



Toolforge webservices are in the final stages of [migrating to the toolforge.org domain](#).
Please help us clean up older documentation referring to tools.wmflabs.org!

Incident documentation/20180711-fundraising undeliverable mail

[< Incident documentation](#)

root@ account was mercilessly spammed by bounces from full fr-tech@ box

Contents [hide]

- 1 [Summary](#)
- 2 [Timeline \(UTC\)](#)
- 3 [Conclusions](#)
- 4 [Actionables](#)

Summary

Fundraising was running a "Big English test" which means banners on English wikis and heavy donation traffic. An error in the Amazon Pay integration lead to an email alert per donation, which quickly overwhelmed delivery.

Timeline (UTC)

- 15:00 banners go up, failmail starts rolling in to fr-tech@
- 15:30 based on the error Casey assumes the firewall needs a hole
- 15:36 Manuel alerts Casey that the root@ alias is getting mail about bounces to fr-tech@
- 16:00 Arzhel deploys Casey's erroneous firewall config, Casey chases tail
- 17:00 Arzhel points out that he cannot connect to the IP from his laptop, indicating the firewall is not the issue
- 18:00 further investigation with fr-tech seems to confirm that Amazon was advertising broken endpoints
- 20:00 Elliott discovers that the error message was misleading and not reporting the endpoint IP after all
- 20:30 Elliott finds the actual timeout was to <http://sns.us-east-1.amazonaws.com/> to retrieve the session certificate
- 20:35 Casey finds the changed IP for that URL has not been whitelisted in local iptables (pfw was not the problem)

Conclusions

- I (Casey) should have a better grasp on the firewalls. This was a good learning opportunity.
- We have had problems for years with Amazon changing IPs (T119002). Most of it was resolved by using a proxy IP they created for us (T176654). However the certificate retrieval URL has up to now not been manually resolved to it.
- The Amazon integration had rusted since last use and should have been kicked, either by a manual test or an automatic check, before being turned on full steam.
- The fr-tech email alert system should be smart enough to not send 1000s of the same message at once.

Actionables

- Try using our proxy IP for the cert URL: [phab:T199382](#)
- Create further health checks for PSP endpoints: TBD, I think there are tasks for this already, combing Phab
- Throttle failmail before this happens: [phab:T161567](#)

Category: [Incident documentation](#)

[Main page](#)
[Recent changes](#)
[Server admin log \(Prod\)](#)
[Server admin log \(RelEng\)](#)
[Deployments](#)
[SRE/Operations Help](#)
[Incident status](#)

[Cloud VPS & Toolforge](#)

[Cloud VPS documentation](#)

[Toolforge documentation](#)

[Request Cloud VPS project](#)

[Server admin log \(Cloud VPS\)](#)

[Tools](#)

[What links here](#)

[Related changes](#)

[Special pages](#)

[Permanent link](#)

[Page information](#)

[Cite this page](#)

[Print/export](#)

[Create a book](#)

[Download as PDF](#)

[Printable version](#)

