Identity Management with midPoint

Radovan Semančík
FOSDEM, January 2016
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
Identity and Access Management

- Identity Management
- Identity Repository
- Application
- System Admin
- Requester Approver
- HR
- CRM
- Users
- AM
There is no security without identity management
If you have no IDM, how can you be sure that ...

- illegal accounts are disabled/deleted?
- temporary accounts are deleted?
- users have only the least privileges?
- the privileges are not accumulated?
- no secondary authentication is possible?
- the data are up to date? (title, affiliation, …)
- notifications and tasks are suspended?
The solution is trivial
Let's put **everything** in LDAP!
Expectation
Reality

HR

LDAP

Relational database

Application

Users

Unsupported

Incompatible identifiers

No standard (ugly script needed)

Incompatible schema

Custom schema

Local copy

SSO

Unsupported

Expensive

Home directory

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

... and this has been known since 2006 (at least)
Identity and Access Management
How IDM works?

Identity Management

Identity Repository

HR

Application

AM
Automatic user provisioning

Identity Management

Policies
RBAC
Rules

Identity Repository

HR

Application

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

Identity Management

HR

Identity Repository

Application

AM
Policy enforcement

Policies
RBAC
Rules

Identity
Management

AM

Identity Repository

HR

Application

Application

Application

Application
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
- ...

Evolveum
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?
midPoint

Identity Management

Identity Repository

CRM

HR

Application

AM

Users
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
Questions and Answers

Provisioning
Synchronization
RBAC
Governance
Consistency
Workflow
Audit
Authorization
Management
Delegated administration
Data mapping
REST
Policy
Entitlements
Segregation of duties
Password reset
Organizational structure
Connectors
HA
Web UI
Governance
Scripting
Self-service
Parametric roles
Bulk actions
Conditions
Expressions
Provisioning
Management
Schema
Extensibility
Consistency
Workflow
Entitlements
Connectors
HA
Delegated administration
Data mapping
REST
Identifiers
Notifications
Localization
Evolveum
Thank You

Radovan Semančík

www.evolveum.com