Æ-DIR - Authorized Entities Directory

- The paranoid and agile IAM for DevOps -

Open Source Datacenter Conference 2018

Michael Ströder <michael@stroeder.com>

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

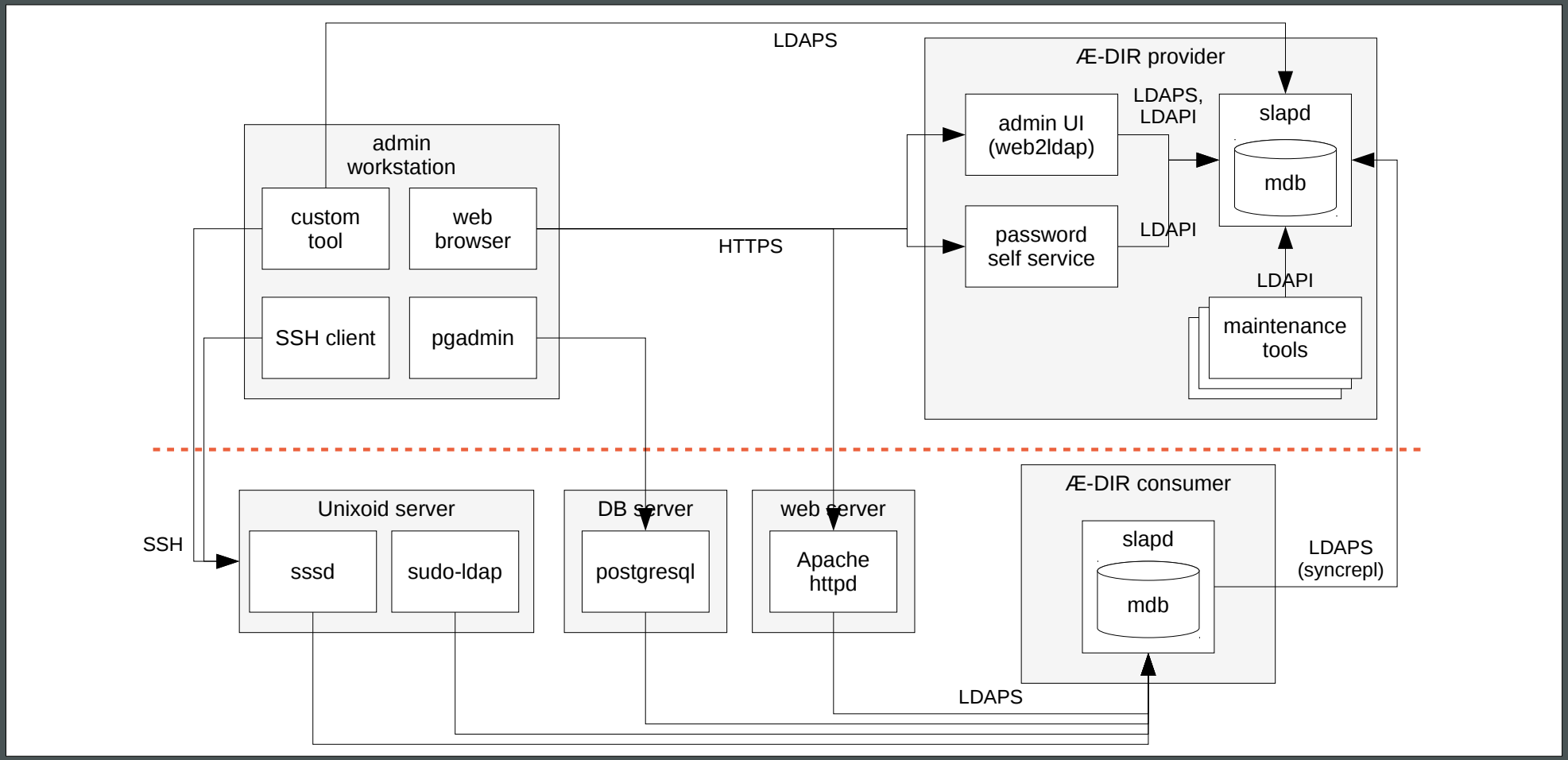
Goals

- Principles
  - Need-to-know
  - Least Privilege
  - Separation of Duties
- Delegated administration of manageable small areas
- Meaningful audit trails
- Compliance checks

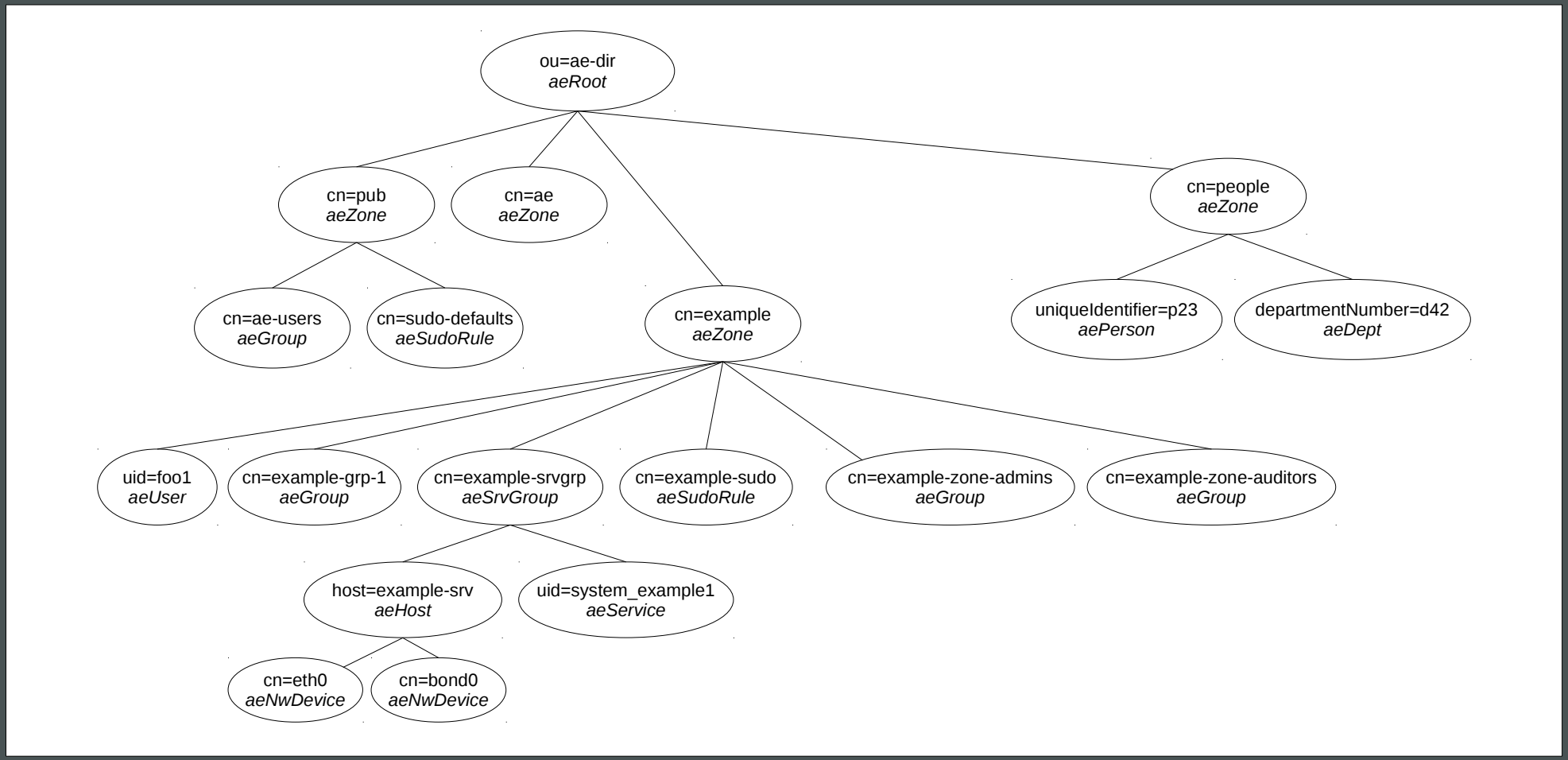
Paradigms

- Explicit is better than implicit
- Secure authorization requires secure authentication
- Avoid all-mighty proxy roles and workflows
- Do not assume hierarchical structure
- A person is not an user account
- Multiple user accounts per person
- Persistent IDs (never re-used) for reliable audit trails

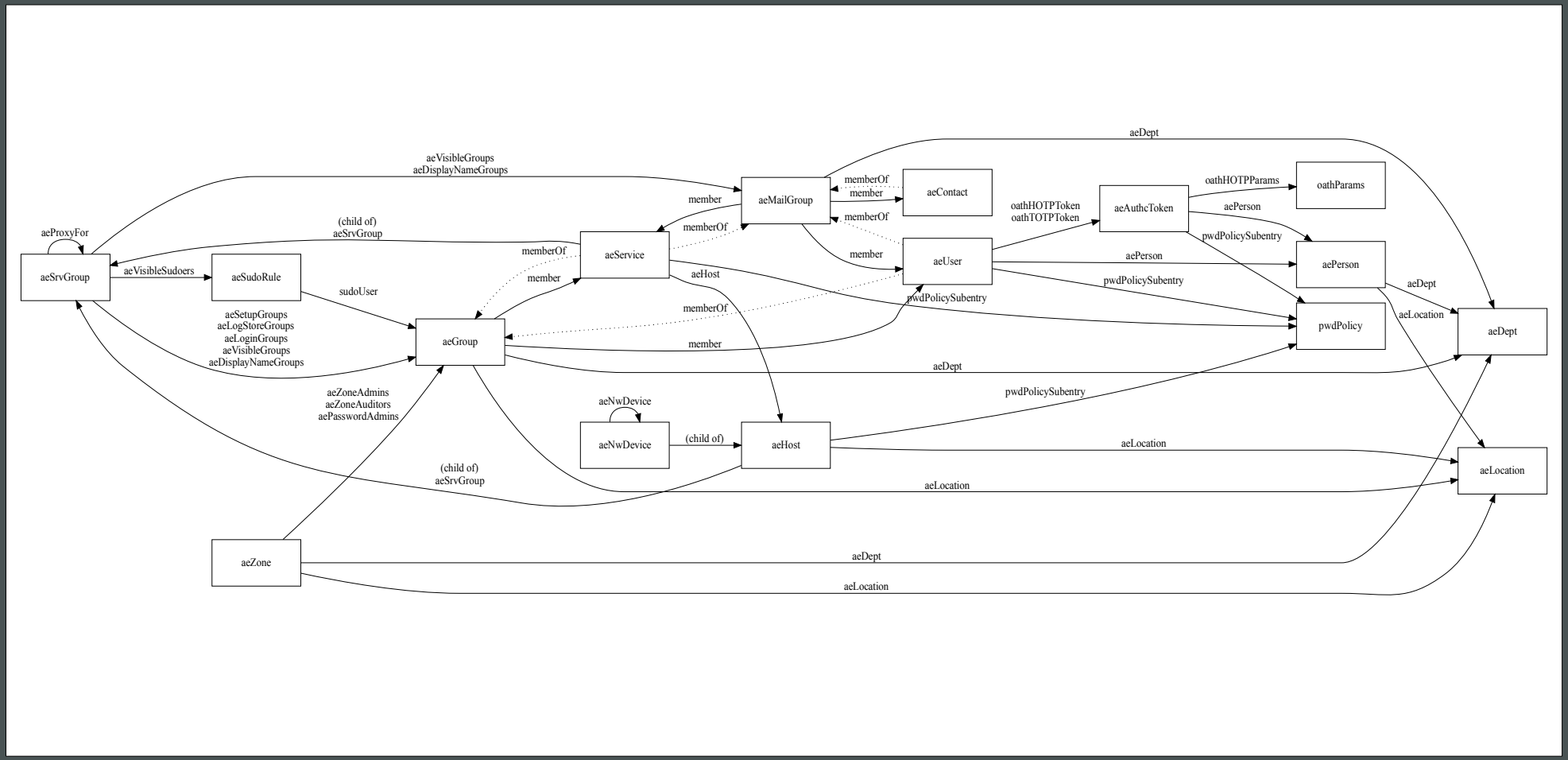
2-tier architecture



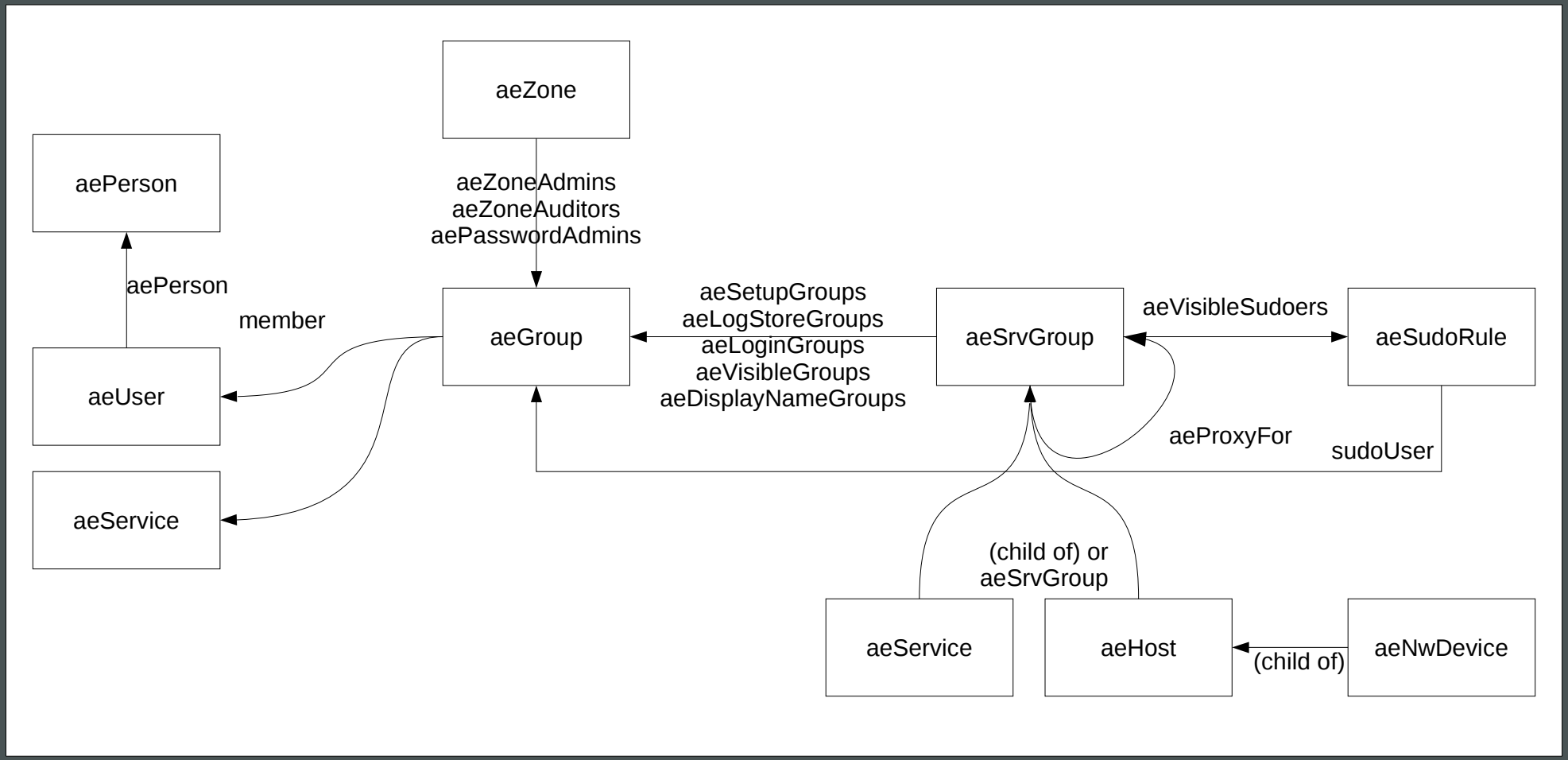
Directory Information Tree (DIT)



Full EER diagram



EER for access control



Installation Æ-DIR server

- *ansible* role installs replicas and all services
- base configuration to be done separately
- site-specific ansible variablen
- Read the comments!
  ansible/roles/ae-dir-server/defaults/main.yml
- Create site directory, see *ansible/example/*
- If things went wrong ansible role corrects it

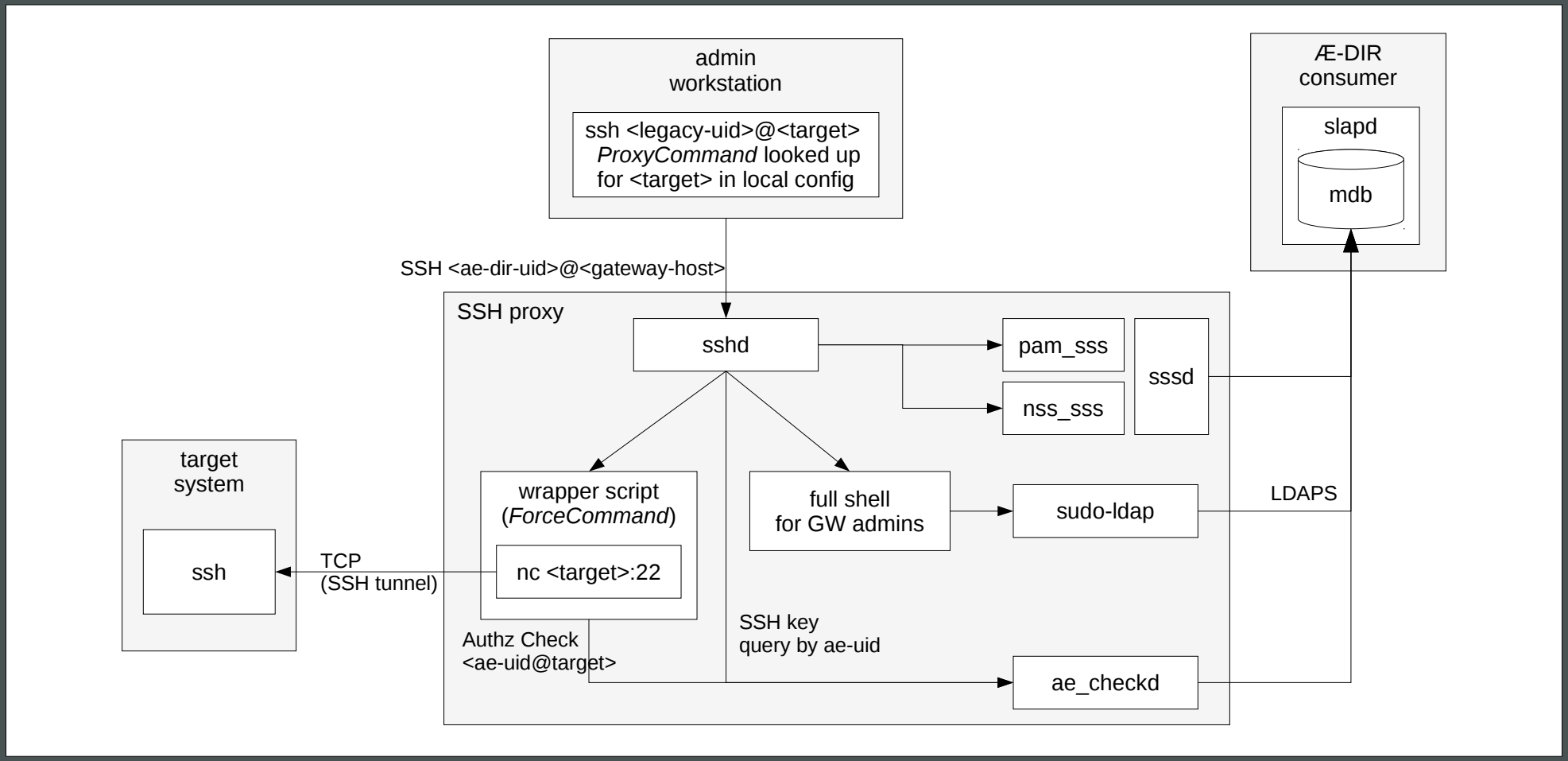
Defense in Depth

- Secure defaults
- Self-contained (zone *ae*)
- Service separated, Unix domain sockets (Peer Credentials)
- *systemd*-Options for hardening (mount points etc.)
- Strict *AppArmor* profiles for all services
  (optional, *targeted* and only for SUSE and Debian)
- 2-faktor-authc: yubikey based on *OATH-LDAP*
- Soon coming: Rule set for *mod_security*

Customer scenario #1

- Æ-DIR is separate IAM for privileged admin accounts
- 15000 hosts
- Person objects pulled from other LDAP server
- Separate accounts for ops and dev people
- Delegated administration of different stages
- Two-factor authc with yubikey
- SSH proxy

SSH proxy authz



Customer scenario #2

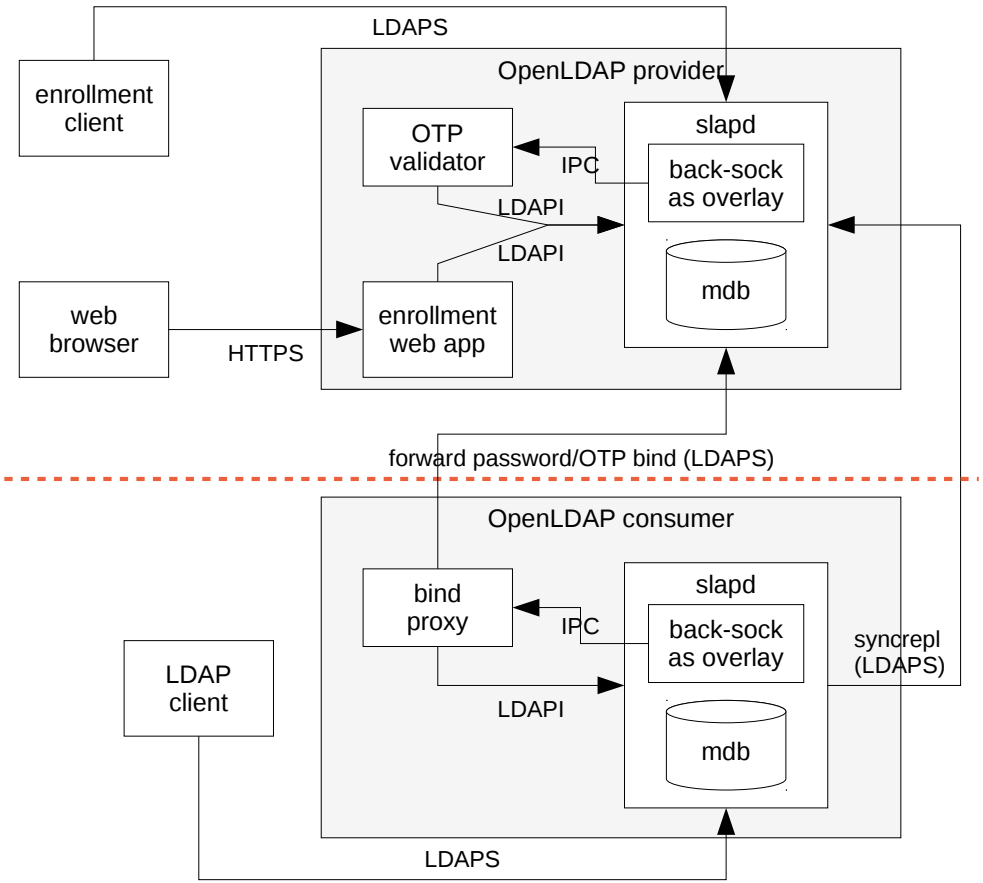
- Æ-DIR is the central IAM
- HR data pulled from NetSuite
- MacOS integration (synced pw change with File Vault)
- “base accounts” get synced to AD/Exchange with pw
- separate DevOps accounts synced to Azure without pw
- Login to Azure portal via SAMLv2 IdP
- two-factor authc with yubikey
- Future: SAMLv2 login to Office 365

SOHO scenario

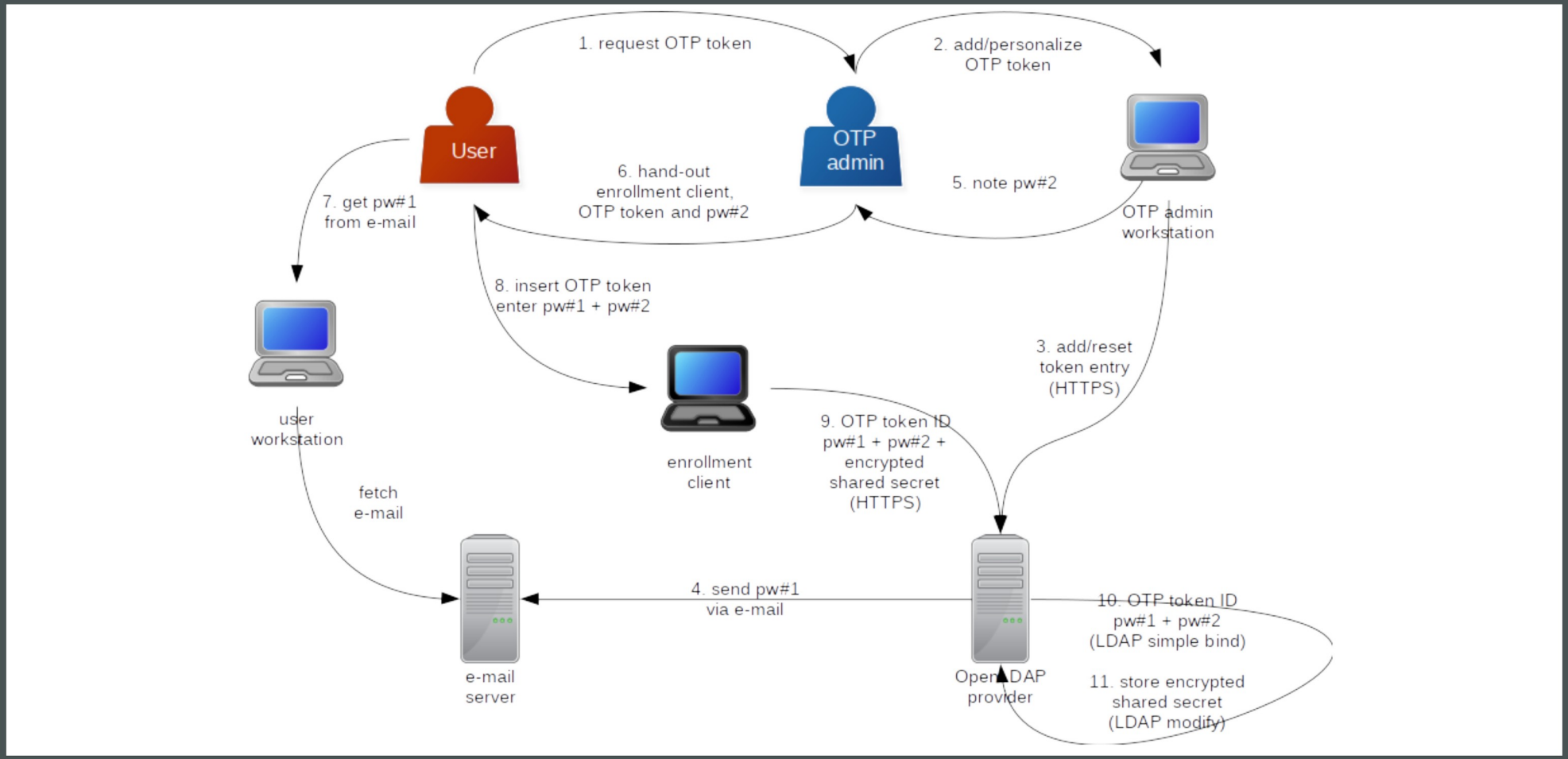
- Eat you own dog food!
- 7 W, libvirt/KVM
- postfix/dovecot
- Apache
- FreeRADIUS (WIFI)
- see client-examples/
- sshd & sssd or nslcd:
  roles/ae-dir-linux-client/

Image: thomas-krenn.com

2-tier architecture with OATH-LDAP



OATH-LDAP -- Enrollment



Conclusion

- Security by design is possible
- Yes, it's painful sometimes
- Admins need help in the beginning
- Backing of management helps (budget!)
- Don't break former security promises later!
  → think twice or more before changing something

Links

- Docs:
  https://ae-dir.com
- Play with it!
  https://ae-dir.com/demo.html
- OATH-LDAP:
  https://oath-ldap.stroeder.com

:-/

? … !

Work in progress: *aehostd*

- Simple custom host demon knows schema
- Even less client configuration
- Optimized search for users and groups (safe CPU cycles)
- Virtual groups (primary GID, role groups)
- LDAP session tracking control f. better logging
- *hosts* map
- sudoers files via *cvtsudoers* (sudo 1.8.23+)
- less code, less dependencies, mainly stripped *pynslcd(8)*