The history of logging

What have we learned?

Central unit of an entrance system.

A swiped card is an event.

Technical problems should be logged.

How do we log?


EPSON

Log retention, solved!

Log indexing, solved!

Log consistency, solved!

Offline storage, solved!

Free text search, not solved…

Syslog, a standard by accident.

Eric Allman, the founder of sendmail. ~1980

RFC 3164 2001

RFC 5424 2009

All problems solved, right?

- *The BSD syslog Protocol*. RFC 3164. (obsoleted by *The Syslog Protocol*. RFC 5424.)
- *Reliable Delivery for syslog*. RFC 3195.
- *The Syslog Protocol*. RFC 5424.
- *TLS Transport Mapping for Syslog*. RFC 5425.
- *Transmission of Syslog Messages over UDP*. RFC 5426.
- *Textual Conventions for Syslog Management*. RFC 5427.
- *Signed Syslog Messages*. RFC 5848.
- *Datagram Transport Layer Security (DTLS) Transport Mapping for Syslog*. RFC 6012.
- *Transmission of Syslog Messages over TCP*. RFC 6587.

Reliable Event Logging Protocol (RELP)

No message loss.

Backchannel

Increases load on client.

How many syslog servers do you need?

Journald

A structured log format.

Container aware

Imjournald for RELP is a new invention.

But syslog (is/was) still used for transport.

Fight over /dev/log

How to ensure log integrity?

Timeresolution

TLS

Auditd

Where do the audit logs from the syslog server go?

Datadiode

What is a datadiode?

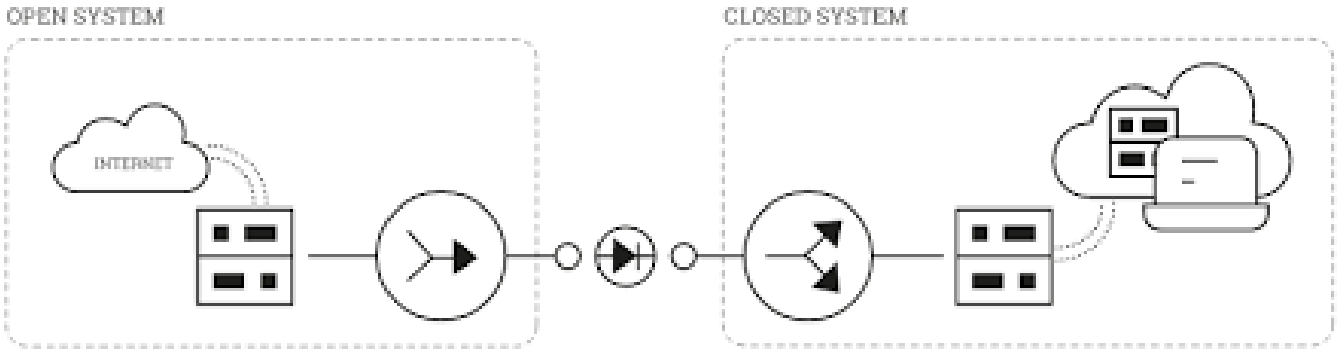
High security environments.

Not a proxy and not a firewall.

One way transport over an airgap.

FEC

DIY



How does TLS really work with syslog?

No client certificate on the client needed.

CA needed.

Server need a cert.

What to do with a certificate mismatch or expiration?

Who can read the logs

Classical syslog server

grep/sed/awk/unique/perl

Database solutions.

Windows eventlogs

Do you want to be a human keyboard?

Self service log portals

Loggly

Splunk

Graylog

ELK

Grafana Loki

Price, features, collectors and cloudiness varies.

Collecting logs

Json over tcp

WEC

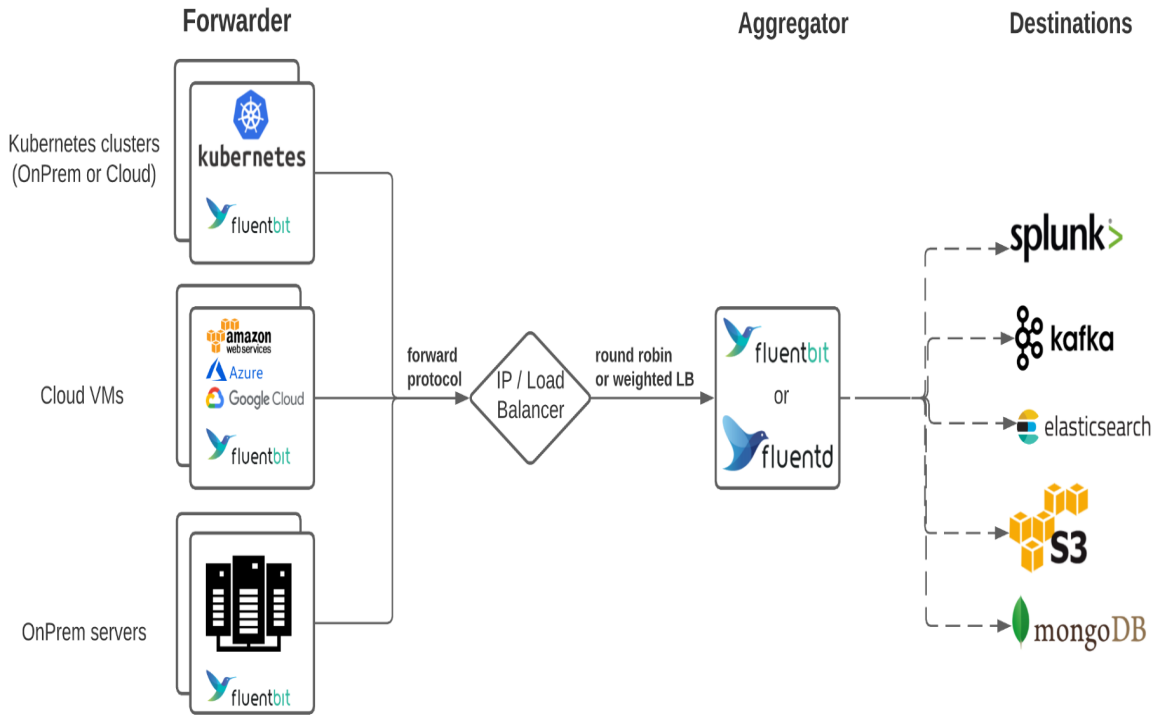
Nxlog/rsyslog

Logcollectors/filebeats

Fluentd

Unique vendors

Fetch from database



logtypes

Security

Audit

OS/infrastructurelogs

Application

Searchlog

Security log content

When

Who

What

Where

Session

Status

Real time monitoring and alerts

Replace yourself with a script.

Replace incident response with a script.

Repair what you just messed up.

Explain why you messed up.

Iterate

Collect from everywhere but not everything

Correlate

Monitor

Harass vendors and developers.

Strip unnecessary data.

What is right for you?

Classical syslog

Splunk

ELK

Grafana Loki

Your cloudvendors solution.

SIEM

Lessons learned the hard way.

Syslog over udp is trivial but everyone might not get the message.

Trim close to the source, especially a DC

Block bruteforce attempts, to save diskspace.

Avoid vendor lockin.

Practice incident response.

Save security logs for several years.

Installing a splunk clients on all computers might take five years.

Big buffers

Never try to send json over syslog.

Elastic might eat 50% of your total infrastructure.

People will forget to disable debugging.

Audit logs and fine grained permissions are usually not included in the open source version of a product.

Rsyslog configuration could have been a one hour talk by itself.

Hacking a server with auditd and syslog enabled is not as fun as without.

Multiline messages

Questions ?

peptekmail@gmail.com