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

Incident documentation/20160606-otrsmail

< Incident documentation

Contents [hide]

Summary

A broken clamav update prevented mail delivery on ticket.wikimedia.org (OTRS) for about 11 hours. The new clamav package deprecated a config option, but if that option is still present (which was the case in our puppetised config), clamd and freshclam refuse to start. No mail was lost, the queue was processed once the option was removed.

Timeline

- 08:39: Moritz deploys the new clamav version as part of the jessie 8.5 point release
- 18:55: The error is reported by an OTRS admin in wikimedia-tech
- 19:14: Alex M pokes ops, Rob and Brandon start investigating
- 19:44: Brandon deploys a hotfix (and one verified via puppet)

Conclusions

- Monitoring didn't spot the error, the "OTRS Icinga" check didn't flag an error and we're missing Icinga checks for ClamAV and FreshClam
- The problematic behaviour wasn't noticed before deploying the update, all further ClamAV updates need more scrutiny (ClamAV is handled differently in Debian compared to other packages: Due to sometimes nontransparent security changes clamav is always updated to the latest version instead of applying isolated changes. Also, virus pattern updates often need newer scan engine features)

Actionables

- Status: **Unresolved** Icinca checks for ClamAV and FreshClam, double check OTRS Icinga plugin behaviour if ClamAV fails (bug T137188)
- Status: **Unresolved** Debian update to handle the presence of AllowSupplementaryGroups gracefully (https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=826607)

Category: Incident documentation