

Daemons, PAGs, and Automated Authentication

Russ Allbery
June 13, 2005

Contents

- Overview of tokens and PAGs
- Srvtabs and keytabs
- Issues with authenticated daemons
- Why kstart?
- PAG or not to PAG
- Single commands

Tokens and PAGs

- External program to get token
- A token is credentials shoved into the kernel
- Association is by PAG or by UID
- Without PAGs, all processes with the same UID share a token, token is not inherited across `setuid`
- Users put into PAGs by the login process
- Daemons started at boot (or from cron or atd) outside of PAGs

Srvtabs and keytabs

- Passwords stored on disk
- srvtab is K4, keytab is K5
- Keytabs are massively better, more structured
- `kinit` can obtain credentials from keytab
- Need distribution mechanism (talk for next year!)

Authenticated Daemons

- Need to obtain Kerberos credentials automatically
- Need to refresh credentials automatically
- Need to refresh tokens automatically
- Must not interfere with each other
- Must not be interfered with by users (including root)
- Application can't do any of the work

Why kstart?

- K4 `kinit` completely deficient
- K5 `kinit` much better, but `kstart` had evolved
- Runs as daemon to maintain credentials
- Forks token-getting program as needed
- Checks ticket expiration (`-H`)
- Can run command with credentials, PAG
- `k4start` and `k5start`
- Similarities to Heimdal `kcm`

kstart Example (daemon)

```
exec /usr/bin/setuidgid www-data /usr/bin/k5start \  
-t -l 10h -K 30 -f /etc/srvtab.www \  
-k /var/run/web/www.k4.tgt service.www
```

PAG or not to PAG

- In a PAG is safest, keeps everything isolated
- Keeps too much isolated – `kstart` or equivalent needs to be in the same PAG
- Harder to monitor/restart `kstart`
- Not in a PAG requires special care to start
- `at now` is very useful
- `kstart` can be run from `init`
- We use djv's daemontools, requires buying into the mindset, best if run everywhere uniformly

Single Commands

- Different but related set of issues from daemons
- Always use a PAG – not colliding is even more important
- Lifetime tied to life of process, not forever – hard to predict in advance
- `kstart` tries to do all the right things
- Replacement for older `runauth` script
- Should be very simple

kstart Example (command)

```
/usr/bin/k5start -qtU -f /etc/keytab.subversion -- \  
  /usr/bin/rsync -rlt --delete /srv/svn/backups/ \  
  /afs/ir/service/pubsw/data/subversion/
```

Bonus Slide: Multiple Realms

- Problem: K5 ticket cache and multiple realms
- Solution: Realm switching aliases
- Ticket cache per realm
- Changing realms changes prompt
- Role of `k5start -H` – only reauth when needed