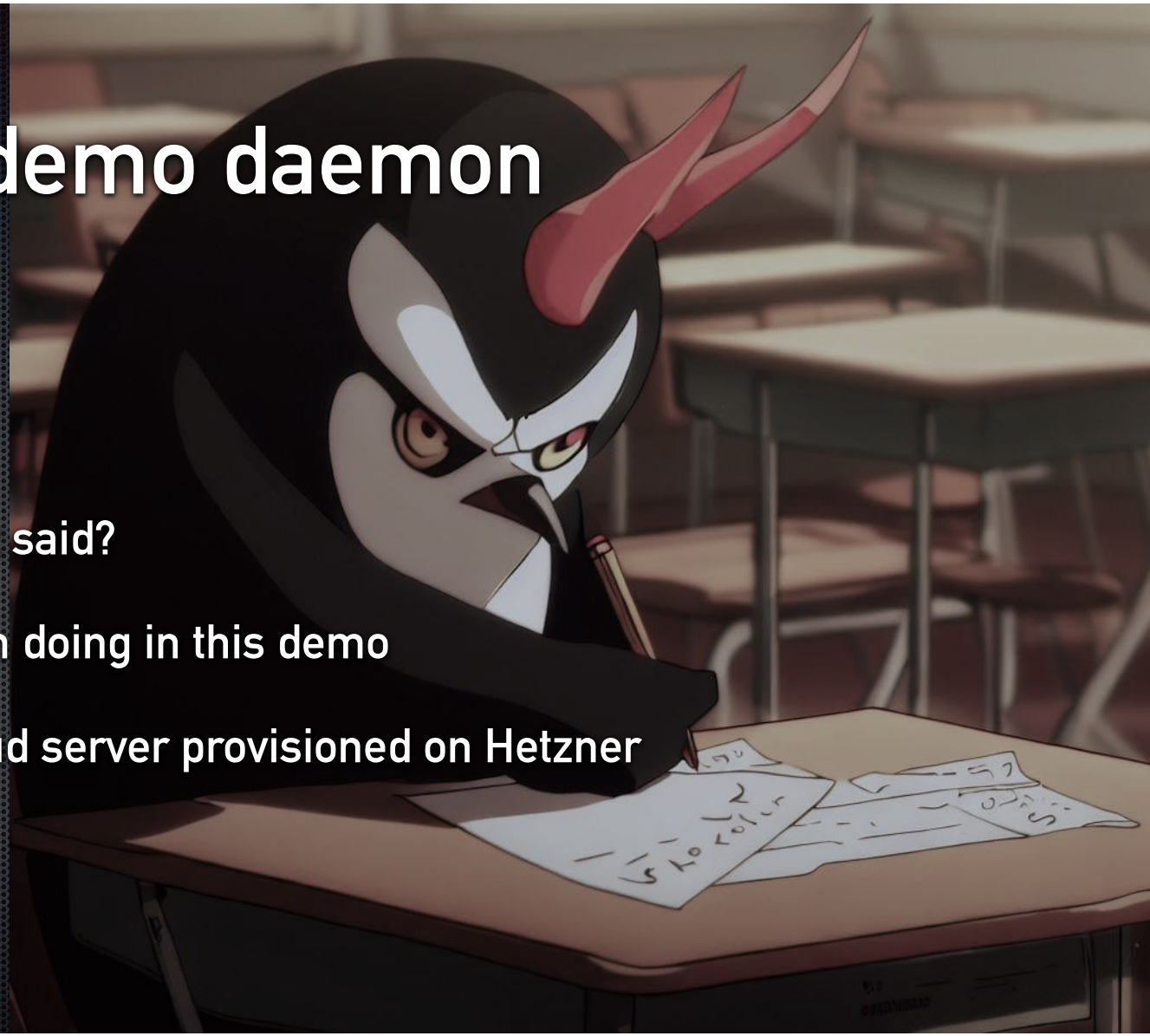


Sizing your syslog collection servers

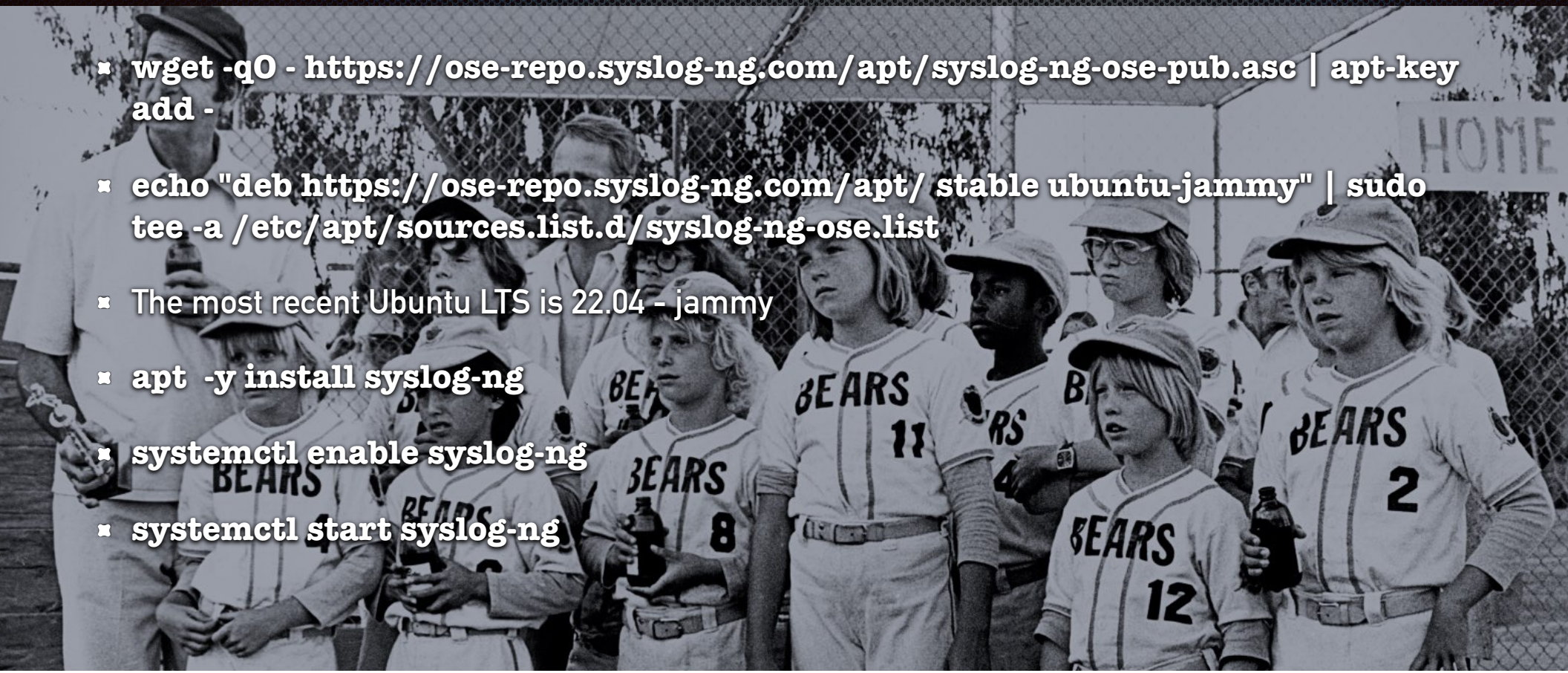
- What you need (and/or should have) to setup a syslog server/collector:
  - A [linux] server running syslog-ng
  - Enough storage, CPU, and RAM to handle plausible buffer of data between reception and sending on
    - On the storage front … I suggest a minimum of 500GB; >1TB is better
  - Network connections to all source subnets
  - Network connections to destination subnet(s)
- Nice-to-haves / Smart-to-haves (in each locale)
  - Multiple, identically-configured (minus host IP(s)) servers behind load-balancer

Tempting the demo daemon

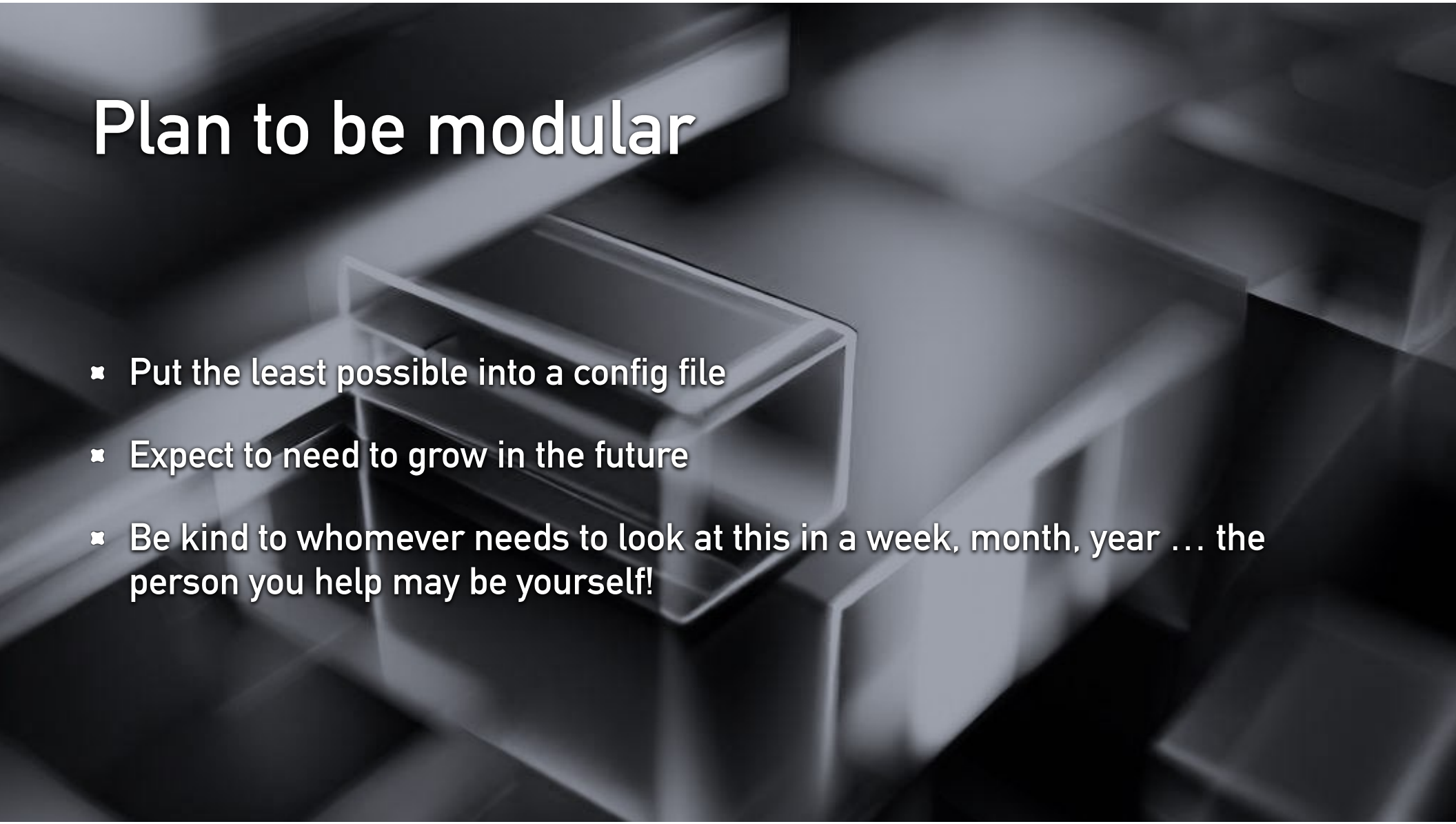
- You know everything I just said?
- Yeah … that's not what I'm doing in this demo
- I've got an entry-level cloud server provisioned on Hetzner



Steps I did not show you



- **wget -qO - https://ose-repo.syslog-ng.com/apt/syslog-ng-ose-pub.asc | apt-key add -**
- **echo "deb https://ose-repo.syslog-ng.com/apt/ stable ubuntu-jammy" | sudo tee -a /etc/apt/sources.list.d/syslog-ng-ose.list**
- The most recent Ubuntu LTS is 22.04 - jammy
- **apt -y install syslog-ng**
- **systemctl enable syslog-ng**
- **systemctl start syslog-ng**



Plan to be modular

- Put the least possible into a config file
- Expect to need to grow in the future
- Be kind to whomever needs to look at this in a week, month, year … the person you help may be yourself!

Sample collector config

```
#@version:4.3

template t_linux {
        template("$ISODATE $HOST $MSG\n") ; } ;

# '12' chosen as a leading number to indicate 'l' for "linux"
source s_linux {
        tcp(port(12514)) ; } ;

#prod data
destination d_linux_prod {
        file("/store/syslog/linux/$FACILITY/$PRIORITY/$HOST/$R_DAY.messages.log" create_dirs(yes) template(t_linux)) ; } ;

filter f_linux_prod {
        level(warning..emerg) ; } ;

log {
        source(s_linux);
        filter(f_linux_prod);
        destination(d_linux_prod) ; } ;

#dev data
destination d_linux_dev {
        file("/store/dev/linux/$FACILITY/$PRIORITY/$HOST/$R_DAY.messages.log" create_dirs(yes) template(t_linux)) ; } ;

filter f_linux_dev {
        level(debug..notice) ; } ;

log {
        source(s_linux);
        filter(f_linux_dev);
        destination(d_linux_dev) ; } ;
```

https://github.com/volcimaster/syslog-ng

Sample sender rsyslog config

- rsyslog is more commonly-found preinstalled on servers
- Add a line like the following to the end of /etc/rsyslog.conf:
  - UDP, port 514, just auth logs:
    - auth,authpriv.* @192.168.43.210:514
  - TCP, port 50514, everything:
    - *.* @@192.168.43.210:50514

Any questions?

References

https://en.wikipedia.org/wiki/Syslog
https://irisnetworks.co.uk/syslog-ng/
https://www.syslog-ng.com/technical-documents/list/syslog-ng-open-source-edition/
https://www.rsyslog.com/doc/v8-stable/
https://splunkbase.splunk.com/
https://www.elastic.co/elastic-stack/
https://linux.die.net/man/8/epylog
https://www.bing.com/images/create
https://www.syslog-ng.com/community/b/blog/posts/developing-a-syslog-ng-configuration

Links

https://antipaucity.com - my blog
https://agn.tech
https://github.com/volcimaster/syslog-ng
https://www.flickr.com/photos/14347751@N00/3009281516
https://kifarunix.com/how-to-configure-remote-logging-with-rsyslog-on-ubuntu-18-04/
https://www.syslog-ng.com/community/b/blog
https://www.syslog-ng.com/community/b/blog/posts/analyzing-apache-httpd-logs-in-syslog-ng
https://blog.augustschell.com/always-architect-demos-proofs-of-concept-for-production-use
https://web.archive.org/web/20101121110308/http://cnx.org/content/m12403/latest/