Open Source Identity Management

OpenAlt 2015

Evolveum

Radovan Semančík
November 2015
Ing. Radovan Semančík, PhD.
Software architect
Co-owner of Evolveum (open source company)
Architect of midPoint project
Apache committer (Directory API)
What is this Identity Management?
Let's start with a story ...

- Pirate Brethren, Inc.
- Fictional company
- Starts small
- Lean, efficient
- Grows quickly
- Focus on profit
Simple and easy start

Keeping access rights matrix in spreadsheet
Some manual work but still quite OK
It gets quite complex very soon ...
Login Nightmares

Shippin' DeLuxe v99.02
Login: mjones
Password: 
Forgot password?

NaviGATE+
Username: p0054358
Password: 

Login: marry
Password: 

CrashSoft Woknous
Realm: PIRACY
Login: jones3
Password: 

Evolveum
# LDAPv3

# base <dc=example,dc=com> with scope subtree

# filter: (entryUUID=48b2295e-c131-4300-835a-fa85c863233e)

# requesting: ALL

# jack, people, example.com
dn: uid=jack,ou=people,dc=example,dc=com
mail: jack2@blackpearl.com
givenName: Jack
objectClass: person
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: top
uid: jack
cn: cpt. Jack Sparrow
sn: Sparrow

---

manual synchronization
(unreliable, slow, costly)

no feedback

--

Policy

untracked changes

---

Reality

---

Evolveum
# LDAPv3

base <dc=example,dc=com> with scope subtree

filter: (entryUUID=48b2295e-c131-4300-835a-fa85c863233e)

requesting: ALL

# jack, people, example.com
dn: uid=jack,ou=people,dc=example,dc=com
mail: jack2@blackpearl.com
givenName: Jack
objectClass: person
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: top
uid: jack
cn: cpt. Jack Sparrow
sn: Sparrow

**AUDIT**

VERY COSTLY

... and it has to be repeated ...
Call Center Goes Crazy

Access request

Password reset

Password reset

Password reset

Password reset

Access request

Password reset

Password reset

Password reset

Password reset

Password reset

Password reset

Password reset
Let's do this IAM* thing. Everybody is doing that.

*) Identity and Access Management
Manager's View

Implementation Details

Application

SSO

Users
High Level Architect's View

Implementation Details

LDAP

Application

Implementation Details

SSO

Users

Evolveum
Users

HR

Realities:

- Relational database
- Application
- LDAP
- Local copy
- SSO

Unsupported:

- Incompatible identifiers
- Custom schema
- No standard (ugly script needed)
- Incompatible schema

Unsupported!

Expensive:

Home directory

Extremely expensive
“Single directory” approach is not going to work

... and this has been known since 2006 (at least)
What are we going to do now?
DO NOT PANIC!

SSO is what you think you want

IDM is what you really need
What is this Identity Management (IDM) thing, again?
Identity and Access Management

- System Admin
- Requester
- Approver
- Identity Management
- Identity Repository
- HR
- CRM
- Application
- Users
- AM
- Evolveum
How IDM works?
Automatic user provisioning

Policies
RBAC
Rules

Identity Management

HR

Identity Repository

Application

AM

Evolveum
Password reset (self-service)
Employee Leaves Company
Automatic user deprovisioning

Identity Management

Policies
RBAC
Rules

HR

Application

Identity Repository

AM

Evolveum
Business As Usual
Bidirectional Synchronization
Policy enforcement

Policies
- RBAC
- Rules

Identity Management

Identity Repository

HR

Applications
What Identity Management does?

- Provisioning
- Synchronization
- Self-service
- Password management
- Credentials distribution (SSH, X.509)
- RBAC
- Organizational structure
- Entitlement management
- Identifier management
- Data mapping
- Segregation of duties
- Workflow
- Notifications
- Auditing
- Reporting
- Governance
- ...
Who needs Identity Management?

IDM Rule of the Thumb:

- < 100 identities: you are fine with manual work
- 100 – 1K identities: you might need it
- 1K - 10K identities: you need it
- > 10K identities: you desperately need it!
This **IDM** looks like the best thing since the sliced bread. What's the catch?
This **IDM** looks like the best thing since the sliced bread. What's the catch?

The *commercial* IDM products are expensive.
This **IDM** looks like the best thing since the sliced bread. What's the catch?

The **commercial** IDM products are expensive.

Very, very expensive.
Open Source to the Rescue

There was no practical FOSS solution until 2010

(Sun Identity Manager was the king)

2010-2011: Syncope, OpenIDM, midPoint, ...

(that was the time when Oracle acquired Sun)

Now there are two leading open source* IDMs:

● Apache Syncope
● Evolveum midPoint

*) by “open source” I mean both license and practice
Evolveum midPoint?
The midPoint Story

- Started 2010-2011 (5 years, 14 releases)
- Github, Apache 2.0 License
- ~500K lines of code (Java)
- State-of-the-art IDM features
Complete Open Source Solution

midPoint

Identity Management

Identity Repository

CAS

AM

Application

Application

CRM

HR

Users

OpenLDAP
Conclusion
Access Management

- Authentication
- Single Sign-On (SSO)

- Quite expensive

What people want

Identity Management

- Provisioning
- RBAC
- Synchronization
- Password management
- Self-service
- … and much more
- Cost reduction

What people need
Access Management

- Authentication
- Single Sign-On (SSO)
- Quite expensive

What people want

Identity Management

- Provisioning
- RBAC
- Synchronization
- Password management
- Self-service
- … and much more
- Cost reduction

What people need

START HERE
Questions and Answers
Thank You

Radovan Semančík

www.evolveum.com
Extra Slides
(Much) More Information

• midPoint Wiki
  • https://wiki.evolveum.com/display/midPoint/Home

• Architecture and Design (in Wiki)
  • Wiki pages under [Architecture and Design] page
  • “Live” architecture documentation
  • Includes UML diagrams
  • We try to keep it (reasonably) up to date

• midPoint Mailing List
Example midPoint Deployment Architecture

- midPoint Identity Repository (Relational DB)
- Custom HR System
- CSV File
- Scheduled Exports
- Web GUI
- User Self-Service (Web GUI)
- Administrator
- Microsoft Applications
- Active Directory
- AD Connector (remote)
- ADSI
- SQL
- Database Applications
- Oracle Database
- FlatFile Connector
- DB Table Connector
- IDM Logic
- Identity Management Policies (rules, processes)
- midPoint
Identity Connectors

• Common Identity Connector Framework
  • Sun Identity Connector Framework → ConnId

• Compatible connectors
  • AD, DB Table, DB2, MySQL, Oracle, RACF, Solaris, SPML, VMS, FlatFile, XML, Solaris, SAP, ...
  • LDAP: OpenLDAP, 389ds, OpenDJ, eDirectory, Active Directory
  • CSV file, Office365, SAS, GitLab, Lotus, LifeRay
Live Demo

http://demo.evolveum.com/

Documentation: search for “Live demo” in wiki.evolveum.com