# Æ-DIR - Authorized Entities Directory

## - Identity & Access-Management mit OpenLDAP -

KA-IT-Si

2018-12-13

# Michael Ströder <michael@stroeder.com>

- Freiberufler
- Schwerpunkte
  - Identity & Access Management, Directory Services (LDAP)
  - Single Sign-On, Multi-Factor Authentication
  - PKI (X.509, SSH), Angewandte Verschlüsselung
- Open Source / Freie Software:
  Æ-DIR, OATH-LDAP, web2ldap

# Allgemeine Sicherheitsanforderungen

- Generelle Prinzipien
  - Need-to-know
  - Least Privilege
  - Separation of Duties
- → Berechtigungen notwendig
- Delegierte Administration überschaubarer Bereiche
- Nachvollziehbarkeit von Änderungen
- Prüfung der Einhaltung von Richtlinien (Compliance)

# Secure DevOps

- Aufgabenteilung nach Teams
- Unterschiedliche Sicherheitsrichtlinien
- Z.B. Netzwerktrennung
  (infra, frontend, middleware, backend)
- DevOps staging environments
  - dev: Entwickler haben vollen Zugriff
  - test: Manche Entwickler haben Zugriff
  - prod: Nur Betriebsteam, ggf. temporärer Zugriff für Entwickler

# Agile DevOps

- Bearbeitung von Anträgen ist nicht agil
- Jemand der entscheiden kann, sollte es gleich selbst tun
- Beantragungsprozesse vermeiden
- Feingranulierte Autorisierung notwendig

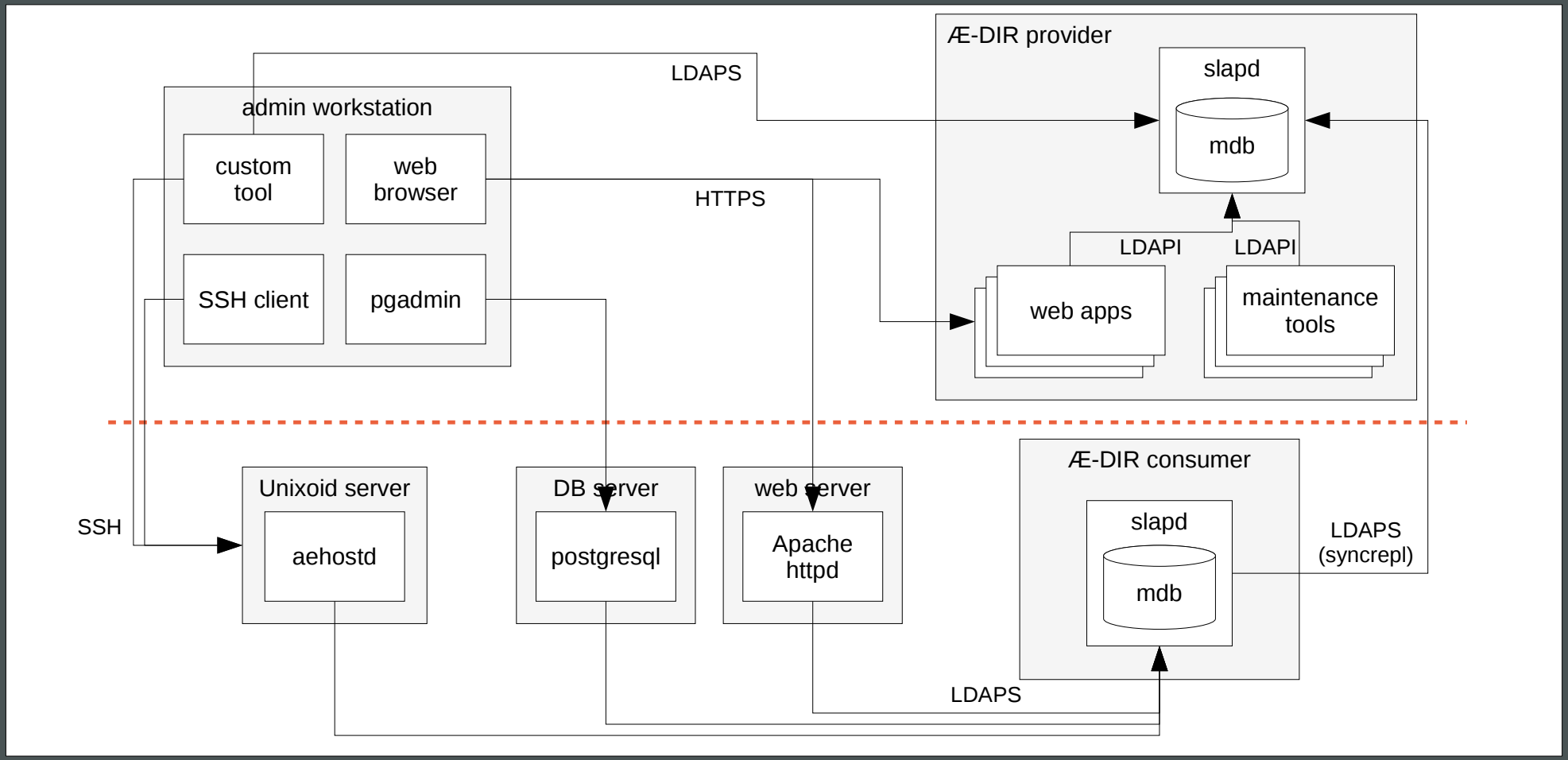
# Paradigmen

- Explizit ist besser als implizit
- Sichere Autorisierung erfordert sichere Authentifizierung
- Vermeiden von Stellvertreterrollen (HelpDesk, Systeme)
- Berechtigungen ohne streng hierarchische Strukturen
- Eine Person ist kein Benutzer
- Mehrere Benutzer pro Person für verschiedene Rollen
- Persistente IDs werden nie wieder benutzt

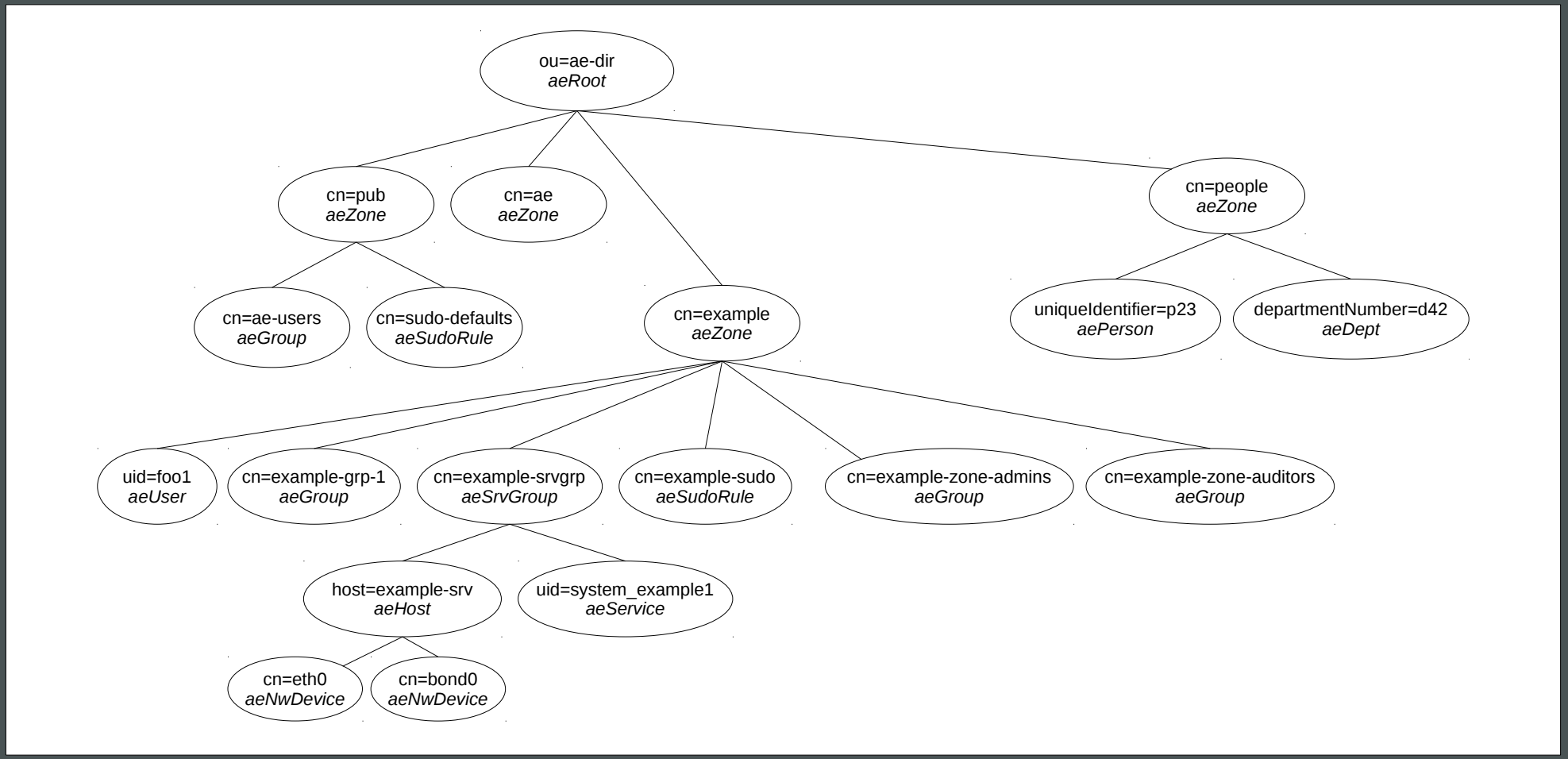
# Rollenkonzept Æ-DIR

- Æ admins delegieren Zonen, sonst nichts
- Æ auditors können (fast) alles lesen
- Zonen-Admins pflegen die Daten einer Zone
- Zonen-Auditoren können eine Zone einsehen
- Setup-Admins verwalten Hosts/Dienste innerhalb einer Service-Gruppe
- Benutzer können eigene Einträge lesen und eigenes Passwort ändern

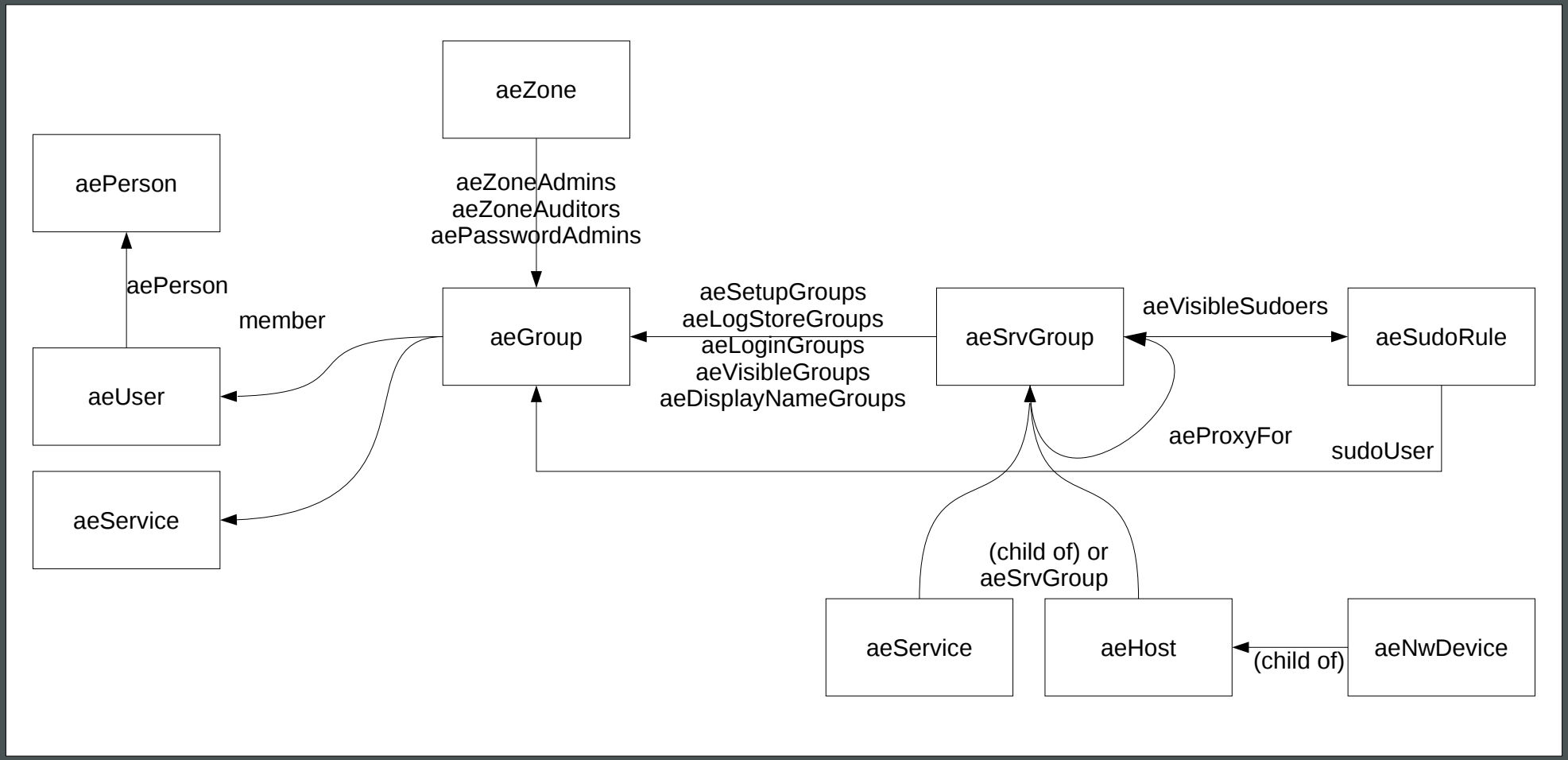
# 2-stufige Architektur



# Directory Information Tree (DIT)



# E/R-Diagramm


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

# Eindeutige IDs

- Sichere Autorisierung erfordert eindeutige Bezeichner
- Eindeutige IDs für verschiedene Objekte:
  uid, uidNumber, gidNumber, cn, aeFqdn, macAddress…
- Durch den Eintrag einer ID in einer Zone werden Zonen-Admins zu “Besitzern” der ID
- Nützlich für die delegierte Administration von DNS/DHCP, NAC, PKI, etc.

# Benutzerkennungen

- Benutzerkennungen sind Primärschlüssel auf Datenbestände angeschlossener Systeme
- Benutzerkennungen werden protokolliert
- → Nicht basierend auf Personennamen!
- → Werden nicht wieder verwendet!
- → Benutzerkonten können nur deaktiviert werden
- Status “archiviert” schränkt Sichtbarkeit ein (DSGVO)

# LDAP-Integration

- Schema basiert auf Standards (inetOrgPerson, RFC 2307,etc.)
- Æ-DIR-Schema wird nicht client-seitig benutzt
- nahezu jedes LDAP-fähige System direkt integrierbar
- Allgemeine Meta-Daten (Status, Nutzungsdauer, Verwendungszweck, Ticket-Nr.)

# Protokollierung

- Schreiboperationen werden in separate Datenbank protokolliert
- vollständige Repräsentation der LDAP-Schreiboperation
- Ein Traum für Auditoren
- Technisch: OpenLDAP-Overlay *accesslog*
- OpenLDAP protokolliert in syslog → zentraler Log-Dienst
- Automatische Log-Auswertung empfohlen (z.B. err=49)

# Praxiseinsatz

- Ca. 150 Mitarbeiter, verteilte Standorte, 300+ Server
- Æ-DIR als zentrales IAM-System
- Personaldaten aus NetSuite
- MacOS-Integration
- “Basis-Accounts” werden in AD/Exchange synchronisiert
- “DevOps-Accounts” werden ins Azure AD sychronisiert
- Login Azure-Portal via SAMLv2 IdP
- 2-Faktor authc mit yubikey

# SOHO-Einsatz

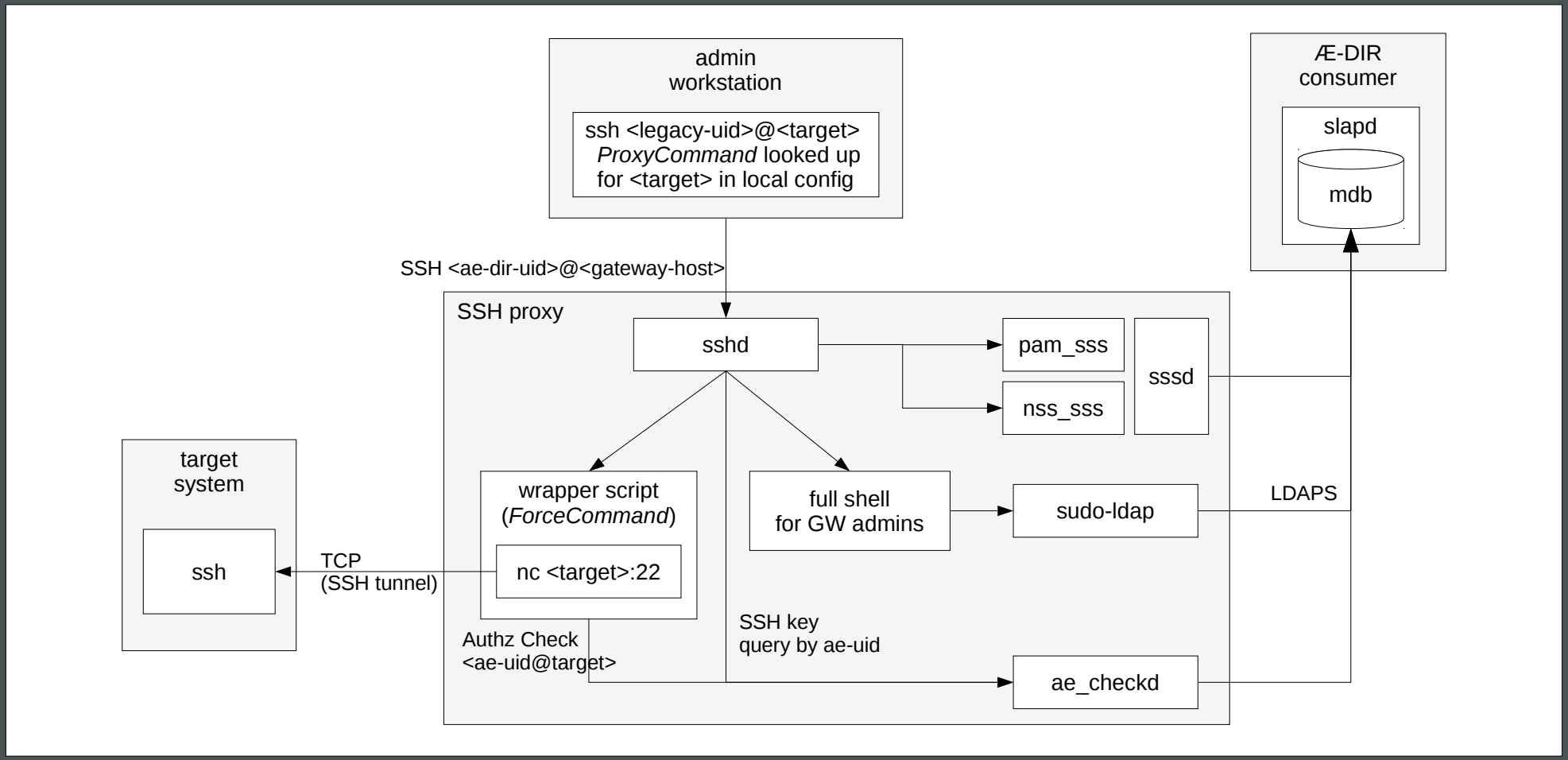
- Eat you own dog food!
- 7 W, libvirt/KVM
- postfix/dovecot
- Apache
- FreeRADIUS (WIFI)

Image: thomas-krenn.com

# aehostd

- Spezielle Client-Komponente für Linux-Logins
- Für Integration vieler Linux-Systeme (1000+)
- Kennt Schema und kann effizienter suchen
- Spezieller Mechanismus für automatisches Enrollment des Host-Passworts
- Besseres Verhalten der LDAP-Verbindungen
- Nützliche Spezial-Features:
  virtuelle Rollengruppen, Client-Tracking-Logs, etc.

# SSH-Proxy mit Autorisierung



# Fazit

- Mehr Sicherheit ist möglich
- … ist aber anstrengend …
- Gute Modellierung der Berechtigungen meist erst im 2. Wurf
- Rückhalt des Managements hilft (Budget!)
- Schulung notwendig
- Change-Management!

# Links

- Dokumentation:
  https://ae-dir.com
- Ausprobieren:
  https://ae-dir.com/demo.html
- Installieren:
  https://ae-dir.com/install.html

:-/

? … !