FOSDEM'18 -- Identity and Access Management devroom

Æ-DIR -- Authorized Entities Directory

from paranoid user management to secure system management

Personal info

- Michael Ströder <michael@stroeder.com>, self-employed
- IAM, PKI, etc.
- Free software
  - Æ-DIR
  - OATH-LDAP
  - web2ldap
  - formerly python-ldap

Objectives

- Strictly follow principles:
  - Need-to-know
  - Least Privilege
  - Separation of Duties
- Agile data maintenance by consequent delegation of manageable small areas
- Provide meaningful audit trails
- Solid base for compliance checks

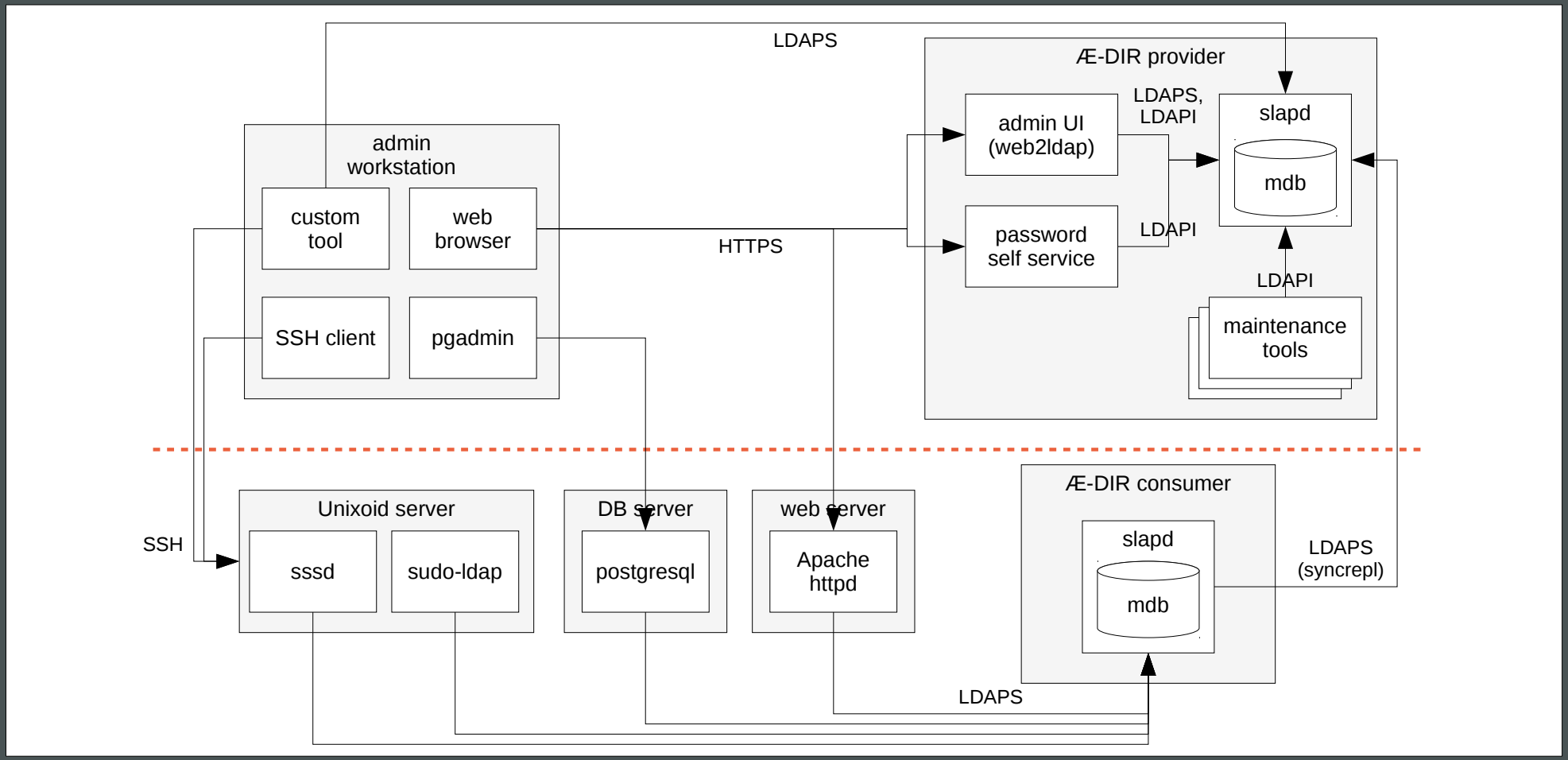
Paradigms

- Explicit is better than implicit
- Secure authorization requires secure authentication
- Individual authentication instead of shared credentials
- Avoid all-mighty proxy roles
- A person is not an user account, avoid org-based authz!
- Role separation with multiple user accounts per person
- Persistent IDs (never re-used) for reliable audit trails

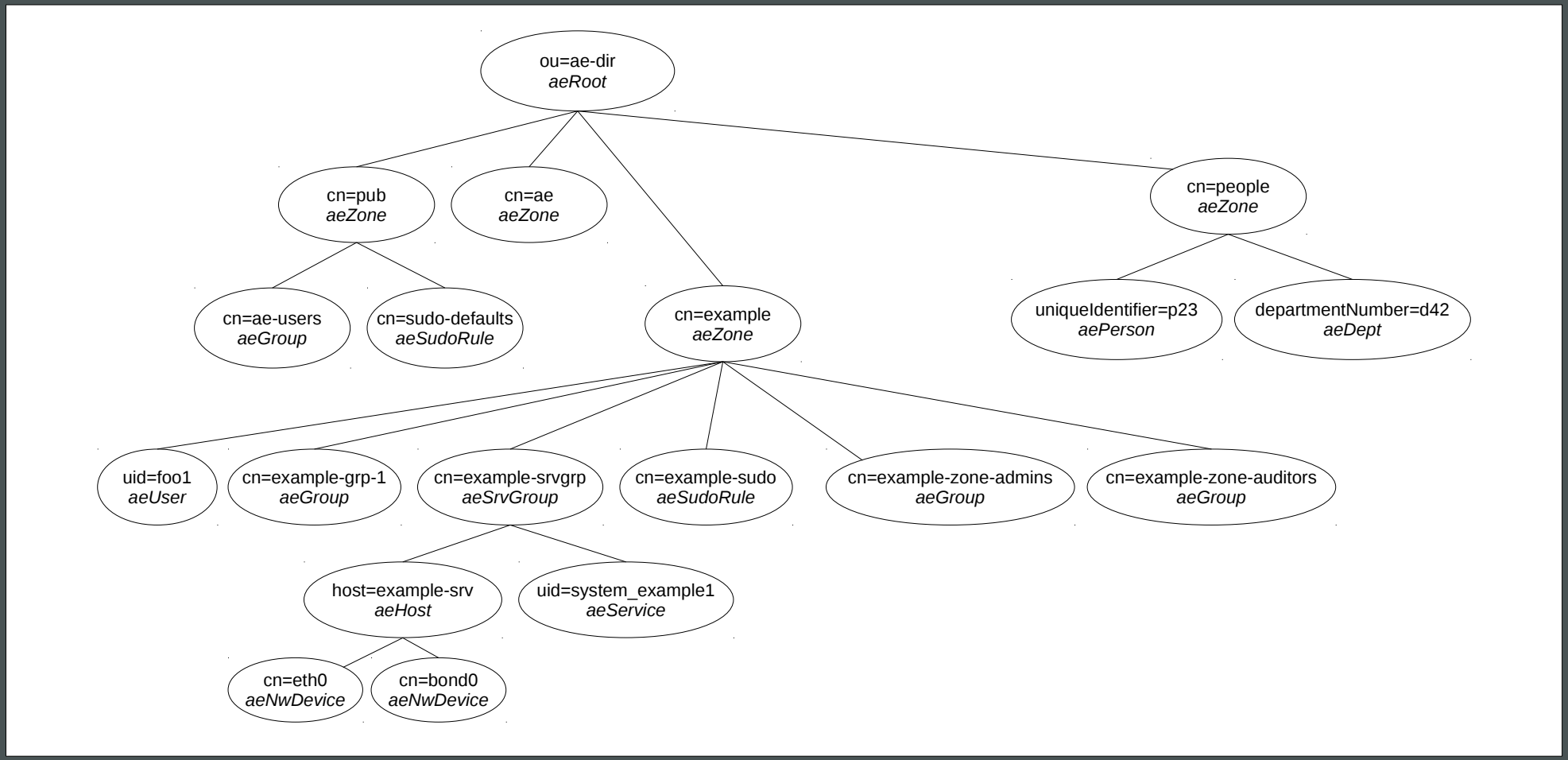
Roles

- Æ admins delegate zones, fix broken entries,
  but they do **not** maintain zones
- Æ auditors may read (almost) everything
- Zone admins are the maintainers doing the daily work
- Zone auditors may read anything within a zone
- Setup admins maintain hosts/services within service groups
- Users may read own entries, see members of own groups,
  change own password

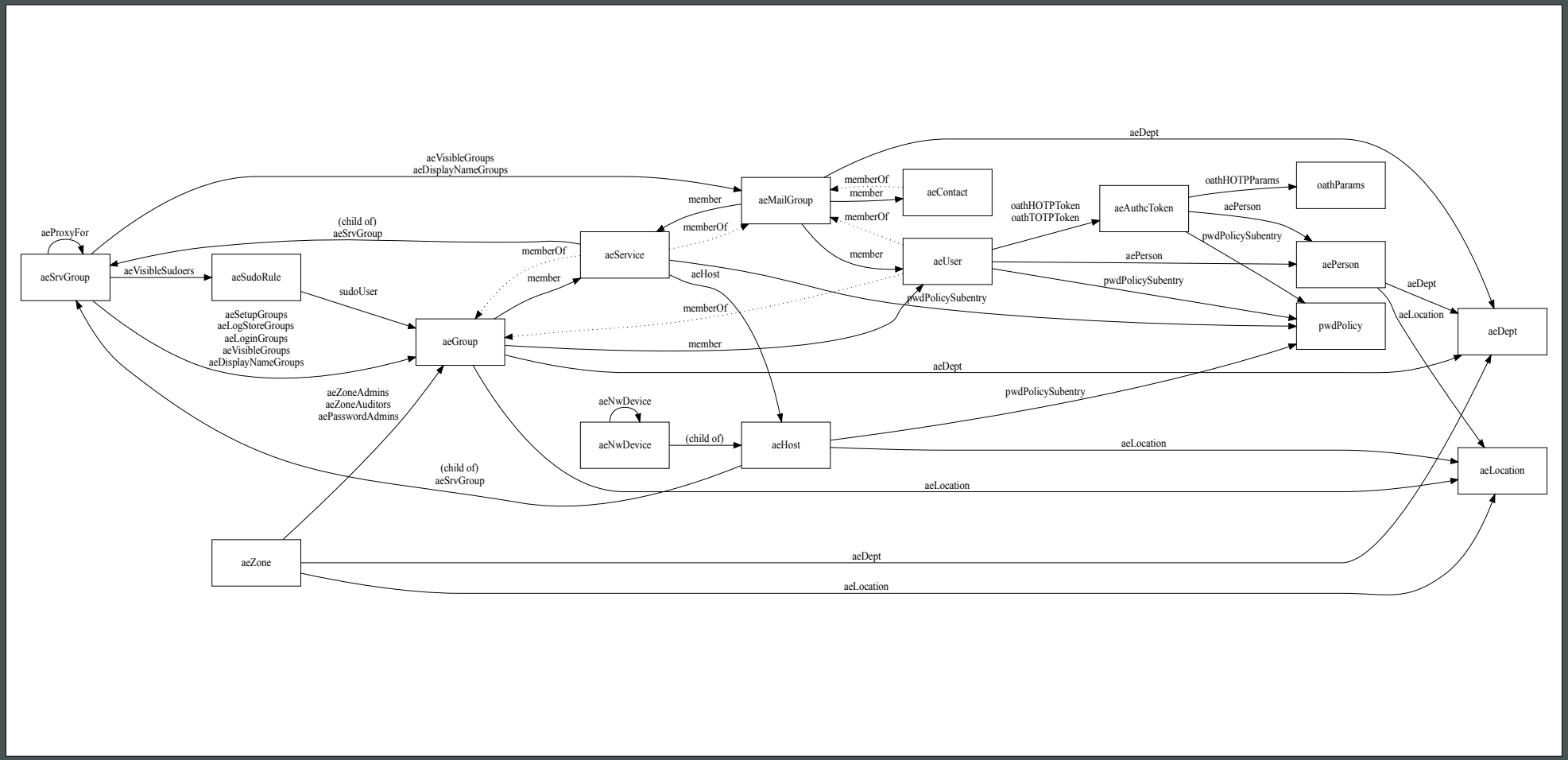
2-tier architecture



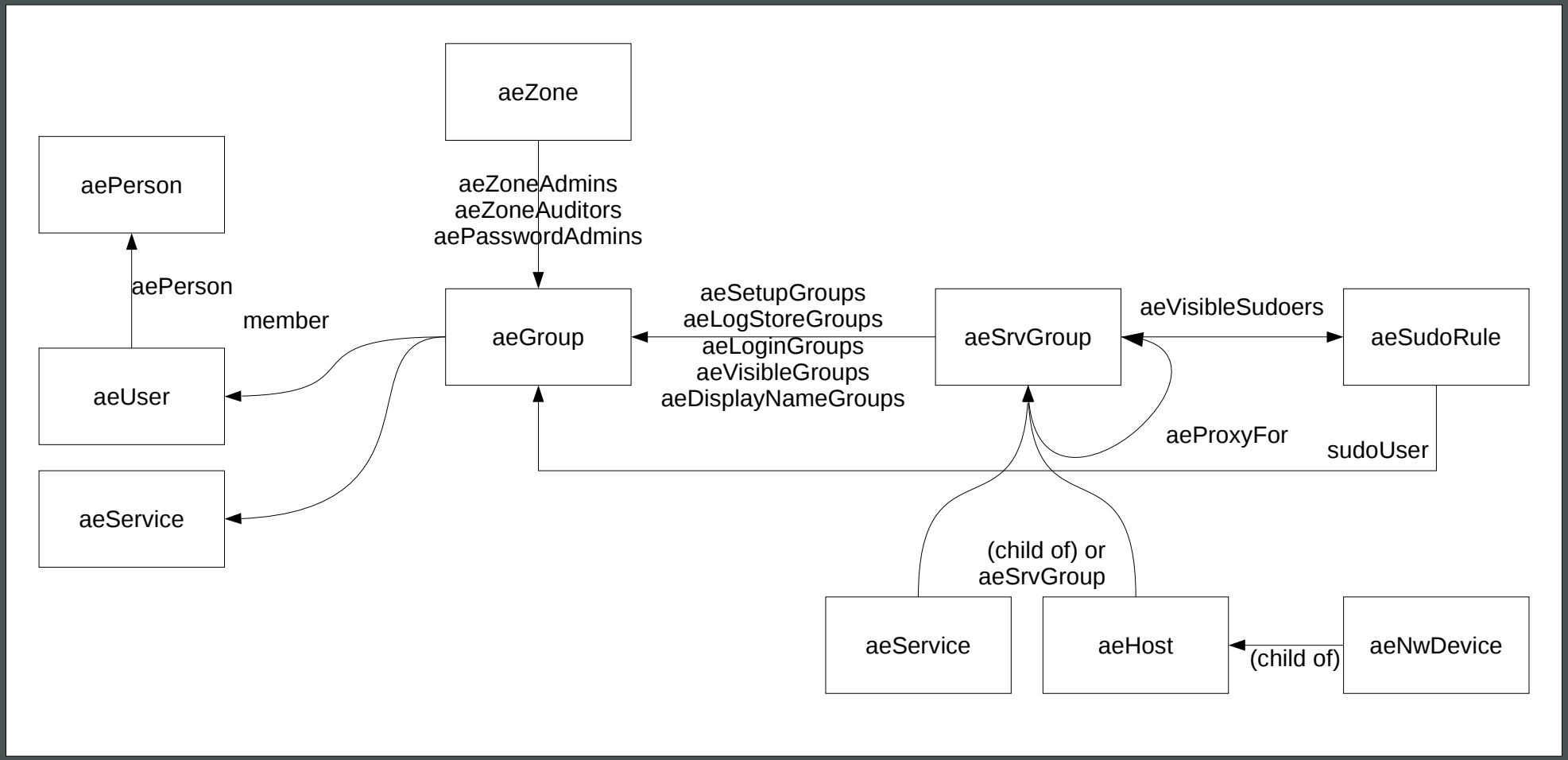
Directory Information Tree (DIT)



Complete EER diagram



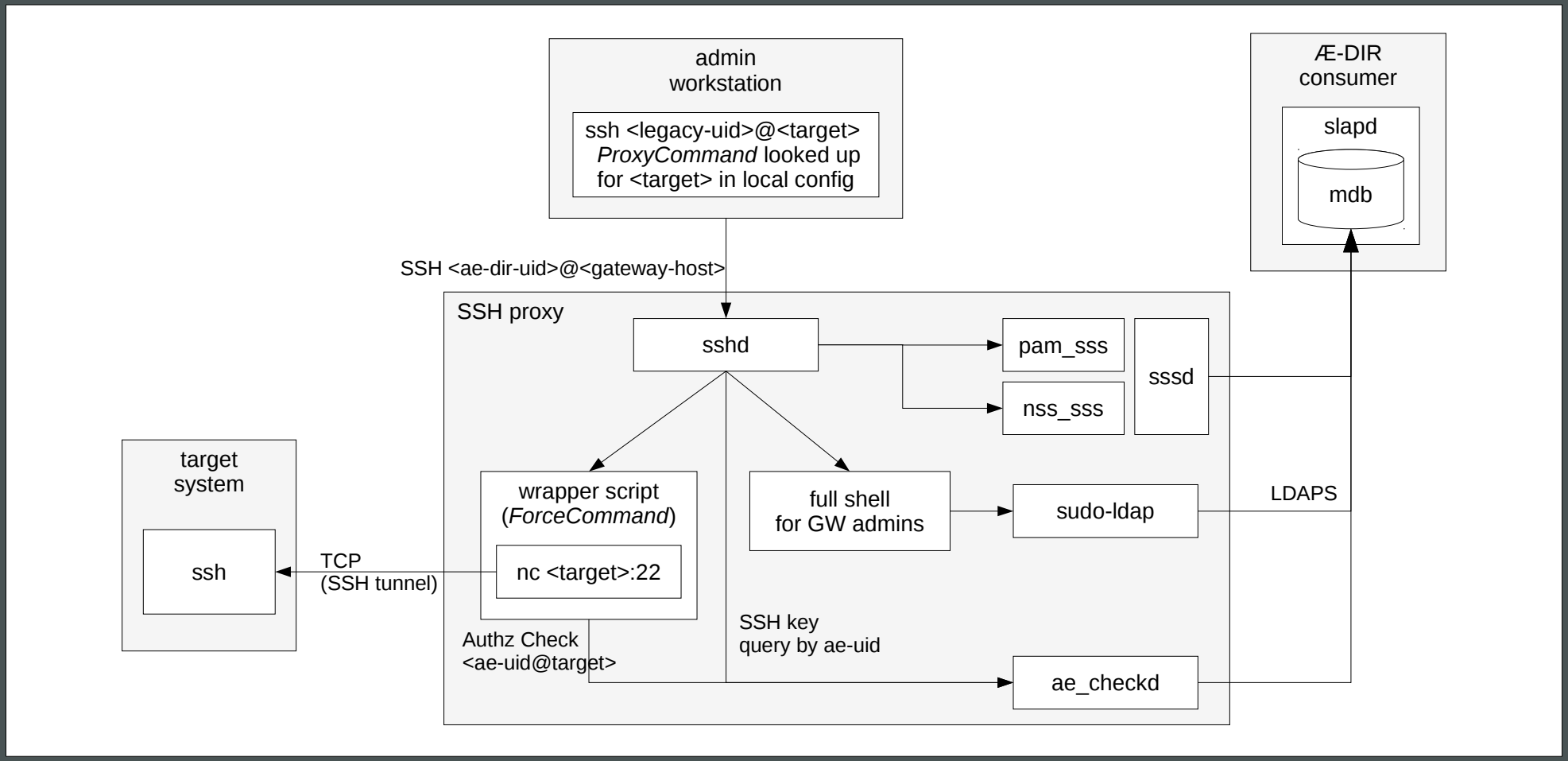
Authz EER diagram



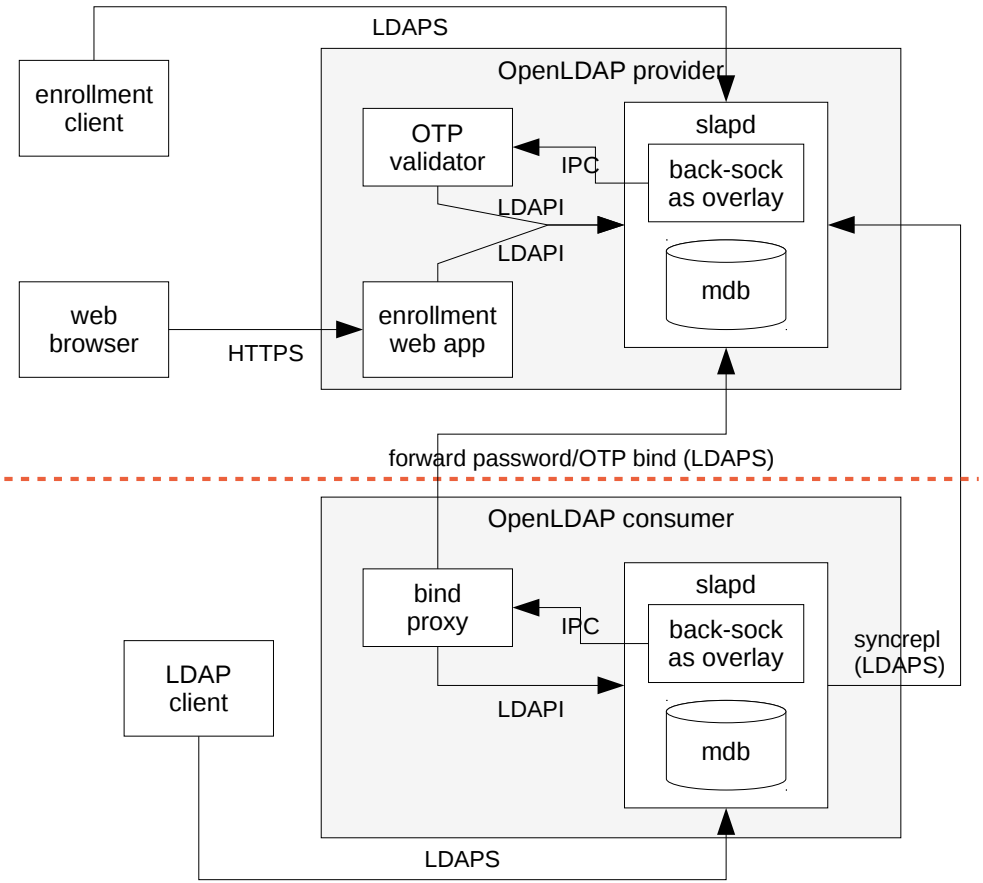
Client integration

- Clients deliberately kept dumb
- Schema derived from common standards:
  - NIS-LDAP
  - sudo-ldap (always *sudoHost: ALL*)
- Hybrid groups for RFC 2307/RFC2307bis compability
- Support for *hosts* map (e.g. with *nss-pam-ldapd* aka *nslcd*)
- Abandon *netgroup* map → migrate to *aeSrvGroup*

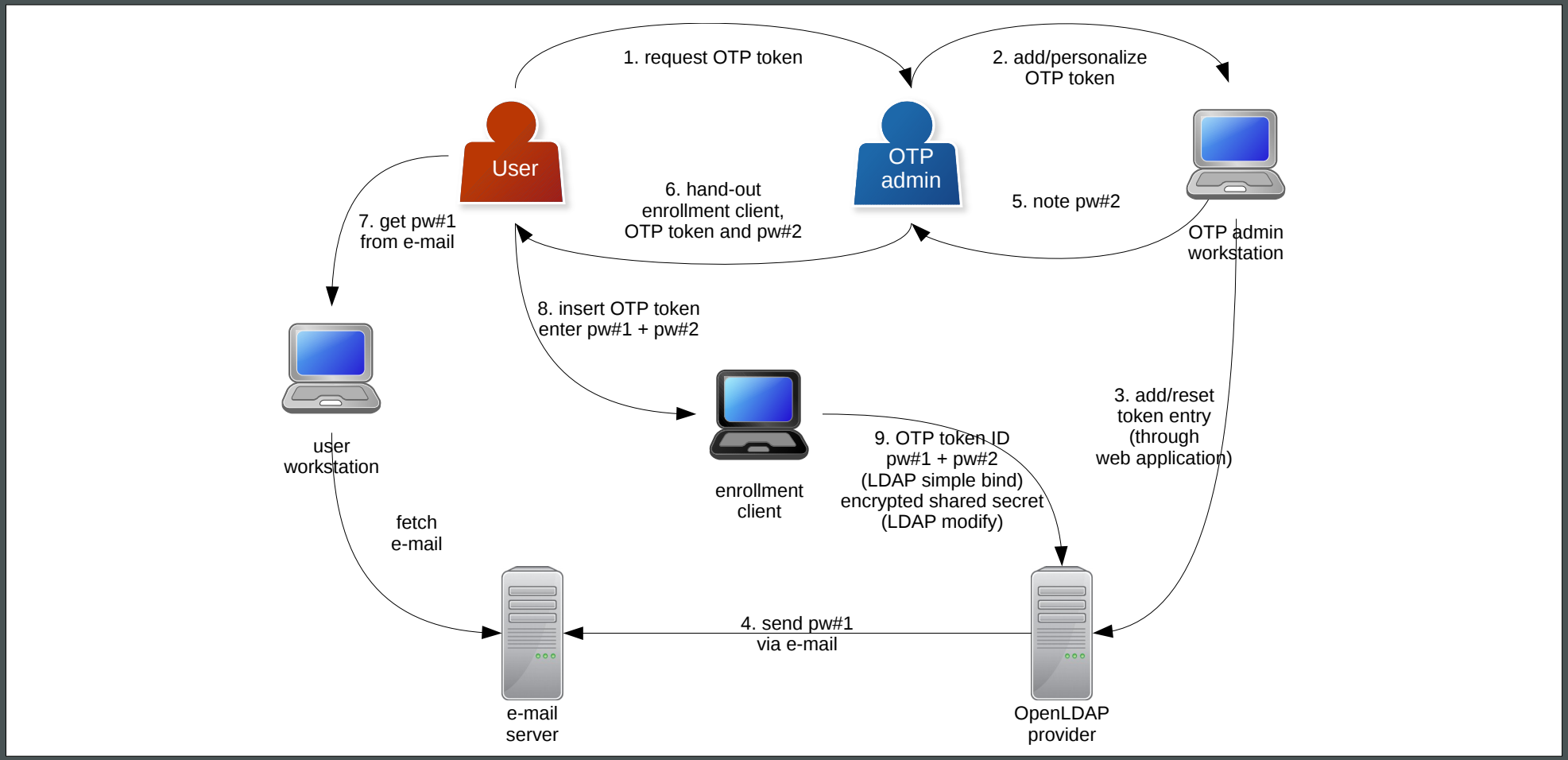
SSH proxy with authz



OATH-LDAP -- 2-tier architecture



OATH-LDAP -- enrollment



Next: System management

- *aeNwDevice* has triple (FQDN, IP, MAC)
- Network access control (802.1x)
- OS deployment (PXE, DHCP, BOOTP)
- Eliminate dynamic hostname updates in DNS
- easy integration of *virt-install* or similar
- *ansible* dynamic inventory
- X.509 server certificates

:-/

? … !

Check out -- https://ae-dir.com/demo.html
Contribute -- https://ae-dir.com/todo.html