Complete open source IAM solution

Evolveum

Radovan Semančík

LDAPcon, November 2015

Radovan Semančík

Current:

- Software Architect at Evolveum
- Architect of Evolveum midPoint
- Contributor to ConnId and Apache Directory API

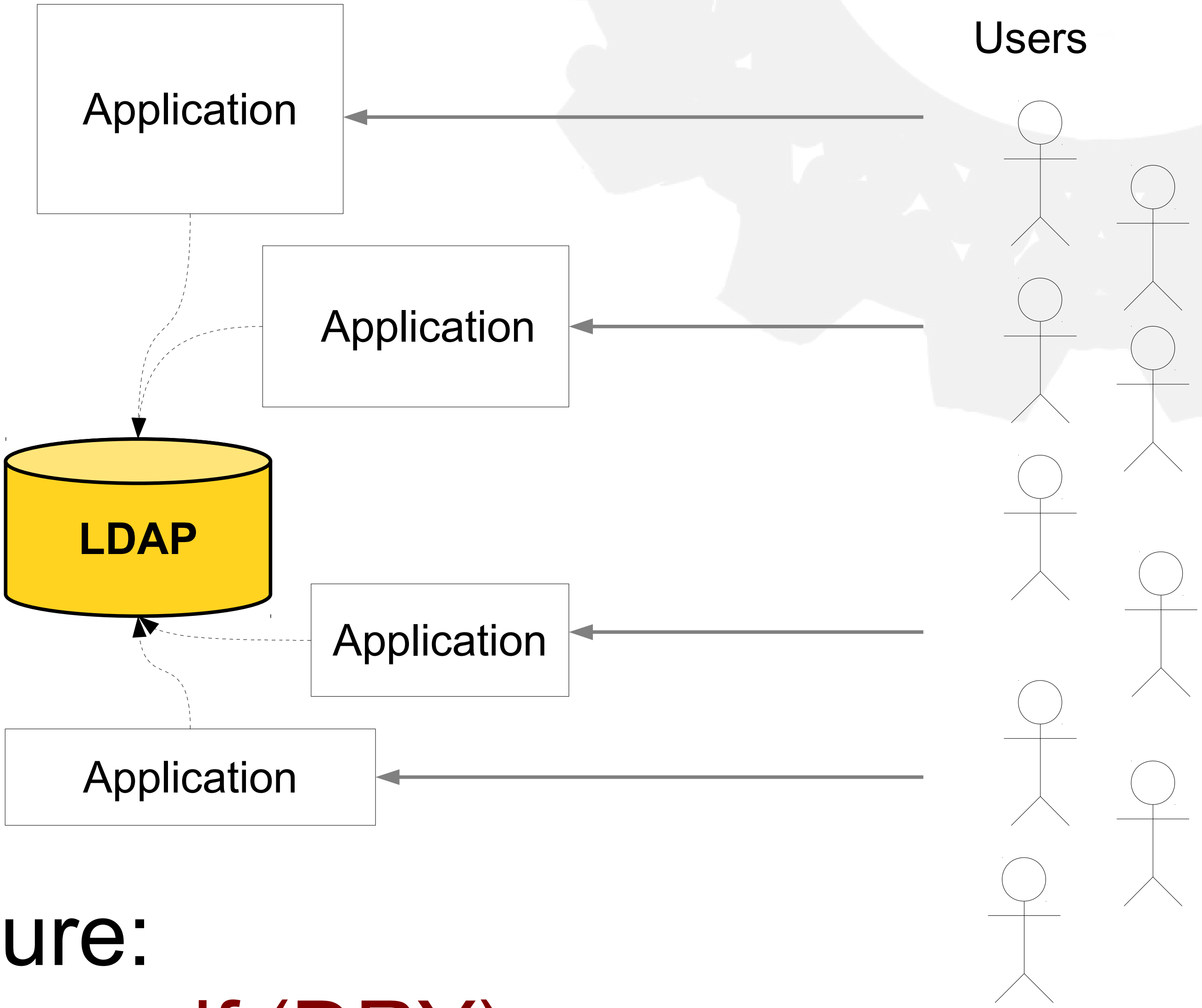
Past:

- Sun LDAP and IDM deployments (early 2000s)
- OpenIDM v1, OpenICF
- Many software architecture and security projects

Evolveum

Complete solution? Why? Is LDAP not enough?

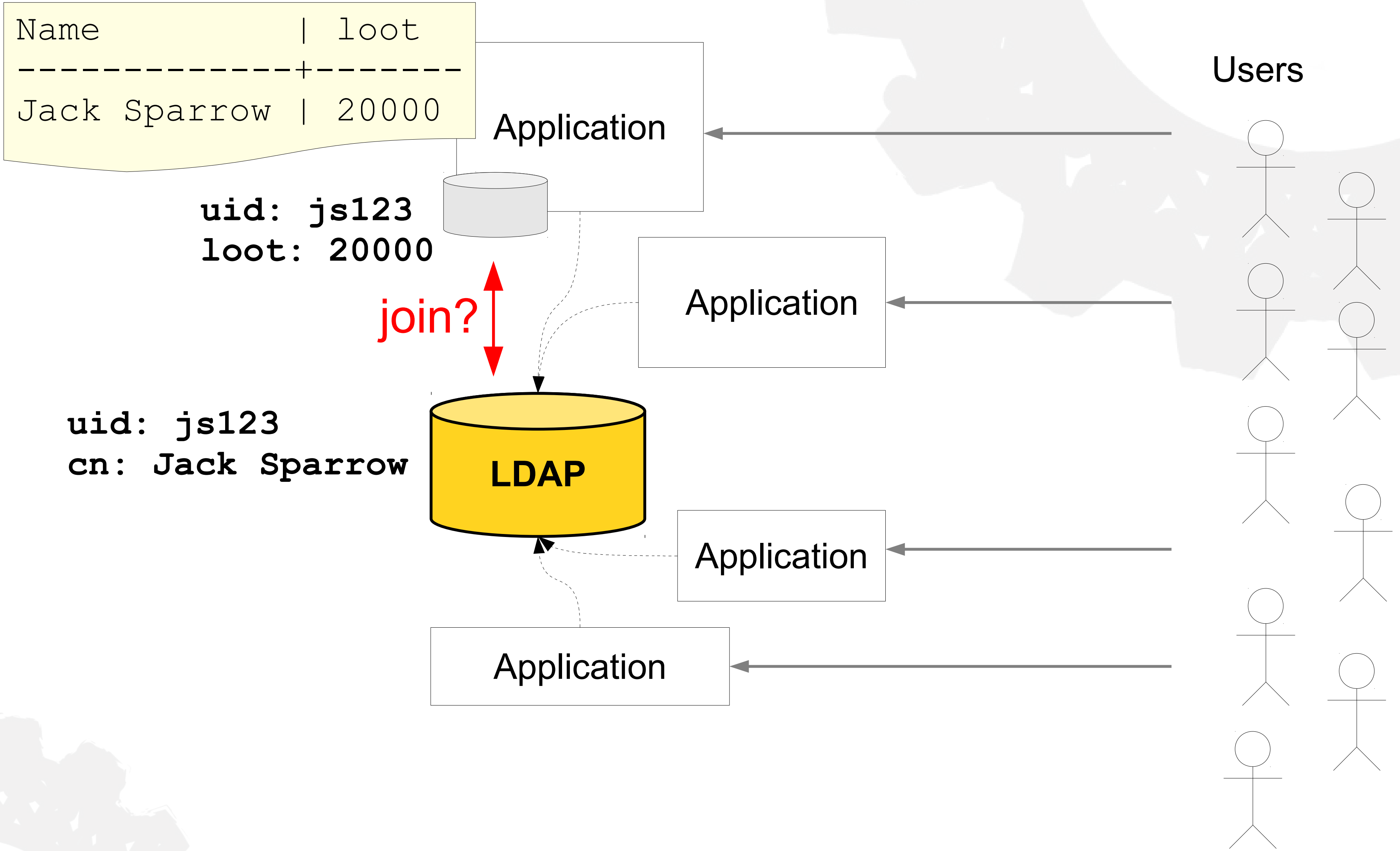
Yes, theoretically ...



Good architecture:

Don't repeat yourself (DRY)

Practice: Application-Local DB

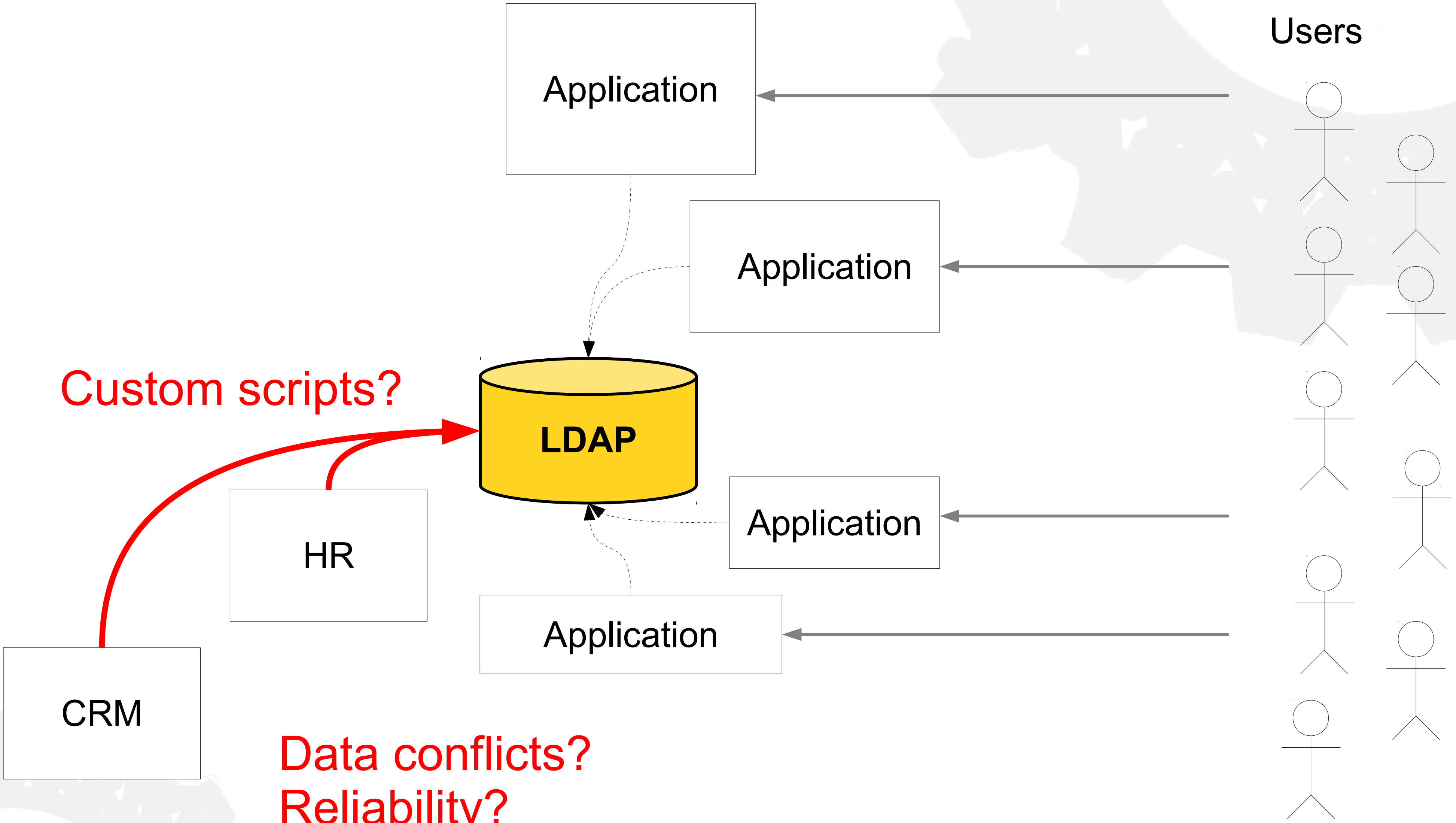


```
Name          | loot
--------------+--------
Jack Sparrow | 20000
```

```
uid: js123
loot: 20000
```

```
uid: js123
cn: Jack Sparrow
```

Practice: Data Sources

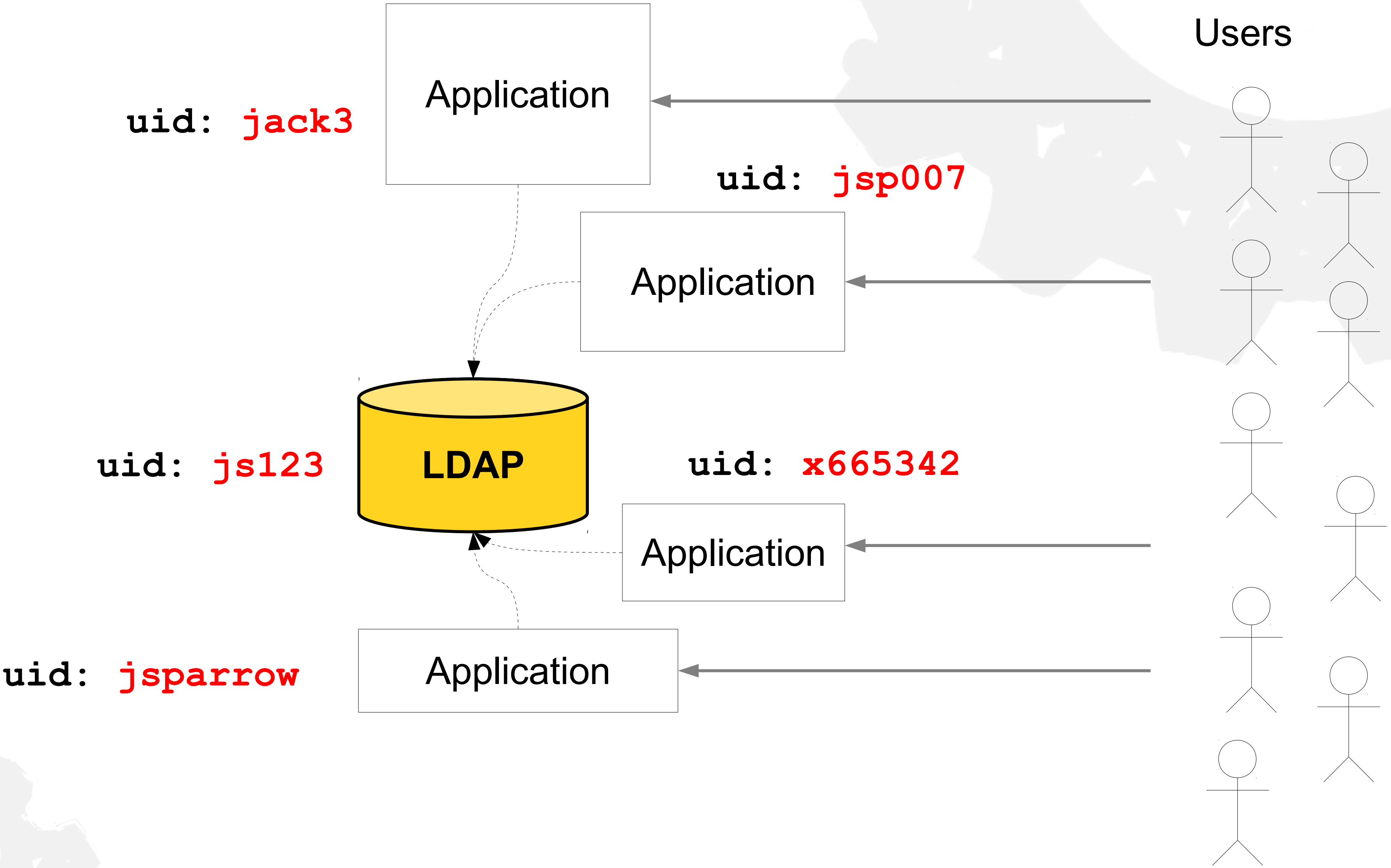


Custom scripts?

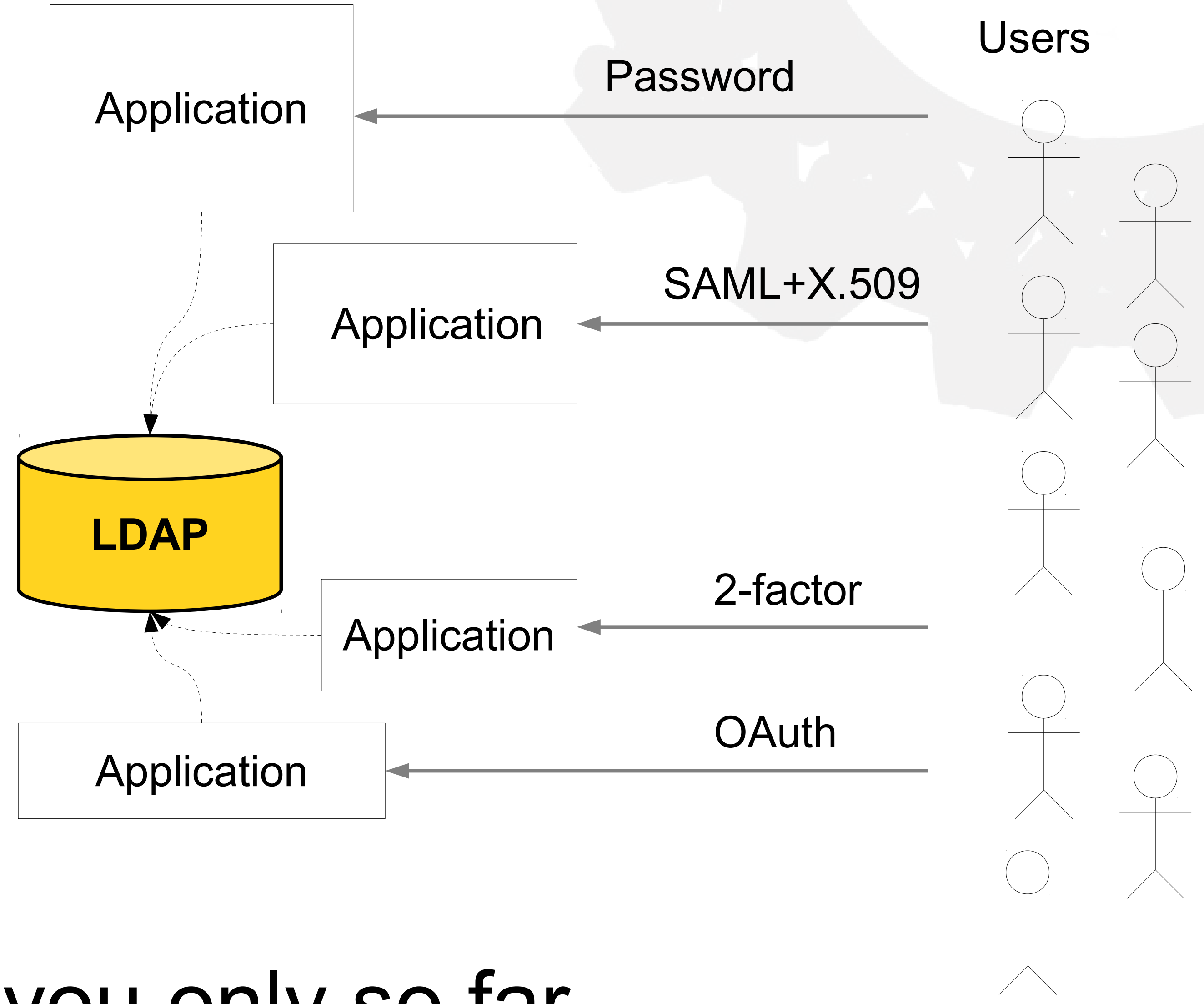
Data conflicts?
Reliability?
Maintenance?

Evolveum

Practice: Legacy



Practice: Authentication



SASL will get you only so far ...

But … these are **application problems**! Let's fix the appliations and **standardize**. We'll be fine.

Standardization? Really?

```
dn: cn=foo,ou=groups,o=example
objectclass: groupOfNames
member: uid=bar1,ou=people,o=example
member: uid=bar2,ou=people,o=example
```

```
dn: cn=foo,ou=groups,o=example
objectclass: groupOfUniqueNames
uniqueMember: uid=bar1,ou=people,o=example
uniqueMember: uid=bar2,ou=people,o=example
```

RFC2256 (1997)

mandatory(!!!)

(Examples are simplified)

Standardization? Really?

```
dn: cn=foo,ou=groups,o=example
objectclass: groupOfNames
member: uid=bar1,ou=people,o=example
member: uid=bar2,ou=people,o=example
```

```
dn: cn=foo,ou=groups,o=example
objectclass: groupOfUniqueNames
uniqueMember: uid=bar1,ou=people,o=example
uniqueMember: uid=bar2,ou=people,o=example
```

RFC2256 (1997)

```
dn: cn=foo,ou=groups,o=example
objectclass: posixGroup
memberUid: bar1
memberUid: bar2
```

RFC2307 (1998)

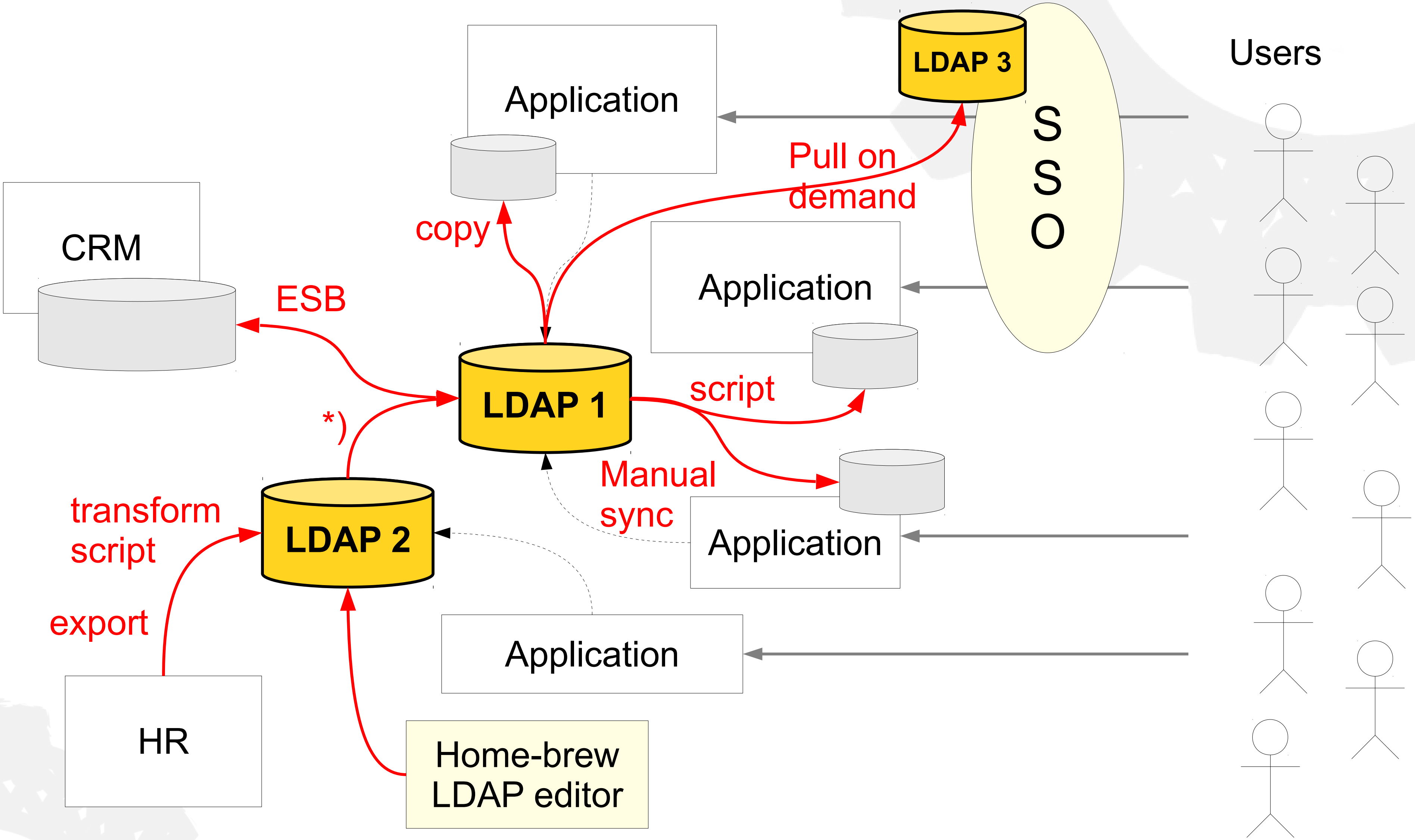
(Examples are simplified)

Practice: more problems

- Password reset
- Adaptive authentication
- SSO
- Session management
- ACLs
- Account activation (enabled/disabled status)
- “memberOf”
- Roles / RBAC
- Password policies
- Access policies (autz)
- Paging (SPR vs VLV)
- Audit
- Reporting
- Data consistency
- Management tools
- User experience
- Schema consistency issues
- Standard violations
- Common sense violations
- Too many data types
- … most of them unsupported
- DN case sensitivity
- Synchronization

Evolveum

Practice: really messy

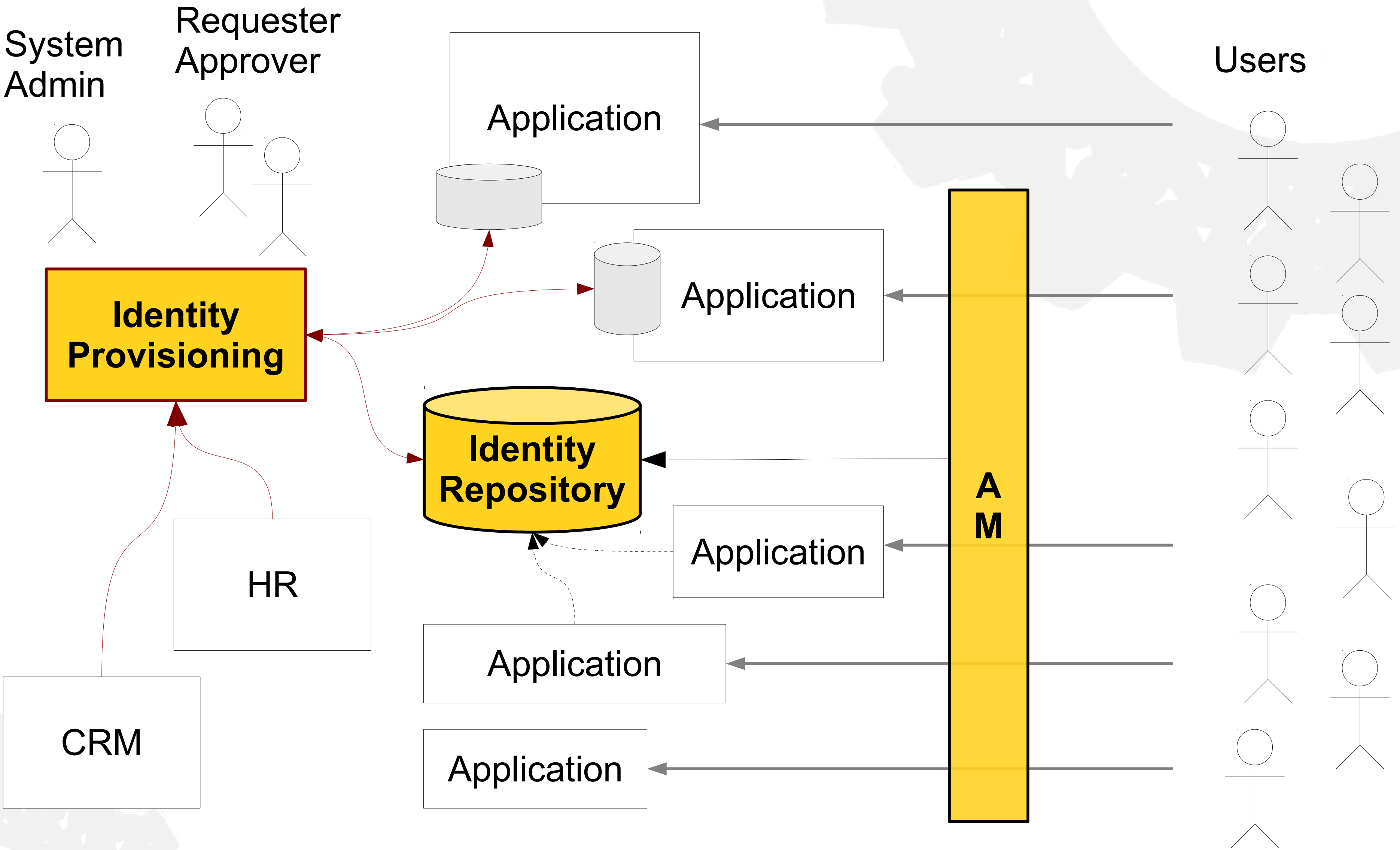


*) nobody really knows how this part works because the guy that did it left 3 years ago

Evolveum

LDAP-only solutions work only in simple cases.

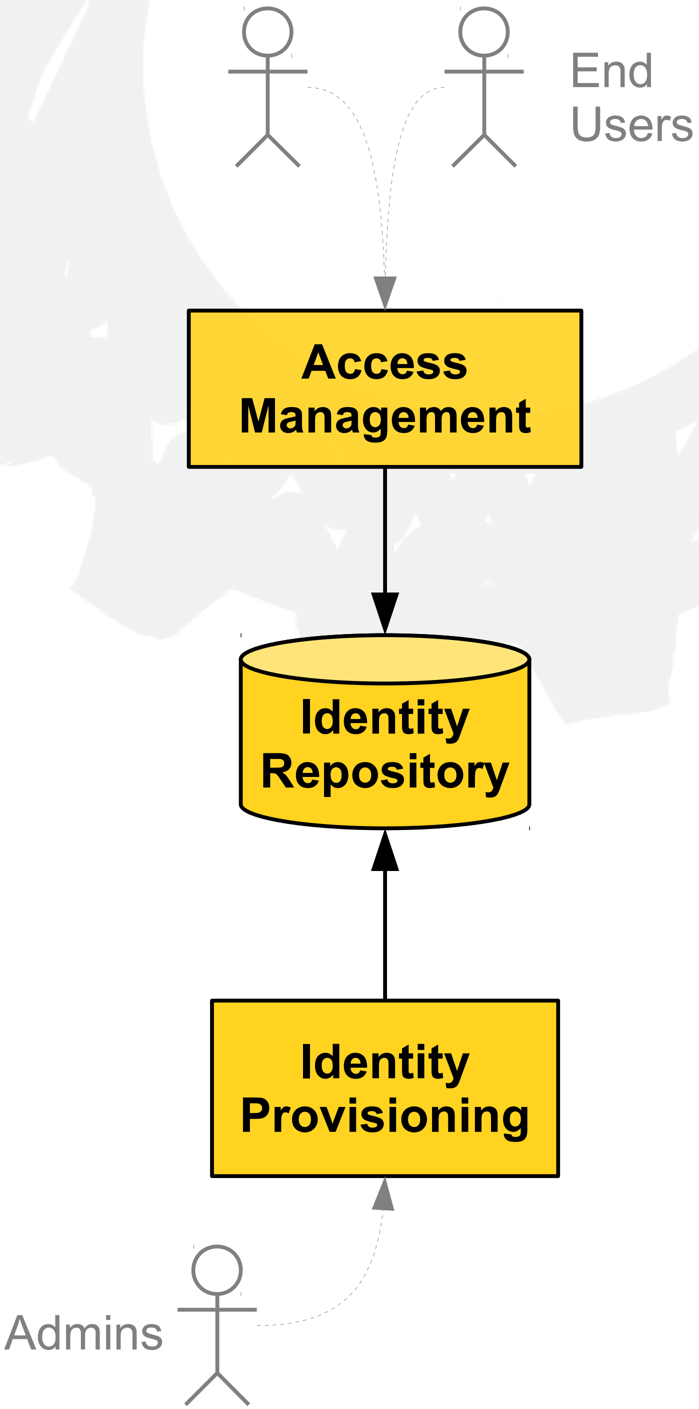
IAM needs more components



Evolveum

Basic IAM Components

- **Access Management**
  - Authentication, single sign-on
  - Basic authorization
- **Identity Repository**
  - Storage of identity data
- **Identity Provisioning**
  - Management (data, policies, workflows)
  - Synchronization



Evolveum

Interoperability

- The components should work together

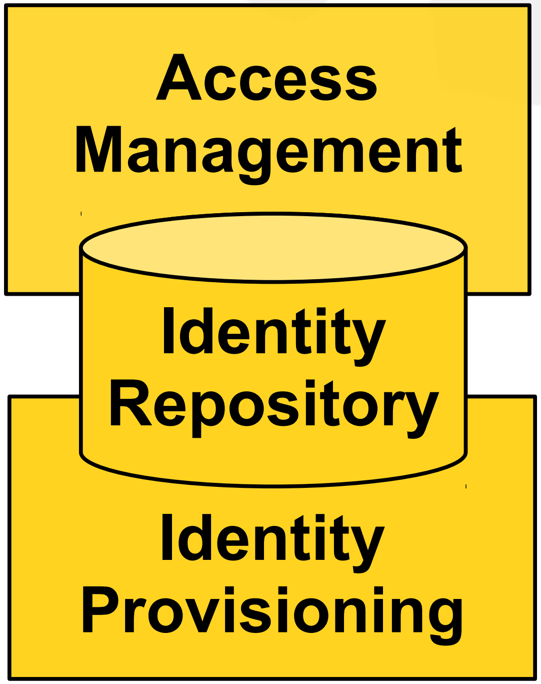
  as one system

- Easy product integration
- Smooth user experience
  - The user should not see component boundaries

Technology stacks

“Stack” is the obvious answer to interoperability problem.

… or … is it?



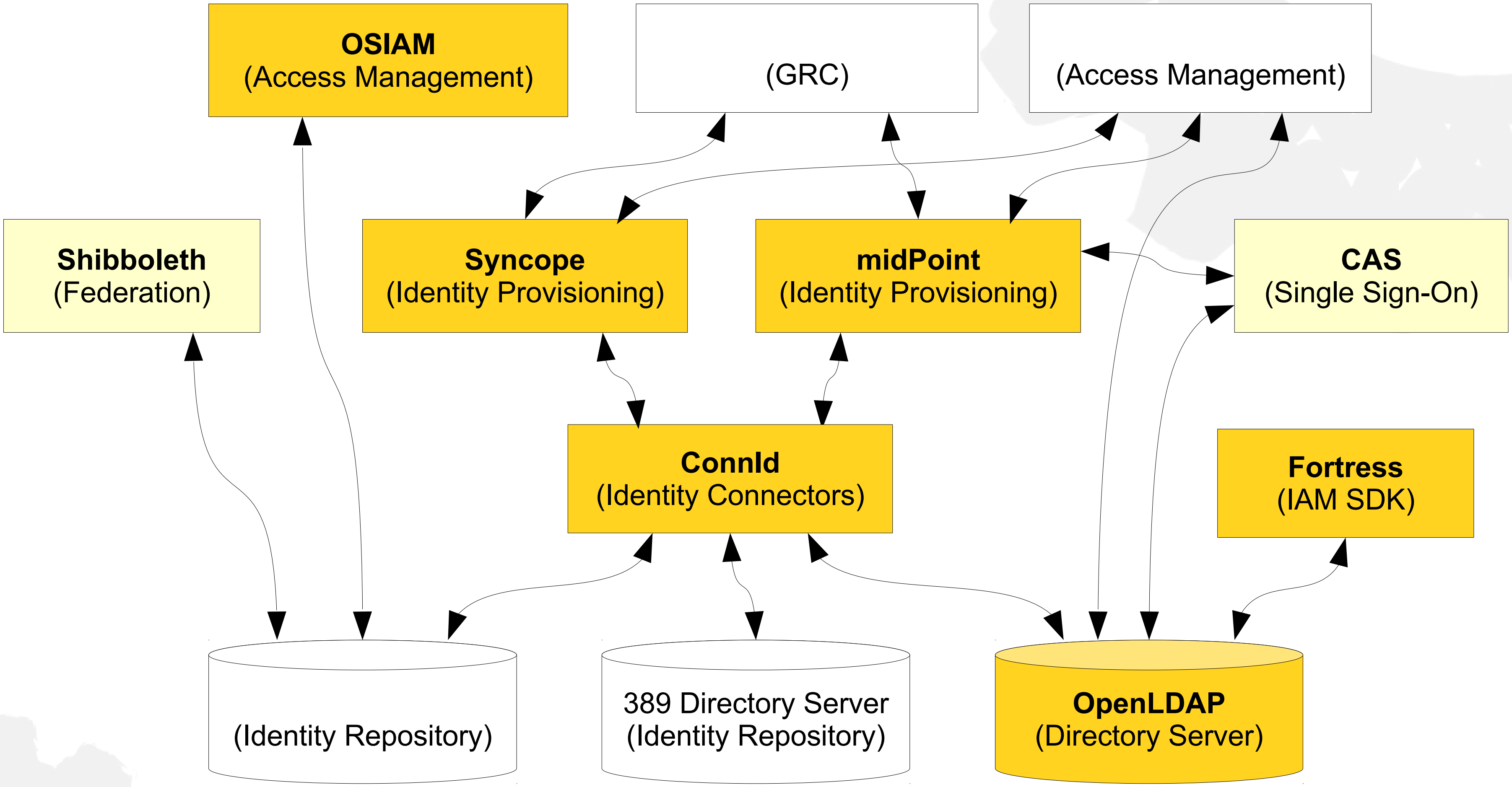
What's wrong with stacks?

- Usually single-vendor stacks
- Still quite heterogeneous due to acquisitions
- Vendor lock-in
  - You can check out any time you like, but you can never leave
- Limited integration options
  - Just one option for each component
  - Proprietary interfaces

Is there any better way?

The Ecosystem

Open Source Identity Ecosystem

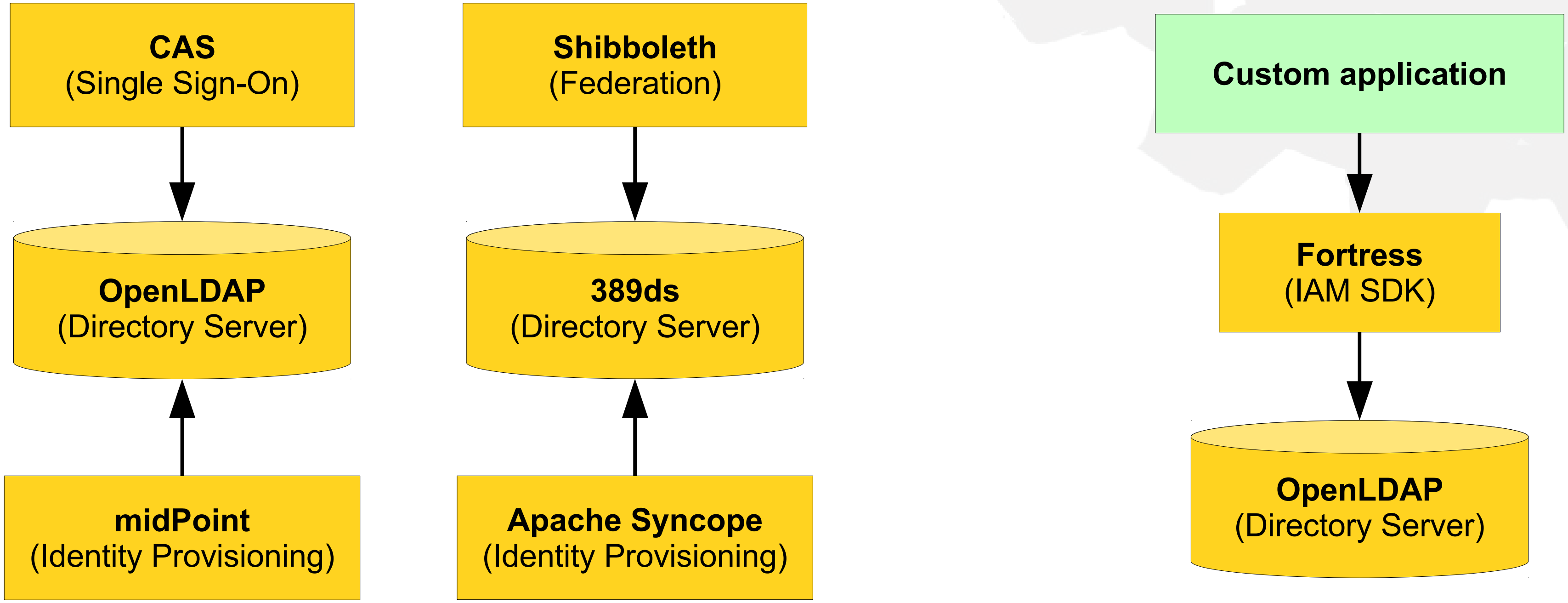


Evolveum

Open Source Identity Ecosystem

- Pure open source model
  - Any engineer can have complete understanding of the technology
  - Technological excellence and efficiency
- Standardized or open source interfaces
  - Unlimited integration options
  - Replaceable components → no vendor lock-in
- Cooperation instead of domination
  - Trade influence for control to get substantial benefits

Ecosystem Deployment Examples



CAS
(Single Sign-On)

OpenLDAP
(Directory Server)

midPoint
(Identity Provisioning)

Shibboleth
(Federation)

389ds
(Directory Server)

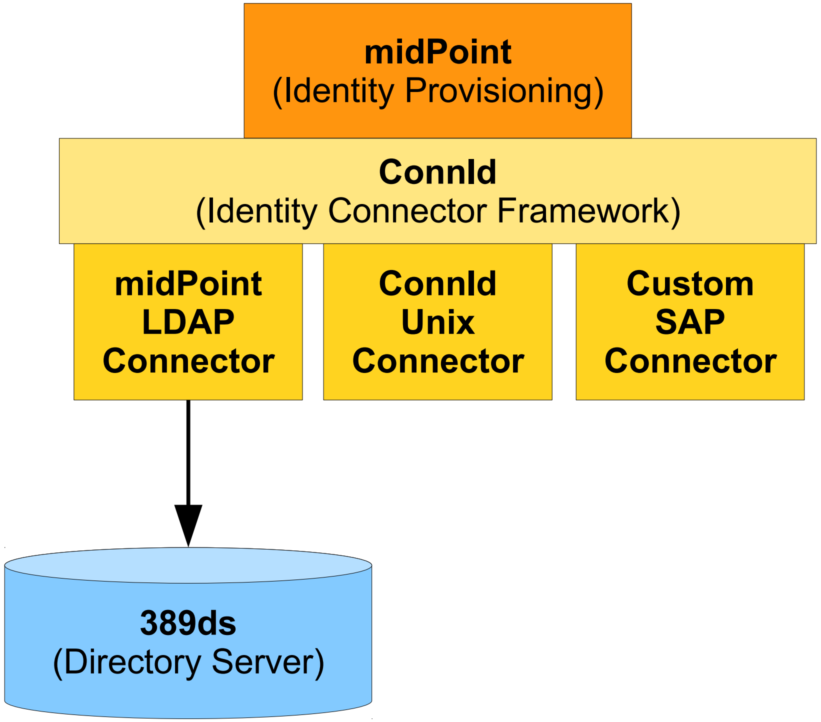
Apache Syncope
(Identity Provisioning)

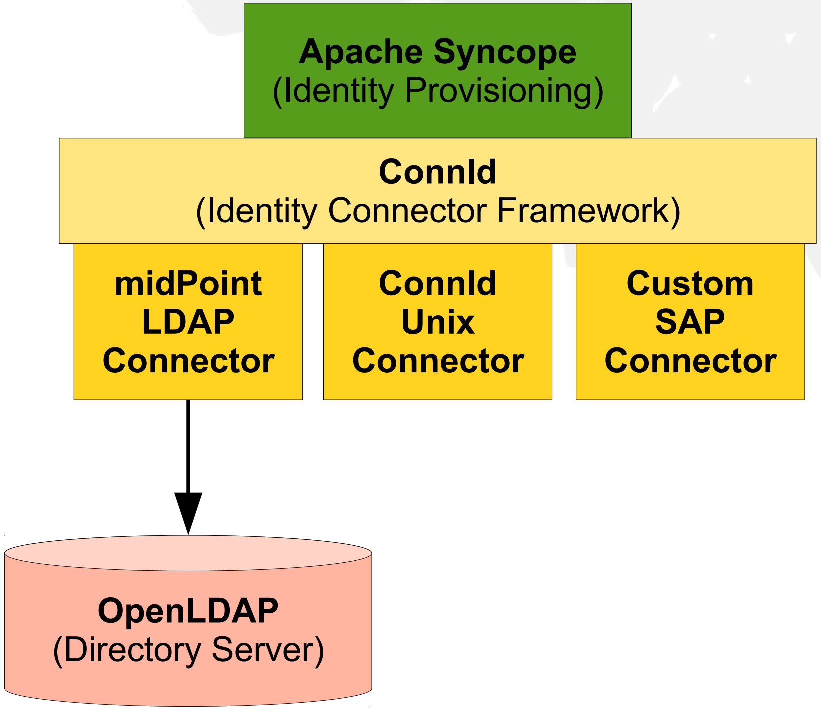
Custom application

Fortress
(IAM SDK)

OpenLDAP
(Directory Server)

Ecosystem Deployment Examples





Evolveum

We know that it works, because ...

- we have tested the technology
  - test suites, pilots, real projects
- we share the same goal
- there are business agreements in place

Join the Ecosystem now!

Questions and Answers

Thank You

Radovan Semančík

www.evolveum.com