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

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/20190603-eqiad-port-saturation

< Incident documentation

Contents [hide]

Summary

We received a LibreNMS alert for port utilization over 80% on cr2-eqiad.wikimedia.org in xe-3/3/3 interface.

After some investigation, we identified a single client running in AWS performing multiple requests for media content using "User-Agent: python-requests".

Impact

No user-facing impact.

Detection

LibreNMS alert on #-operations

Timeline

(In UTC)

- 12:23: <librenms-wmf> Critical Alert for device cr2-eqiad.wikimedia.org - Primary outbound port utilisation over 80%
- 13:22: faidon@weblog1001:/srv/log/webrequest$ head -n 2560000 sampled-1000.json | jq -r '.ip + " " + (.response_size | tostring)' | awk '{ sum[$1] += $2 } END { for (ip in sum) print sum[ip],ip }' |sort -nr | head -10
- 13:35: cdanis opens abuse report with AWS abuse team
- 13:50: crawler begins scraping larger objects again, network usage increases to max
- 14:00: ema merges https://gerrit.wikimedia.org/r/#/c/operations/puppet/+/514005/ to block their User-Agent (also unavoidably blocking some legitimate traffic)
- 14:01: ema runs puppet on cp1084
- 14:05: outbound network returns to normal

Actionables

- phab:T224884 - Rate limit requests to cache_upload
- phab:T224888 - Network port saturation should page
- phab:T224891 - Return HTTP 403 to requests violating User-Agent policy
- Begin enforcing our existing meta:User-Agent policy, after notifying community (TODO: file task). Some summary of discussion:
  - Ratelimit/block 'default' UAs, like "curl", "python-requests", "python-urllib2", etc.
    - Probably allow only so many reqs/sec from a given IP for these 'default' ones
  - First investigate how much traffic this would hurt
  - wikitech-l@, mediawiki-api-announce@, and m:Tech/News are reasonable venues for announcements

Category: Incident documentation

This page was last edited on 4 June 2019, at 06:33.