aehostd

The PAM/NSS service for Æ-DIR

Michael Ströder <michael@stroeder.com>

OpenLDAP Developer's Day 2018

Michael Ströder <michael@stroeder.com>

- Freelancer
- Topics the last 20 years
  - Identity & Access Management, LDAP
  - Single Sign-On, Multi-Factor Authentication
  - PKI (X.509, SSH), Applied Crypto
- Open Source / Free Software:
  Æ-DIR, OATH-LDAP, web2ldap

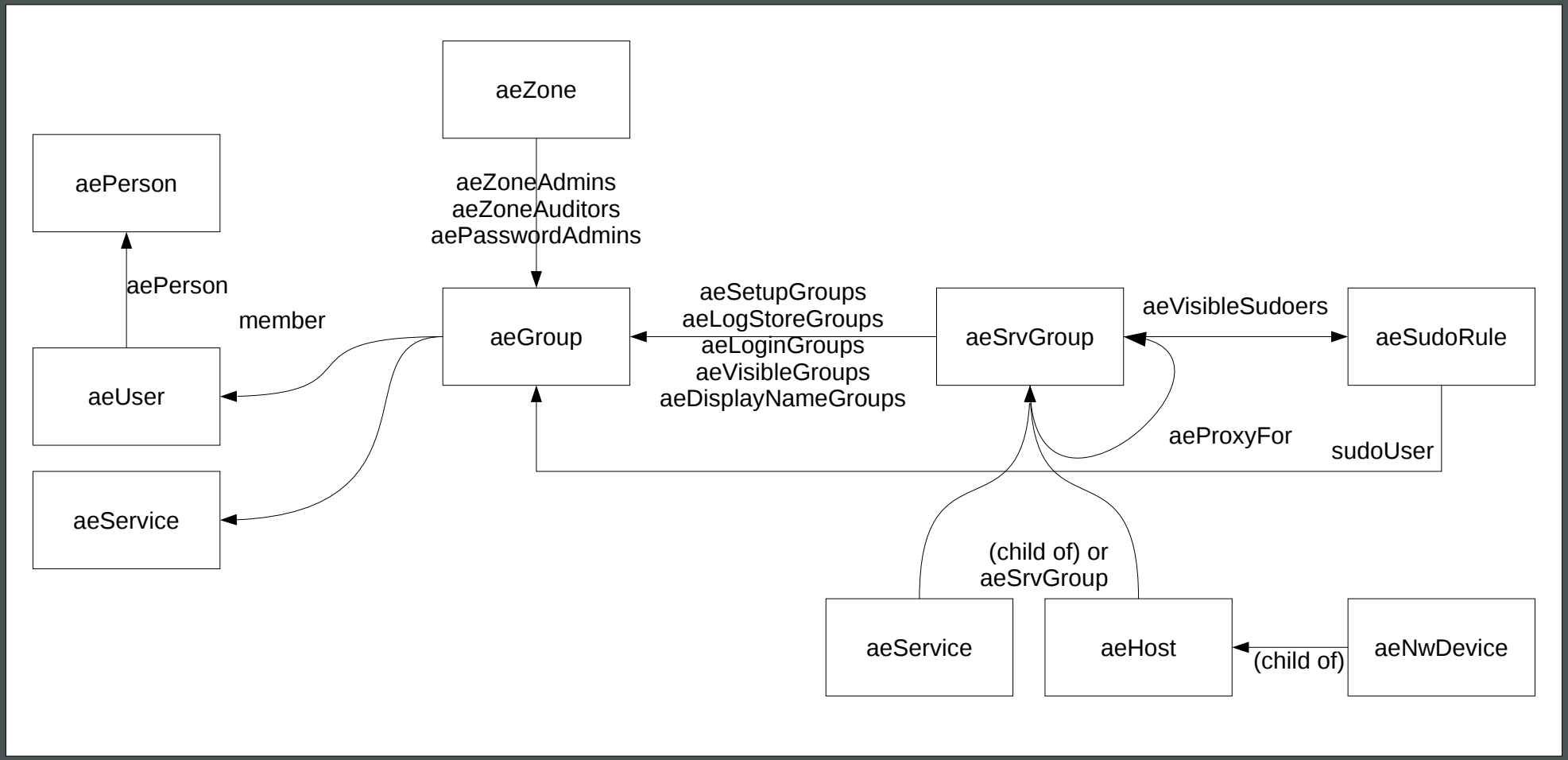
Why?

- *Æ*-DIR's slapd burns CPU cycles with set-based ACLs
- Better automated enrollment needed (host password)
- *sudo-ldap* causing lots of parallel TLS connections
- Connection behaviour unpredictable
- LDAPI support for NSS/PAM on *Æ*-DIR servers
- Fed up by asking others for simple features

Goals

- Better performance
- Better behaviour for lots of NSS clients:
  - Load-balancing
  - Update timing
- Enrollment automation with pseudo SSH login
- Simple! Less configuration, less code, less dependencies, less privileges

Data Model


aeZone
aePerson
aeZoneAdmins
aeZoneAuditors
aePasswordAdmins
aePerson
member
aeGroup
aeSetupGroups
aeLogStoreGroups
aeLoginGroups
aeVisibleGroups
aeDisplayNameGroups
aeSrvGroup
aeVisibleSudoers
aeSudoRule
aeUser
aeProxyFor
sudoUser
aeService
(child of) or
aeSrvGroup
aeService
aeHost
(child of)
aeNwDevice

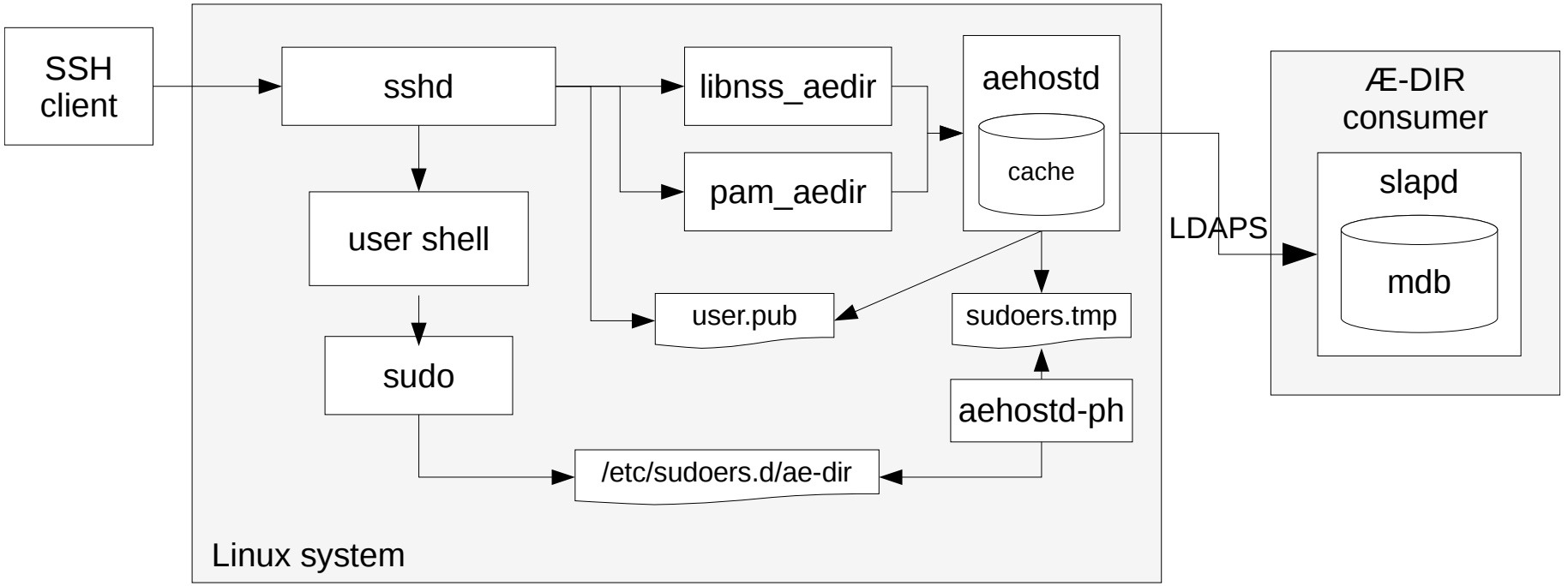
Implementation (1)

- Started with *pynslcd(8)* - rewrote completely
- Multi-threaded NSS/PAM responder based on Python's *SocketServer* module (Python 2.7)
- Main demon *aehostd* runs non-privileged
- Privileged helper *aehostd-ph* moves sudoers file and sets ownership/permissions
- sudoers.ldif is converted with *cvtsudoers* (needs sudo 1.8.23+)

Implementation (2)

- Always a single LDAP connection
- Better performance because schema is known
- Search operations follow Æ-DIR references
- Refreshing in-memory data in separate threads
  → LDAP operations do not block NSS/PAM responder
- Caching with *nscd* likely not needed

aehostd / aehost-ph



Specific Features

- Virtual groups:
  - primary user GIDs
  - role groups
- Syncing of SSH authorized keys
- LDAP session tracking control for better logging
- *hosts* map based on *aeHost* entries
- Enrollment via pseudo login with password

```
ssh aehost-init@host.example.com
```

Configuration

- LDAP URIs, trusted CA cert(s), bind-DN and password
- Separate password file
- *uri_list* vs. *uri_pool*
- Load balancing without external load balancer:
  rotate(uri_pool, hash(FQDN) mod N)
- Example on Æ-DIR servers:

```
uri_list = ldapi://
uri_pool = ldaps://ae-dir1.example.com ..
```

Installation

- *pip*-based installation (in virtual env)
- Also easy to generate Debian and RPM packages
- Front-end modules of nss-pam-ldapd:
  `./configure --with-module-name=aedir`
- Identifier *aedir* in /etc/nsswitch.conf
- ansible role *ae-dir-hostd* (site-specific variables)

Conclusion and To-Dos

- Implementation easier than expected (~20 days)
- Works just fine with systemd hardening
  Private*= Protect*= etc.
- Not yet in production
- More maps wanted?
  (pseudo netgroups, aliases, ethers)
- Docs not yet finalized but it's a start:
  https://ae-dir.com/aehostd.html

:-/

? … !