• audit framework allows to record security-relevant events
• if your system is compromised use can use audit logs to perform post mortem analysis
• problem: audit logs are stored on a machine you cannot trust anymore
  • how do you know the logs are intact?
auditdistd

- a daemon to distribute audit logs to remote hosts
- logs are distributed immediately as they show up, optionally we can delay distribution and send them in bigger chunks
- ability to send audit logs to several daemons in parallel and ability to receive logs from several daemons
challenges

• reliability (we cannot afford losing audit records)
• low latency in logs delivery
• performance
• on-the-wire data protection
• dealing with compromised clients
status

- around 30% done

Paweł Jakub Dawidek <pjd@FreeBSD.org>