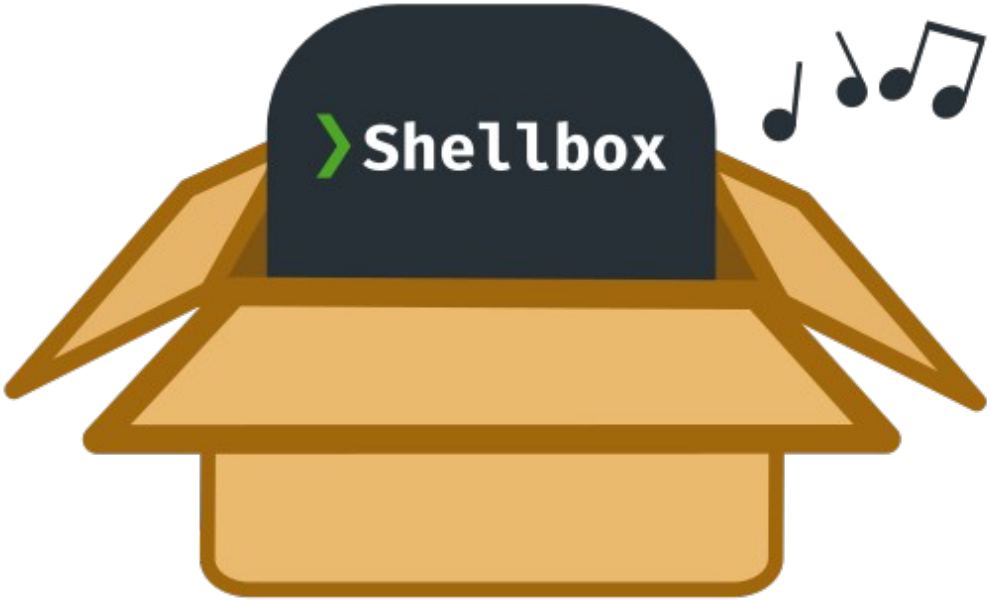


November 2021

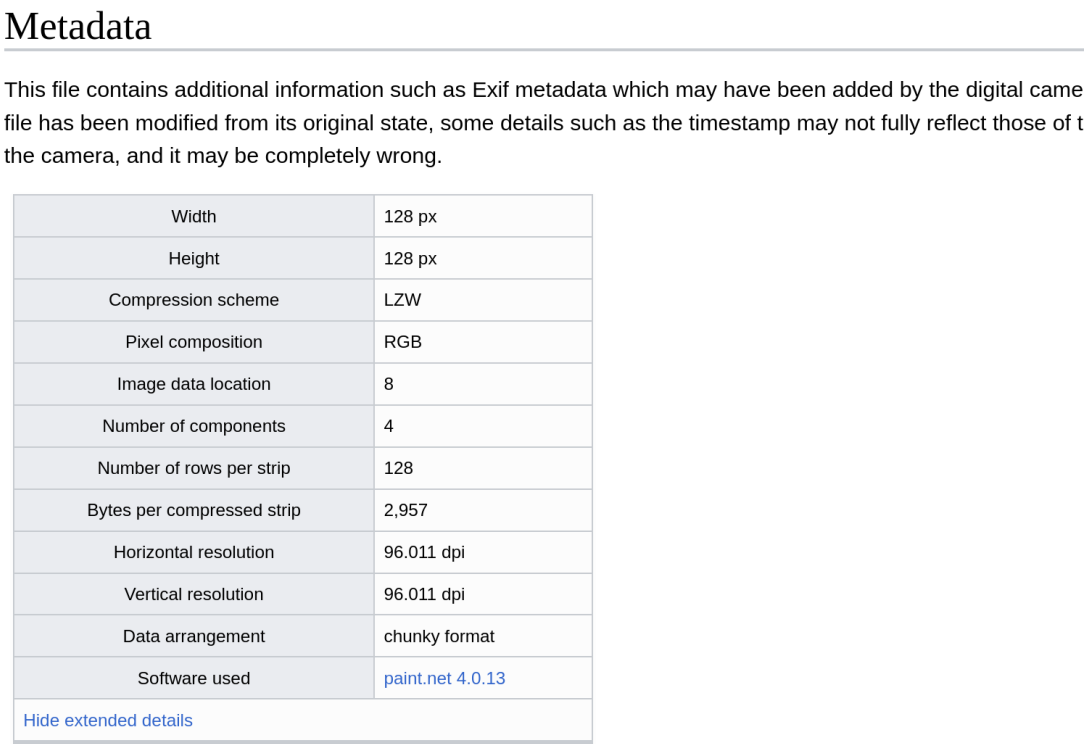
Logo by Thcipriani, CC-BY-SA 4.0

What shell outs?

- Media handling: metadata extraction and (formerly) thumbnailing
- Timelines
- Syntax highlighting
- Musical scores!

Media handling

- djvulibre-bin
- libtiff-tools
- poppler-utils (PDF)



Metadata

This file contains additional information such as Exif metadata which may have been added by the digital came
file has been modified from its original state, some details such as the timestamp may not fully reflect those of t
the camera, and it may be completely wrong.

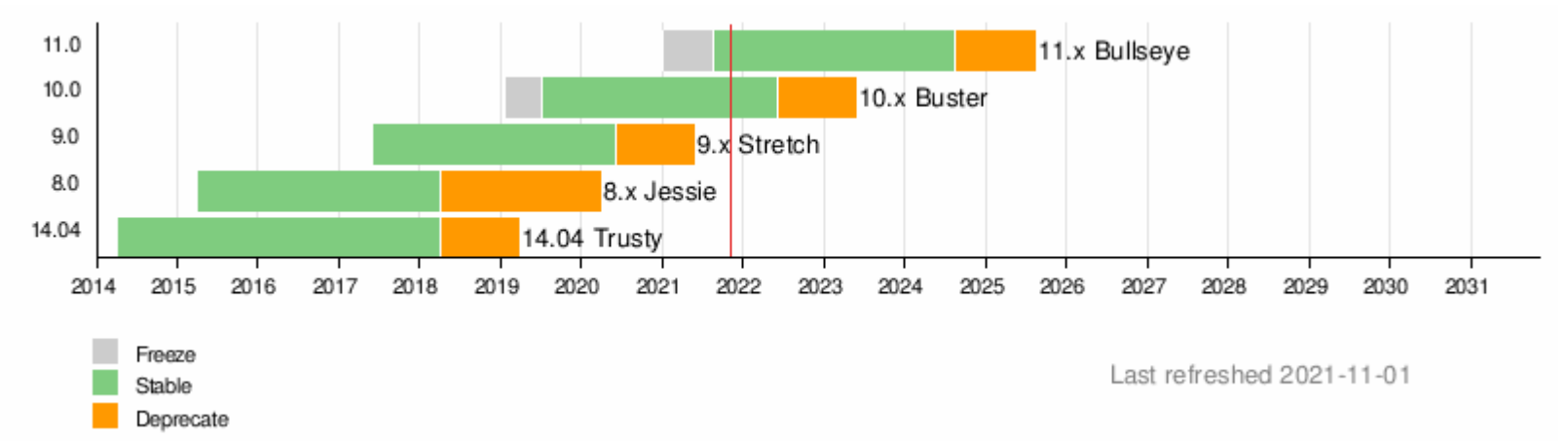
Width	128 px
Height	128 px
Compression scheme	LZW
Pixel composition	RGB
Image data location	8
Number of components	4
Number of rows per strip	128
Bytes per compressed strip	2,957
Horizontal resolution	96.011 dpi
Vertical resolution	96.011 dpi
Data arrangement	chunky format
Software used	paint.net 4.0.13

Hide extended details

https://commons.wikimedia.org/wiki/File:Example.tiff

Timelines

- Perl script: EasyTimeline.pl
- Calls ploticus and librsvg



https://wikitech.wikimedia.org/wiki/Operating_system_upgrade_policy

Syntax highlighting

- Pygments (Python)
- Formerly in PHP with GeSHi

```rust
fn factorial(i: u64) -> u64 {
    match i {
        0 => 1,
        n => n * factorial(n-1)
    }
}
```

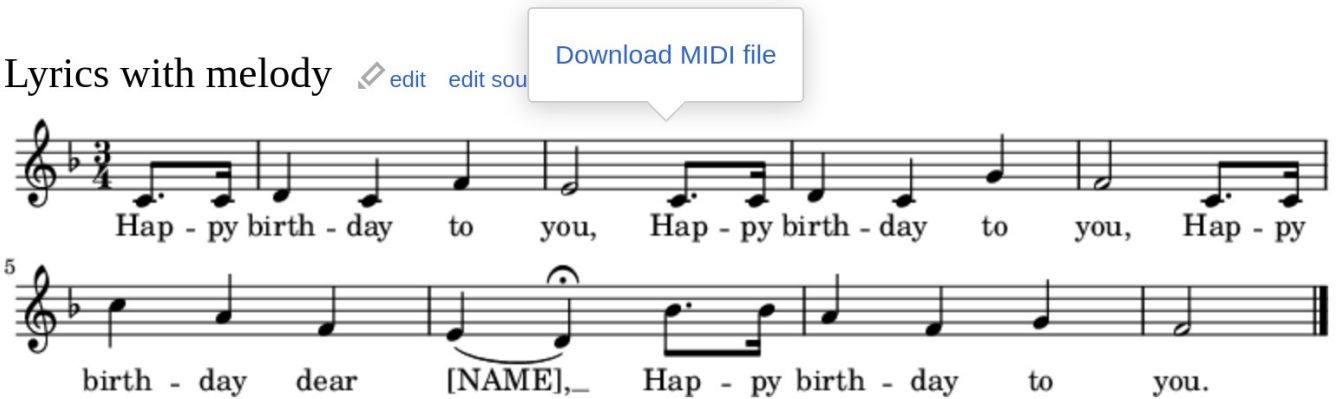
The following iterative implementation uses the `..=` operator to cr

```rust
fn factorial(i: u64) -> u64 {
    (2..=i).product()
}
```

https://en.wikipedia.org/wiki/Rust_(programming_language)

Musical scores

- LilyPond, imagemagick, ghostscript, fluidsynth, lame
- LilyPond safe mode has limited features



https://en.wikipedia.org/wiki/Happy_Birthday_to_You

LilyPond security issues

- July 2020, security report of RCE via Score
- firejail containment wasn’t active because of configuration typo
- After being disabled, investigation found more issues in LilyPond and firejail

LilyPond security issues

- CVE-2020-17353: LilyPond allows arbitrary PostScript and doesn’t use -dSAFER
  - MediaWiki now calls ghostscript directly
- CVE-2020-17354: safe mode escape (undisclosed/unfixed)
- T260225: safe mode escape (undisclosed/unfixed)

firejail security issues

- CVE-2020-17367, CVE-2020-17368: Vulnerabilities in firejail due to --output
  - MediaWiki errors if someone tries to use --output as a CLI arg
- PHP-FPM socket inside sandbox, allows for escape

Re-evaluate sandboxing

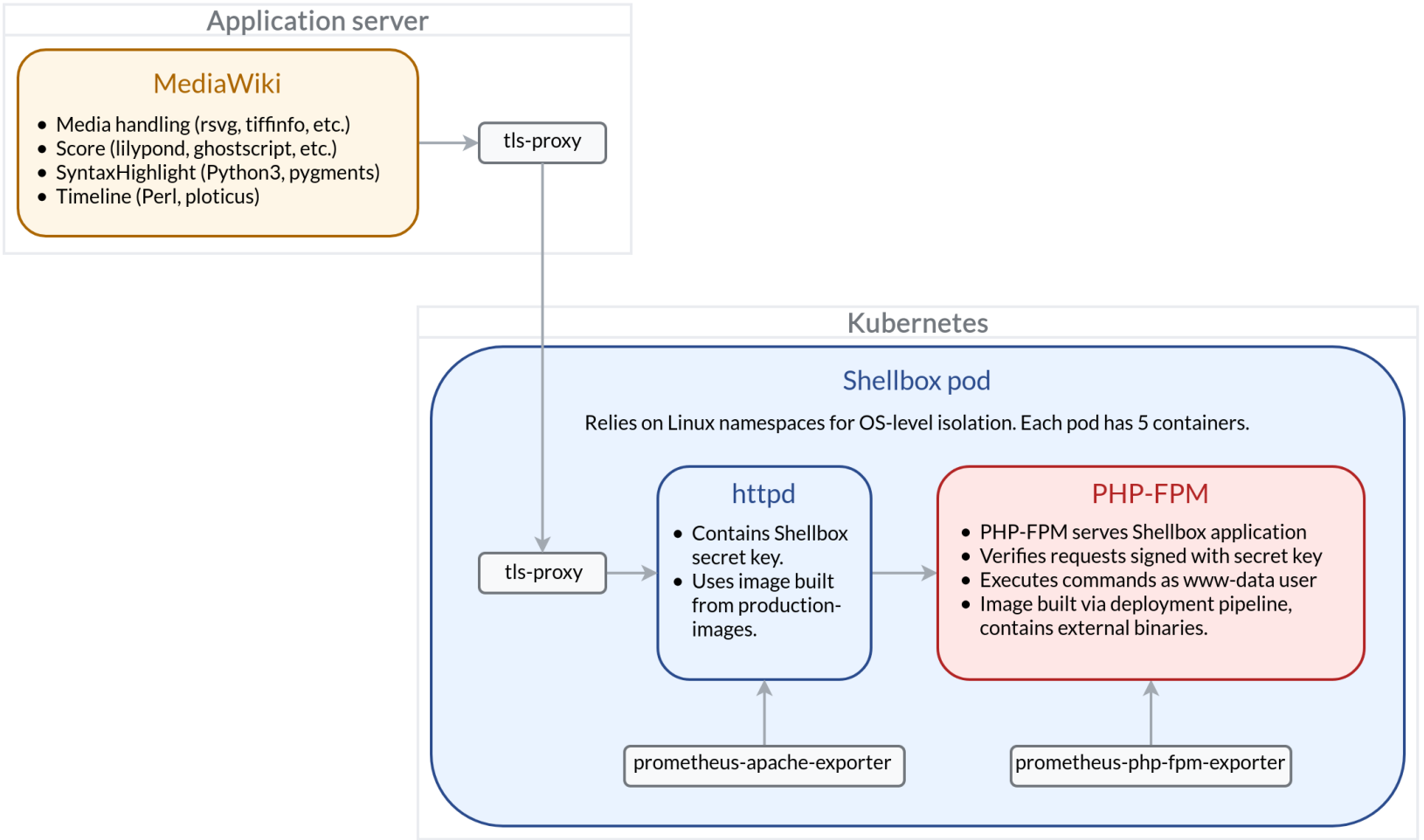
- LilyPond upstream tried to implement a seccomp sandbox, gave up
- T257090 (private) has Tim’s security review of LilyPond and firejail. Conclusion is to use OS-level isolation.
- For Kubernetes, did not want to do shellouts in the container

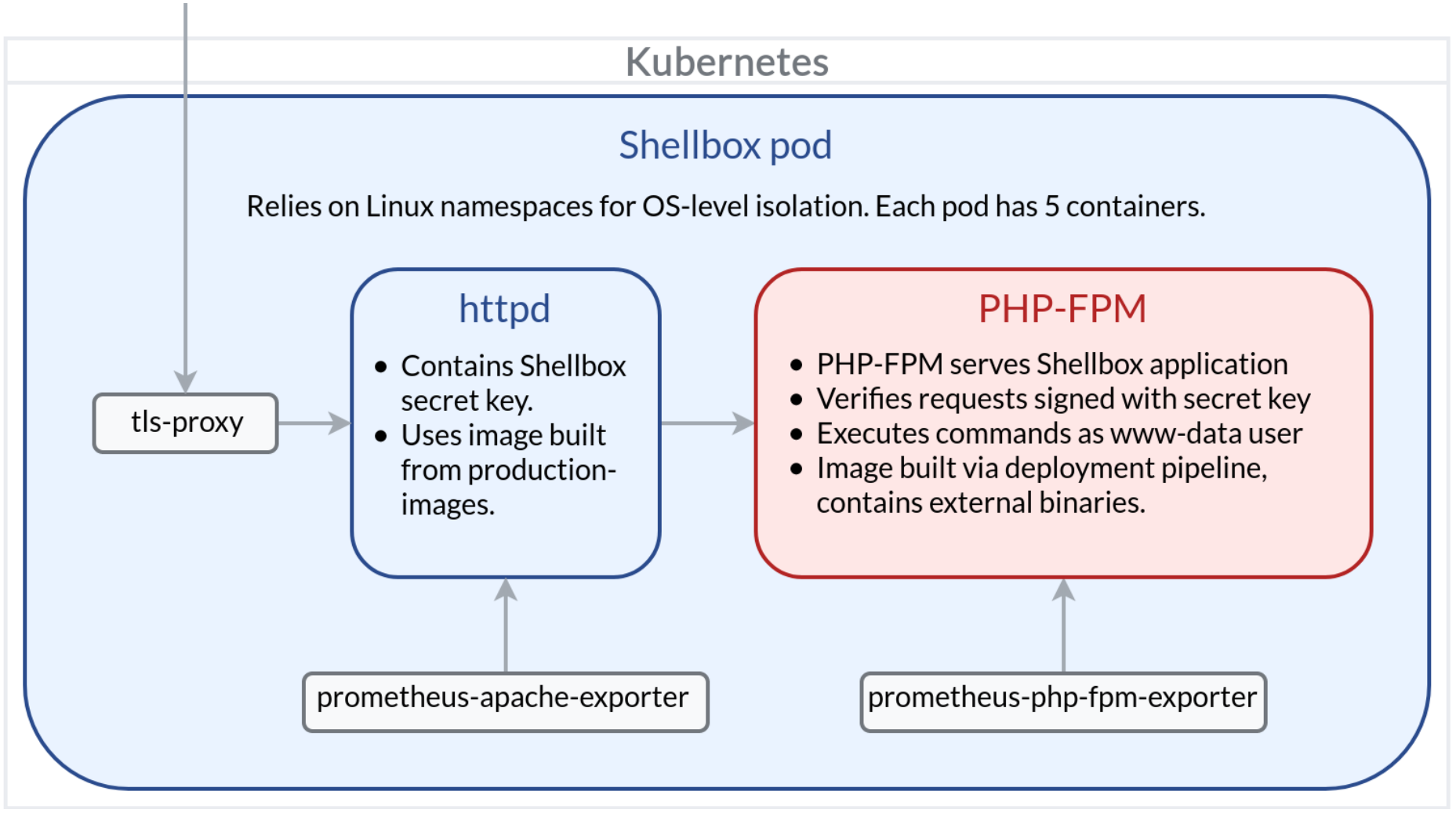
Enter Shellbox

- T260330: RFC: PHP microservice for containerized shell execution
- Survey of all callers to figure out needs
- limit.sh, firejail, systemd, or remote container
- API to send/receive files transparently
- Lightweight PHP-RPC interface

Shellbox overview

A server for secure command execution, August 2021.

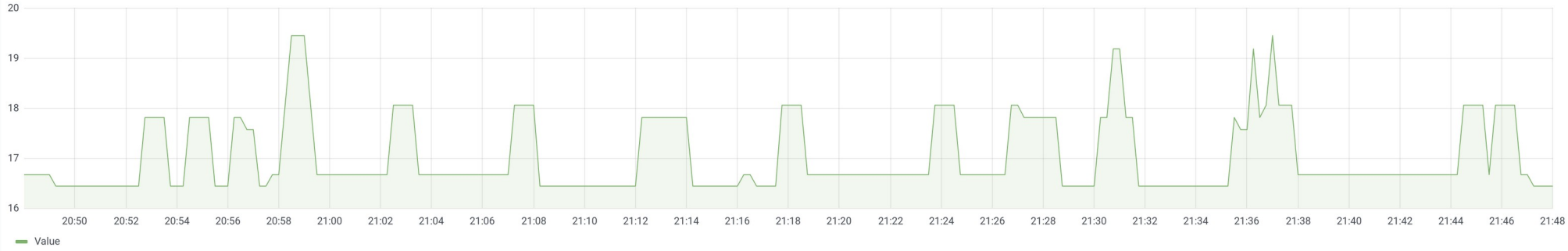



Kubernetes
Shellbox pod
Relies on Linux namespaces for OS-level isolation. Each pod has 5 containers.
tls-proxy
httpd
Contains Shellbox secret key.
Uses image built from production-images.
PHP-FPM
PHP-FPM serves Shellbox application
Verifies requests signed with secret key
Executes commands as www-data user
Image built via deployment pipeline, contains external binaries.
prometheus-apache-exporter
prometheus-php-fpm-exporter

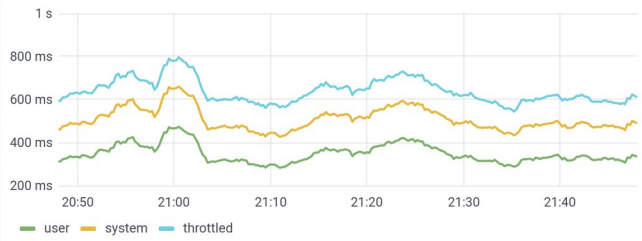
Service / Shellbox

Last 1 hour UTC

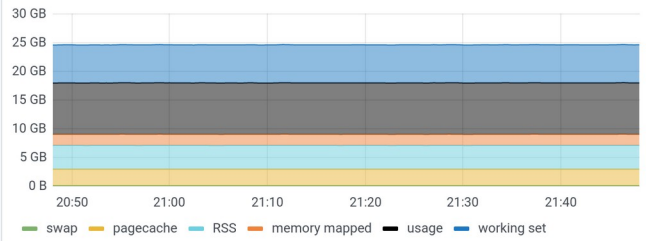
php-fpm workers saturation



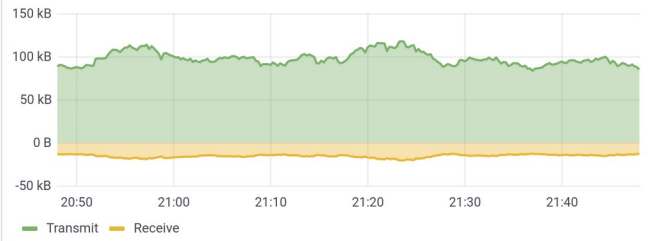
Total CPU



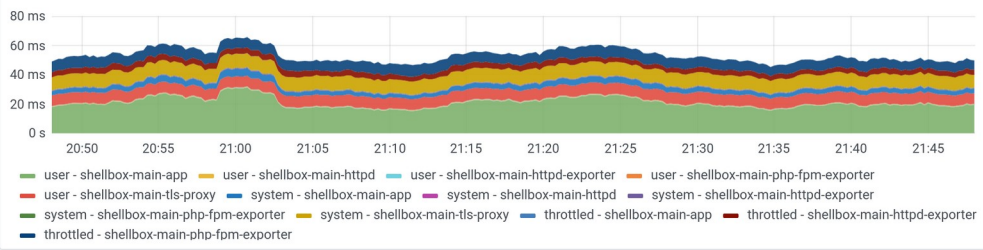
Total Memory



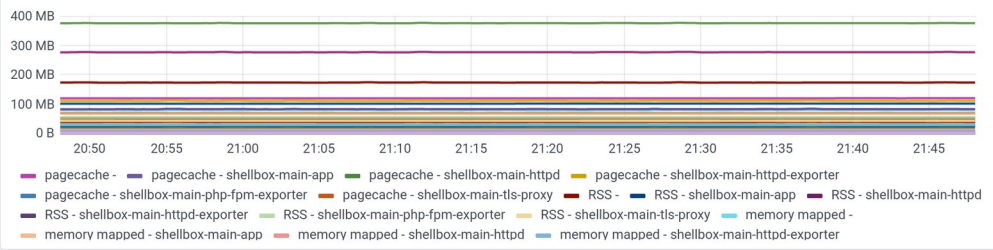
Total Network



avg CPU per container name



avg by container name memory usage



Top 5 pods CPU (current)

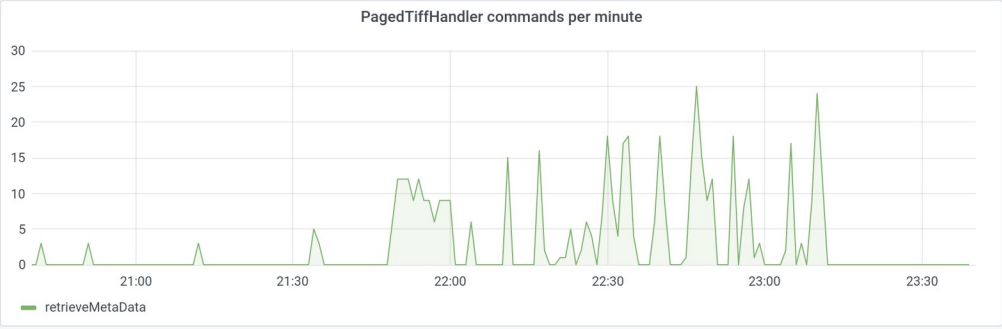
Top 5 pods Memory (current)

Top 5 pods network in/out (current)

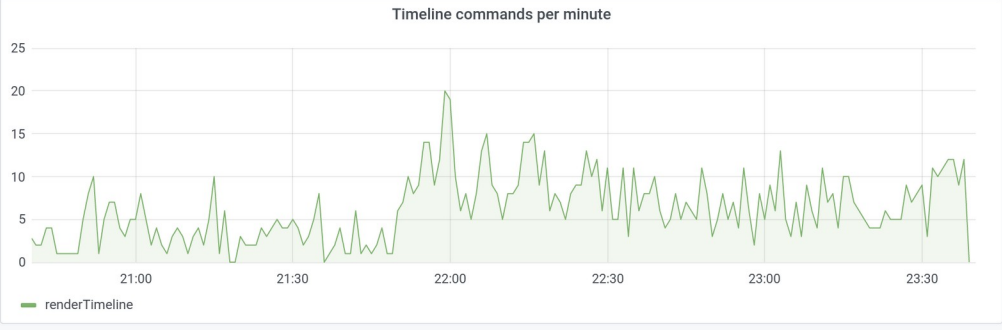
Application Servers / MediaWiki shellouts

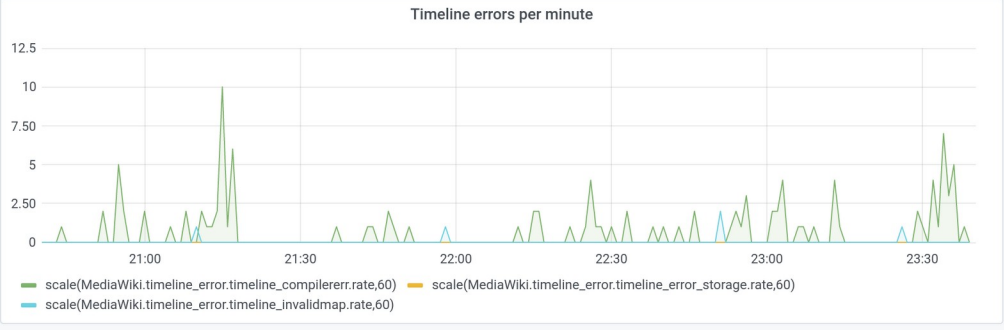
Last 3 hours UTC | 30s

PagedTiffHandler

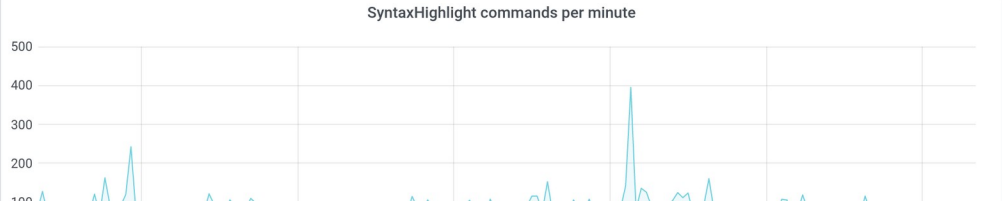


Timeline (ploticus)





SyntaxHighlight (pygments)



Shellboxes

- shellbox – Score
- shellbox-constraints – evaluates PCRE regexes for Wikidata Constraints checking
- shellbox-media – file metadata
- shellbox-syntaxhighlight
- shellbox-timeline

Not migrated

- SecurePoll: Shells out to gnupg1, hopefully will switch to OpenSSL/libsodium: T209892
- Videoscalers: Needs dedicated plan
-

Limitations

- Vulnerable to Kernel/Kubernetes/Docker/etc. escapes
- Containers are not ephemeral, possible cross-channel leaks (Score disabled on private wikis)
- No extra isolation within Kubernetes cluster

Documentation

- https://www.mediawiki.org/wiki/Shellbox (general overview, local dev setup)
- https://wikitech.wikimedia.org/wiki/Shellbox (deployment information)
- https://www.mediawiki.org/wiki/Manual:BoxedCommand (how to use in MediaWiki)
- https://www.mediawiki.org/wiki/Extension:Score/2021_security_advisory
-