Ticketing system integration

5th TF-NOC meeting
Dubrovnik 15/2-12
Stefan Liström

Agenda

- Background
- Current problems and solutions
- Our idea and implementation
- Conclusions

Background

- Before and now
  - Early 1970’s we started sending e-mails over the network
  - 2012 The most preferred way to communicate with external parties is still e-mail (see NOC survey).
- Two main ways to send out ticket info
  - Disseminate to only selected parties
    - Very restrictive and can be hard to manage
  - Disseminate everything to everyone
    - Can become very “spammy”

Problems

- Problems (primarily multi-domain)
    - Large customers (projects that buy services from several NRENs) have a hard time to get a complete overview of their service.
    - Coordinating troubleshooting on the same service in several domains is very challenging
    - Information sent between different organisations have to be manually added to ticket systems

Current solutions

- Current solutions (workarounds)
  - Implement a separate ticket system (LHCOPN)
  - Implement a separate organisation to collect and disseminate information (E2ECU)
- Both solutions have overhead
  - I.e. NOC have to use two ticket systems for same information or someone have to "manually" collect information from several sources and redistribute it

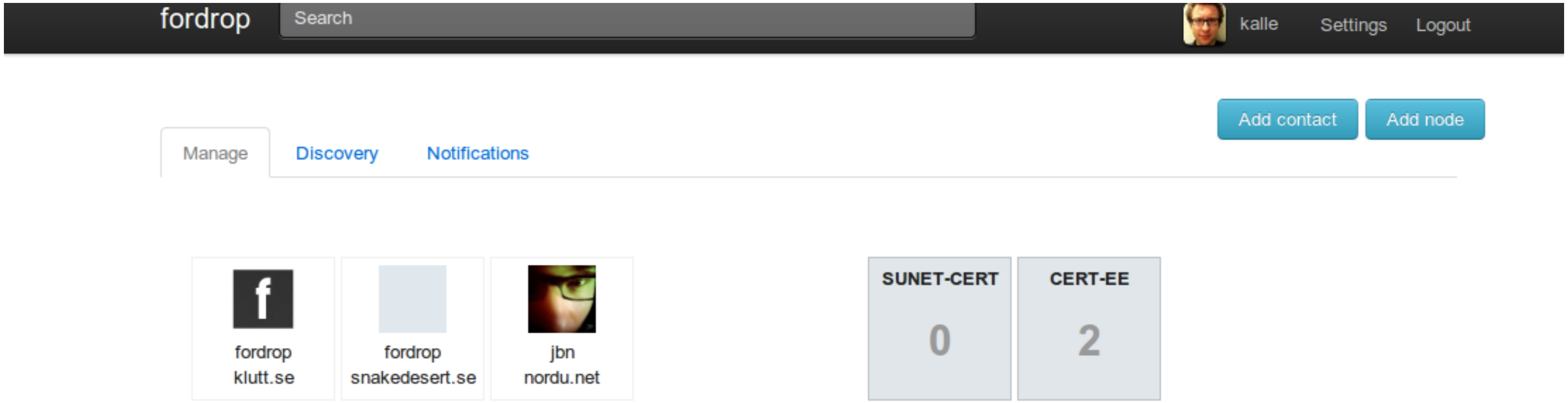
Earlier work

- Correlation of information in e-mails in the EGEE project
- Proved very hard
  - Due to loose constraints on e-mails almost every organisation use different structures, information and language in their e-mails
- However part of that work resulted in RFC6137 (NTTDM)
  - Some bias towards grid community but for most parts very generic and useful

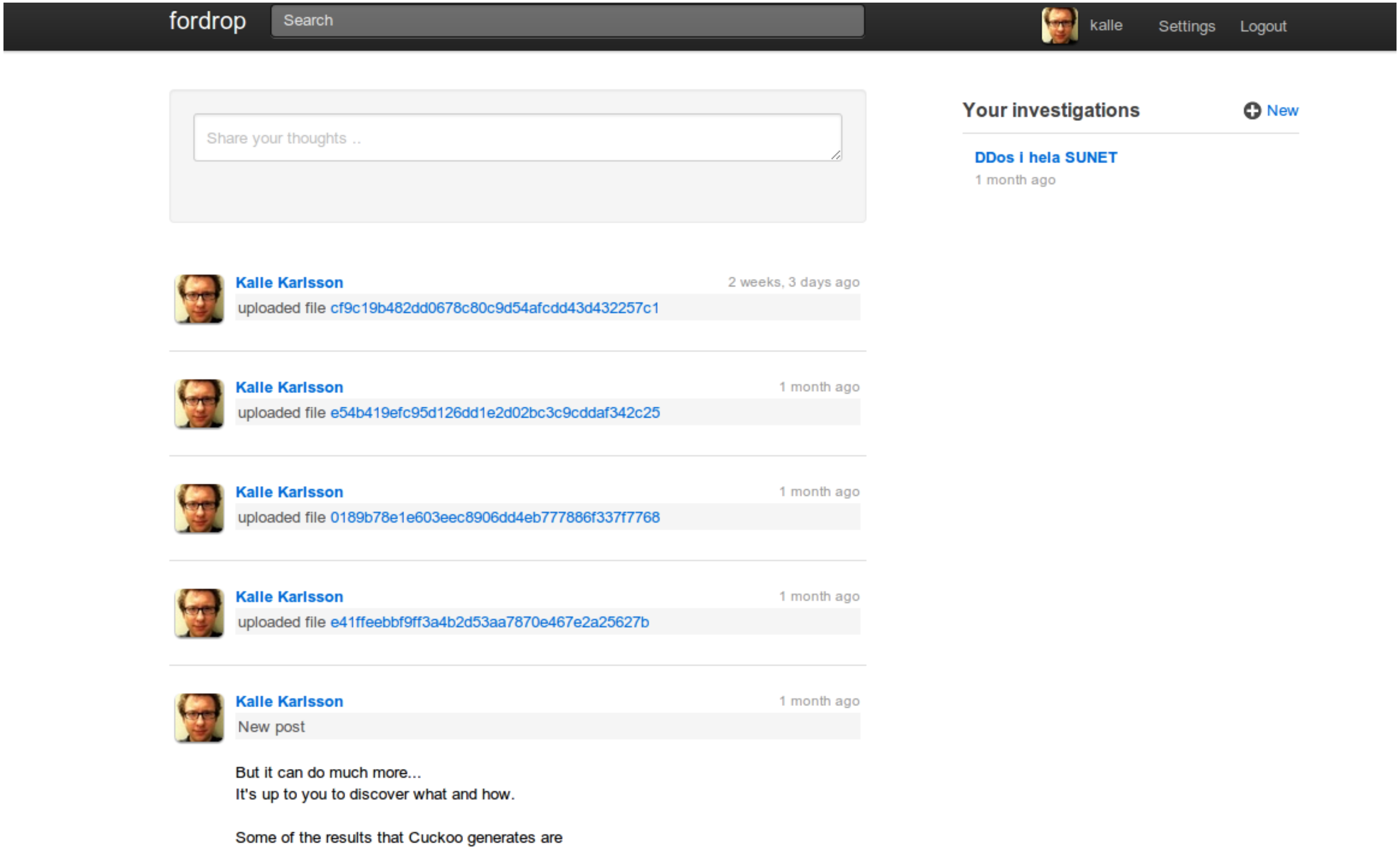
Fordrop

- Forensic dropbox is a social tool for collaborative computer forensic analysis (fordrop.org)
- Targeted towards CERT community
- Distributed (bootstrap as centralized)
- Subscribe and publish using XMPP federations
- Messages are structured as Activity streams (JSON)
- Presentation at Terena 2012 conf.

Users and nodes



Message thread



Your investigations

DDos i hela SUNET
1 month ago

Kalle Karlsson 2 weeks, 3 days ago
uploaded file cf9c19b482dd0678c80c9d54afcdd43d432257c1

Kalle Karlsson 1 month ago
uploaded file e54b419efc95d126dd1e2d02bc3c9cddaf342c25

Kalle Karlsson 1 month ago
uploaded file 0189b78e1e603eec8906dd4eb777886f337f7768

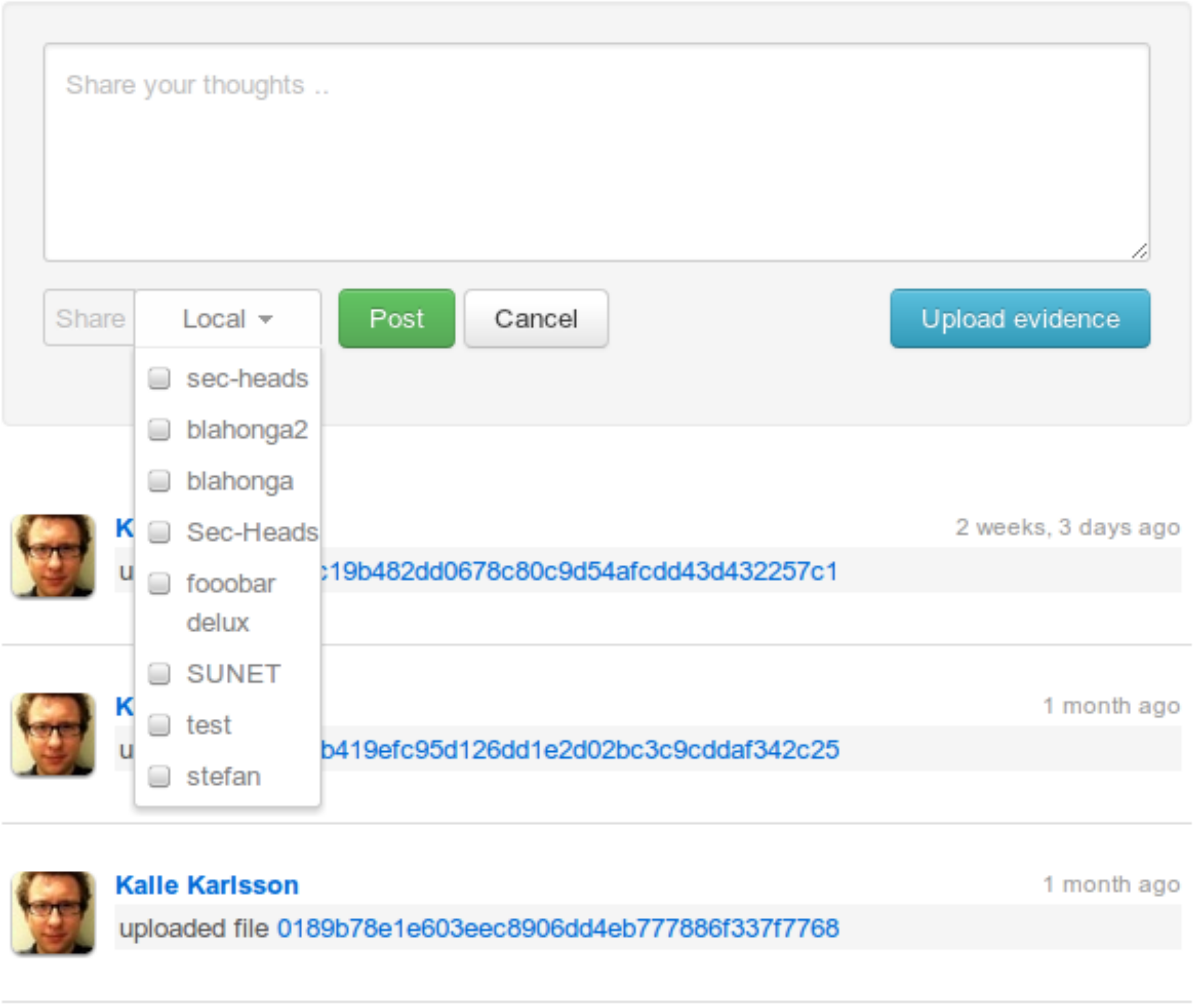
Kalle Karlsson 1 month ago
uploaded file e41ffeebbf9ff3a4b2d53aa7870e467e2a25627b

Kalle Karlsson 1 month ago
New post

But it can do much more...
It's up to you to discover what and how.

Some of the results that Cuckoo generates are

Message dissemination

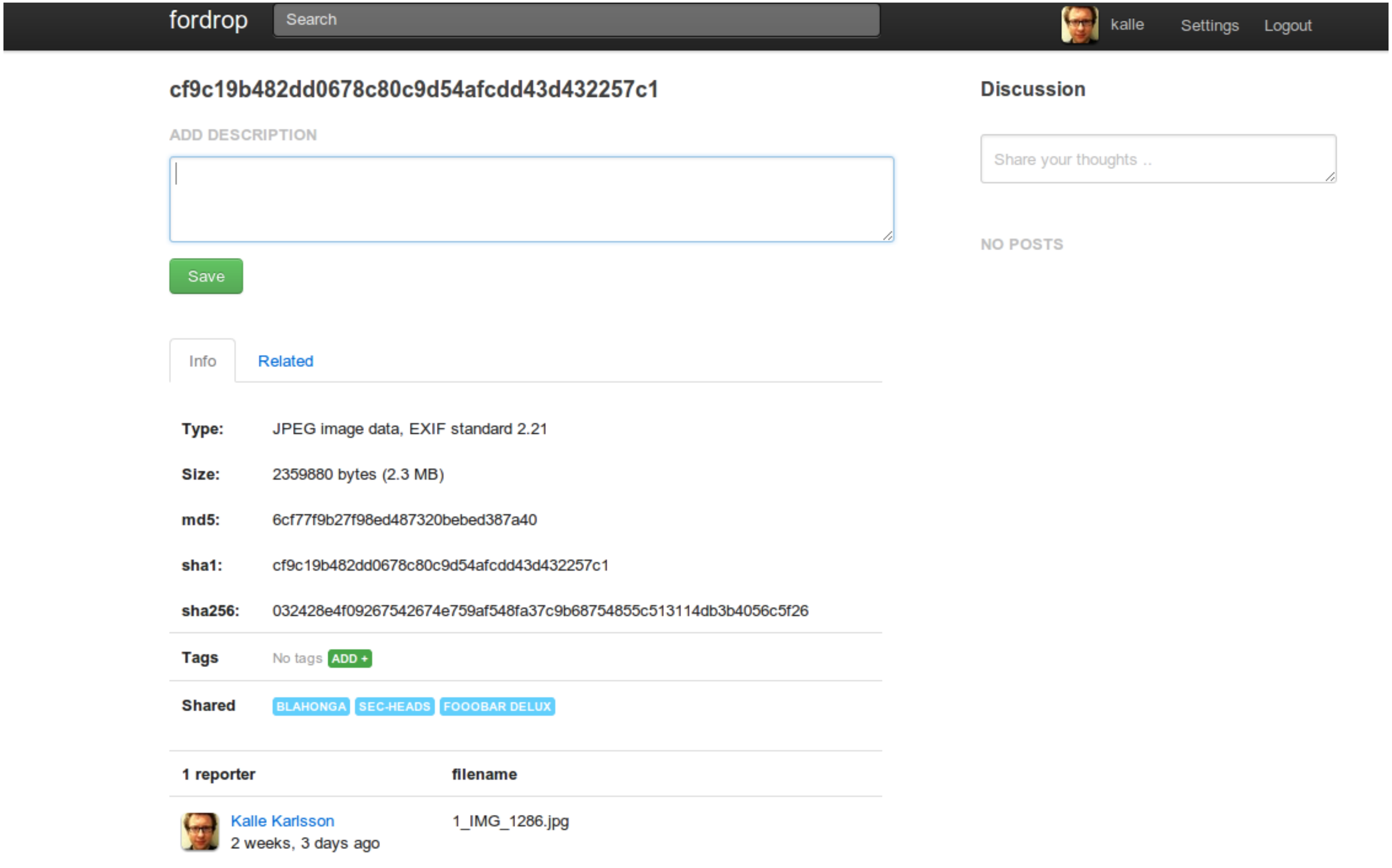


K 2 weeks, 3 days ago
u :19b482dd0678c80c9d54afcdd43d432257c1

K 1 month ago
u b419efc95d126dd1e2d02bc3c9cddaf342c25

Kalle Karlsson 1 month ago
uploaded file 0189b78e1e603eec8906dd4eb777886f337f7768

Message details



cf9c19b482dd0678c80c9d54afcdd43d432257c1

ADD DESCRIPTION

Type:	JPEG image data, EXIF standard 2.21
Size:	2359880 bytes (2.3 MB)
md5:	6cf77f9b27f98ed487320bebed387a40
sha1:	cf9c19b482dd0678c80c9d54afcdd43d432257c1
sha256:	032428e4f09267542674e759af548fa37c9b68754855c513114db3b4056c5f26
Tags	No tags
Shared	BLAHONGA SEC-HEADS FOOOBAR DELUX

1 reporter	filename
Kalle Karlsson 2 weeks, 3 days ago	1_IMG_1286.jpg

Discussion

Share your thoughts ..

NO POSTS

Trouble ticket developments

- Building on Fordrop to automate trouble ticket dissemination
- Done so far
  - RSS to Activity stream translator
  - Correlation of two different activity streams
- Next step
  - Create a module to automatically create/ update/close tickets in RT

What makes this succeed?

- Based on open standards
  - Activity streams is widely adopted (e.g. by Facebook and Google)
  - Several ticket systems already support RSS feeds
  - Many organisations already have their own XMPP servers
- More and more organisations are restructuring their ticket systems and introducing more structured data

Interested?

- Think this is a good idea and want to help this initiative?
    - Let us know what kind of fields you have in your ticket system
    - Turn on a RSS feed from your system that we can experiment with

Conclusions

- We are still using the same method to disseminate information as the 1970's
- Current solutions makes coordination very challenging
- We now have the standards and technology to make something better
- You can with make a difference!

Questions?

stefan@nordu.net