PAGs. . . Unthrottled

Andrew Deason

June 2021

OpenAFS Workshop 2021

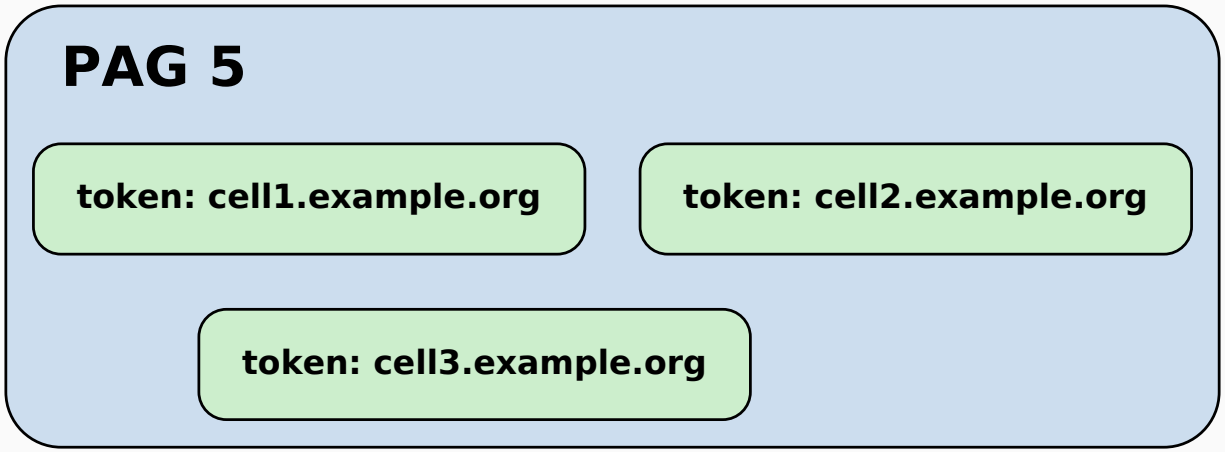
Preamble

- Background: PAGs
- PAG throttling
- Unthrottled PAGs

Speedometer icon by MD Badsha Meah: https://freeicons.io/business-set-1/ (icon 38103)

What is a PAG? (Process Authentication Group)

- "A miserable little pile of ~~secrets~~ tokens"
- AFS client token storage
- Without PAGs, creds are uid-based

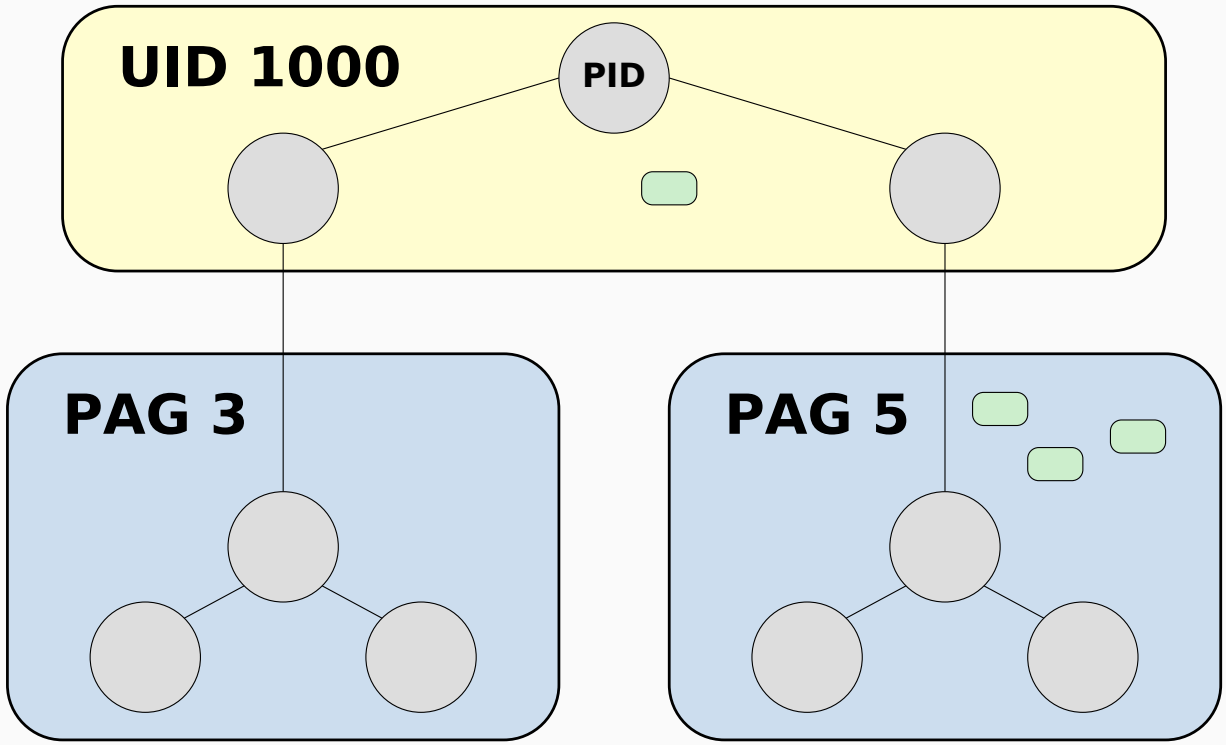


Why PAGs?

- More control over creds/identity
- No PAGs, same uid? Same tokens
  - Daemons
  - Separate user sessions (e.g. ssh)
  - Switching creds
- Need more containers: PAGs

What is a PAG?

- At most 1 PAG per pid (not per-thread)
- Child pid stays in same PAG
- Create new PAGs with `pagsh`
- Non-hierarchical



PAG IDs

- How do we track PAGs?
  - Kernel facility (AIX)
  - Groups (Solaris)
  - Keyrings (Linux)
  - N/A (macOS)
- Need an ID (PAG 3, PAG 5, etc)
- Anyone can create many PAGs

```
$ id -G
1001
$ pagsh
$ id -G
1001 1100805323
$ pagsh
$ id -G
1001 1100805324
```

PAG ID Collisions

- Collisions mean stealing credentials
- Why not skip over used PAG IDs?
- Historically, hard to accurately track used PAGs
  - Cross-platform
  - Iterating over pids
  - Checking grouplists
- Instead, just alloc/free PAGs based on tokens

PAG Throttling

- To limit collisions, throttle PAGs
- Not perfect, collisions still possible
- Cannot create many PAGs at startup

```
$ pagsh
[...]
$ dmesg | tail -n 1
[3889227.586299] afs_pag_wait() PAG throttling triggered, pid 27030... sleeping.  sleepcnt 0
```

Unthrottled PAGs

- On Linux, we *do* have accurate tracking
  - Kernel keyrings
  - We know when a PAG goes away
  - Technically don't even need IDs
- A SMOP later, and we can skip in-use PAGs
- No more throttling
- Linux-only for now

Other PAG Possibilities

- Dropping PAGs
  - But what if the non-PAG uid has more privs?
  - Need some kind of control

- Deliberate PAG infiltration
  - Token renewing
  - New command suite? Or `fs`

Postamble

Gerrits

https://gerrit.openafs.org/#/q/topic:unthrottled-pags

Slides

http://dson.org/talks

Contact

adeason@dson.org

adeason@sinenomine.net