OSIAM

Sichere Identitätsverwaltung auf Basis von SCIMv2 und OAuth2

LINUX TAG

↪ tarent

Agenda

↪ tarent

- 1. Sichere Identitätsverwaltung
  - Unser Anspruch
  - OAuth2
  - SCIMv2
- 2. OSIAM
  - Wann und Warum?
  - Wo?

Unser Anspruch

tarent

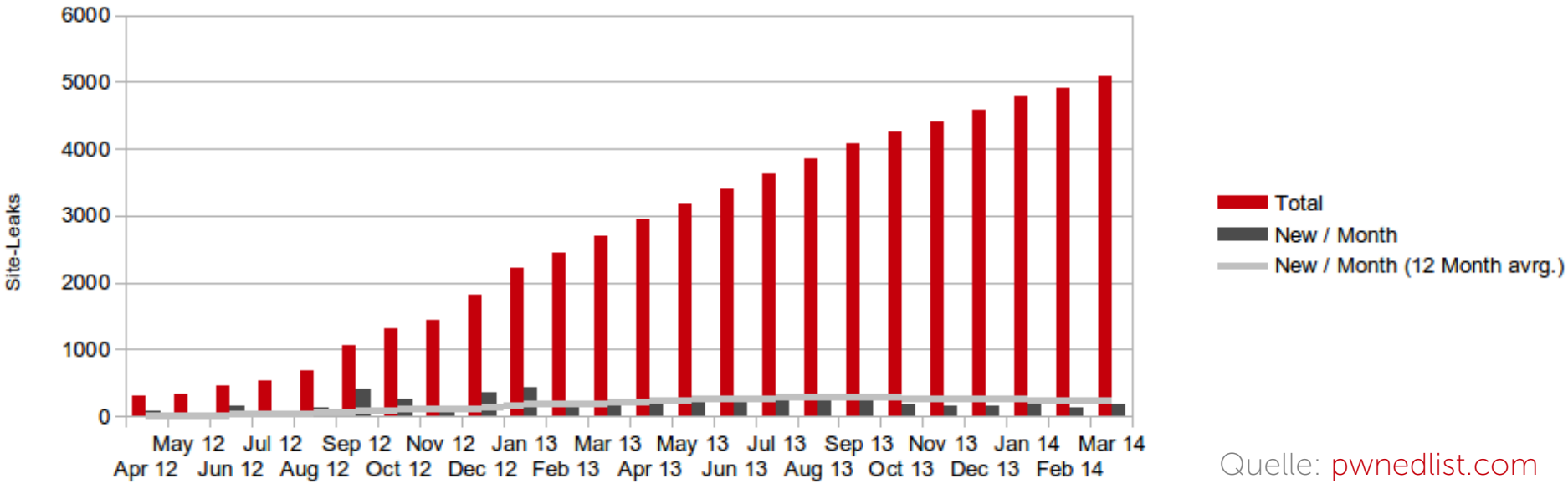
Die Nutzung moderner Services mit Fokus auf

- **Sicherheit**
  - Kontrolle und Übersicht
- **Verfügbarkeit (offene Standards)**
  - Technologien und Trends
  - Einfache Benutzung
- **Flexibilität**
  - Schnittstellen zu gängigen Anwendungen
  - Robustheit und Skalierbarkeit

Warum?

↪ tarent

April 2014: 18 Millionen E-Mail-Passwörter aufgetaucht



Quelle: pwnedlist.com

↪ Geleakte E-Mails prüfen: BSI, PwndList

OAuth 2.0 Standard

↪ tarent

Informationen: oauth.net

- Für Desktop-, Web- und Mobile-Applikationen
- Bekannter Standard für sicheren API-Zugriff
- Entwickelt, um einer Anwendung Zugriff auf meine Daten zu erlauben, ohne Benutzername und Passwort preiszugeben
- Aus Entwicklerperspektive relativ geringe Komplexität bei Client-Implementierungen

3-legged OAuth Flow

↪ tarent

Specification: RFC6749

Demo

SCIM v2 Standard

↪ tarent

Informationen: simplecloud.info

↪ **System for Cross-domain Identity Management**

Entwickelt mit Fokus auf Web- und Cloud-Kompatibilität

Umfangreiche Such- und Update-Funktionen

↪ **RESTful**

Nutzung des HTTP-Protokolls

Selbsterklärende URLs/Endpunkte

↪ **Zukunftssicher**

Hohe Akzeptanz und Verbreitung bei großen Playern

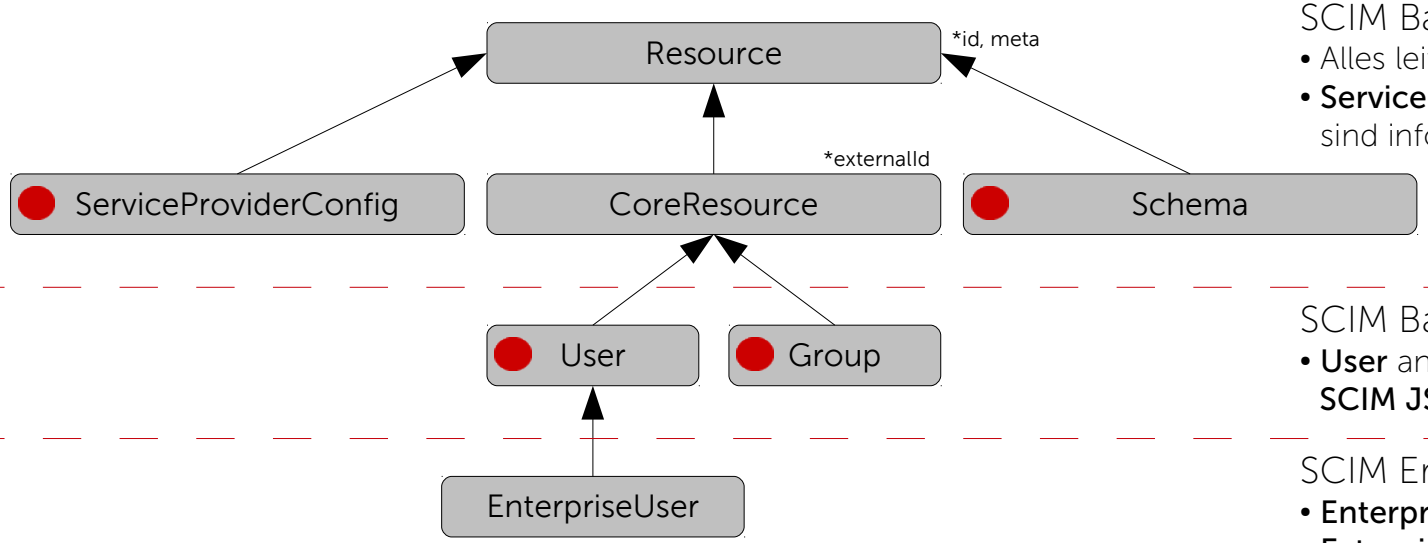
Leichtgewichtige Struktur im Web (vgl. Directory Services)

Single Sign-On (SSO) und Web-Provisionierung

SCIM v2 Übersicht

↪ tarent

Informationen: simplecloud.info



SCIM Basis:
- Alles leitet von **Resource** ab
- **ServiceProviderConfig** und **Schema** sind informativ und eher statisch

SCIM Basis:
- **User** and **Group** sind definiert als **SCIM JSON Schema**

SCIM Erweiterung(en):
- **EnterpriseUser** als Standardbestandteil
- **Extensions** über /Schemas abrufbar

Ressourcen-Endpunkte: https://host/ServiceProviderConfigs
https://host/Schemas
https://host/Users
https://host/Groups

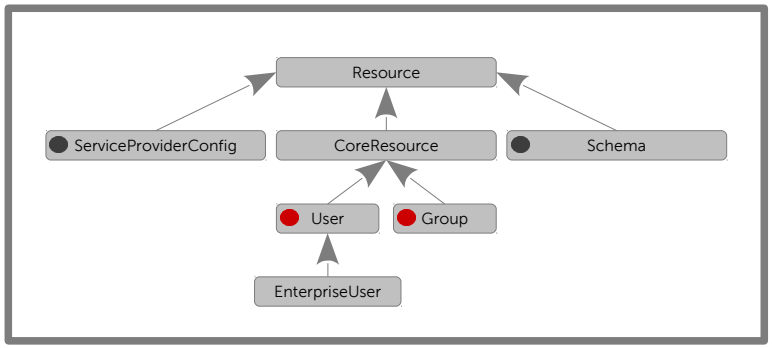
SCIM v2 API

↪ tarent

Vereinfachte Übersicht

Informationen: IETF Draft

- Create
  POST https://host/{Resource}
- Read
  GET https://host/{Resource}/{id}
- Replace
  PUT https://host/{Resource}/{id}
- Delete
  DELETE https://host/{Resource}/{id}
- Update
  PATCH https://host/{Resource}/{id}
- Search
  GET https://host/{Resource}?filter / sortBy / sortOrder
  POST https://host/{Resource}/.search



Agenda

↪ tarent

1. Sichere Identitätsverwaltung
   - Unser Anspruch
   - OAuth2
   - SCIMv2
2. OSIAM
   - Wann und Warum?
   - Wo?

Was ist OSIAM?

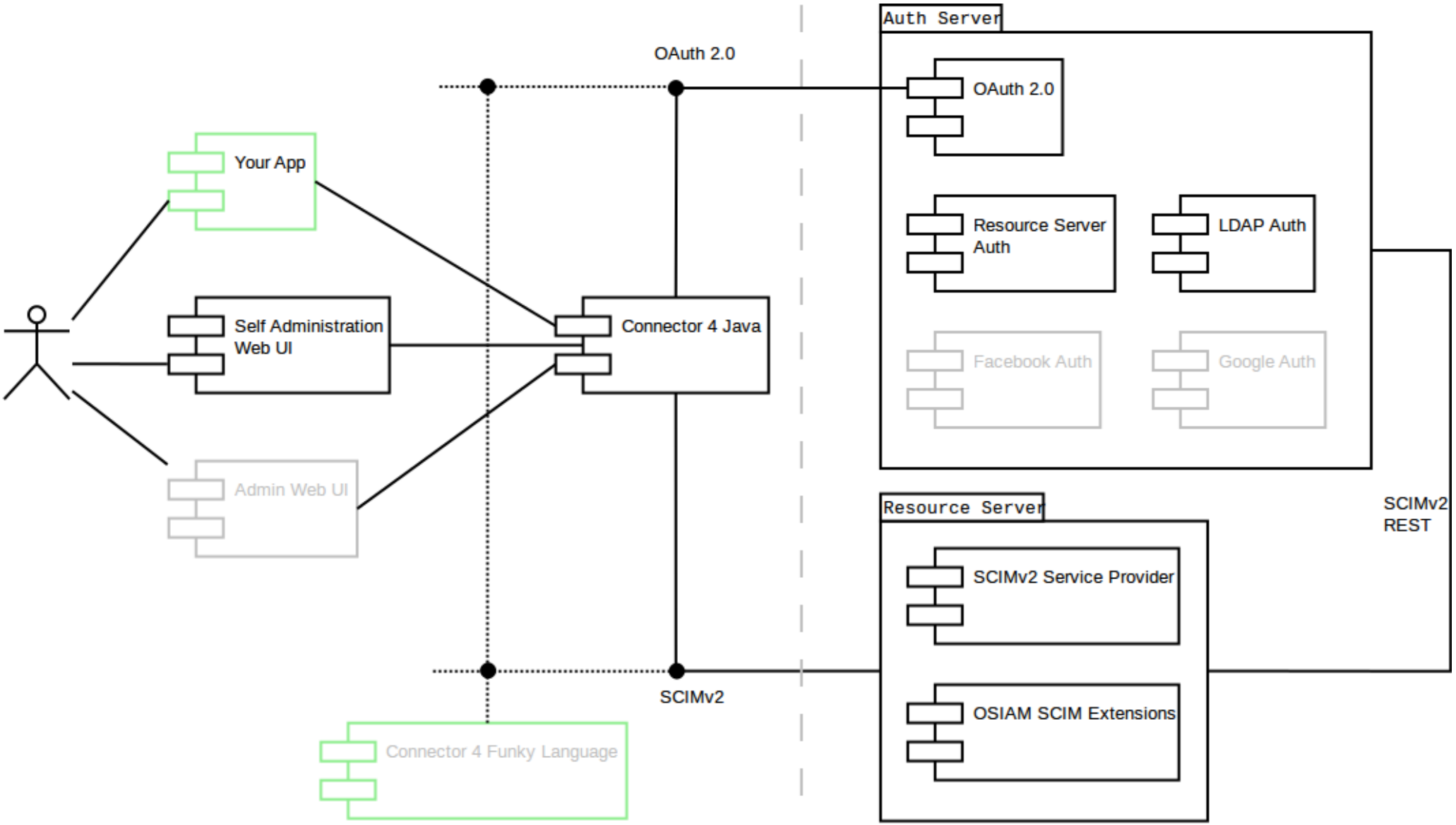
↪ tarent

Sichere und flexible Stammdatenverwaltung
zur einfachen Integration in Web- und Fachanwendungen

- ↪ OSIAM dient als Speicher für sensible Daten
- ↪ Anwendungen können z. B. Account-Daten zur Benutzerauthentifizierung nutzen
- ↪ Anwendungen können Benutzerdaten und deren Berechtigungen abfragen
- ↪ Wesentliche Merkmale OSIAMs sind neben **Sicherheit, einfacher Integration** und der **Verwendung offener Standards, geringe Systemvoraussetzung** und **hohe Performance.**

OSIAM
OPEN SOURCE IDENTITY & ACCESS MANAGEMENT

Was ist OSIAM?



Wann und Warum OSIAM?

↪ tarent

↪ Bestehende Nutzerverwaltung an meine Anwendung anbinden

- **Zeitersparnis** im Vergleich zur Eigenentwicklung
- Mit **wenig Aufwand** integrierbar

↪ Zentrale Stammdatenverwaltung für mehrere Anwendungen

- Diverse Benutzerrollen **übersichtlich** verwalten
- **Flexible Schnittstelle** zur Abfrage der Berechtigungen

↪ Single Sign-On für meine Anwendungen

- **Vereinfachte Bedienung** als Nutzer durch einen zentralen Account
- Nutzer bestimmt selber die Datenfreigaben pro Anwendung

Wo finde ich OSIAM?

tarent

- Community-Einstiegspunkt: https://osiam.org

- Source Code Repository: https://github.com/osiam
- Story- und Issue-Tracker: https://jira.osiam.org

- Mailing-Liste: https://groups.google.com/forum/?fromgroups#!forum/osiam

OSIAM Roadmap

↪ tarent

- **Security**
  OAuth-Scopes, Tokens, Multi-Factor-Auth, Auditing
- **Einfache Benutzung**
  Paketierung (Betrieb, Entwicklung, …), Automatisierung
- **Robustheit**
  Optimierung (Performance, Speicher), Monitoring
- **Federation**
  Google, Xing, Facebook, OpenID, …
- **UI-Addons**
  Administration, Selbstverwaltung

Ausprobieren!

↪ tarent

- **Erprobte Security-Frameworks sind besser als eigene**
- **offen (MIT-Lizenz)**
- **Einfach integrierbare API**
- **Freier SCIM Service Provider, kompatibel mit anderen SCIM Clients**
- **Freie SCIM Client Connectoren, kompatibel mit anderen SCIM SP**
- **Und dann: Mitmachen!**

Kontakt

Andreas Grau
Consultant
Mail: a.grau@tarent.de

Thomas Krille
Software Developer
Mail: t.krille@tarent.de

Rochusstraße 2-4
53123 Bonn

Voltastraße 5
13355 Berlin

Telefon: +49 (0) 228 54 881 -0
Telefax: +49 (0) 228 54 881 -235