Evolveum

Authentication and Authorization Infrastructure (AAI)

Slavek Licehammer
slavek@evolveum.com
10. 5. 2021

AAI – main logical components

- Identity management
  - Centralized DB of identity objects (user, groups, roles, …)
  - Authorization definitions
  - Provisioning
  - Primary for administrators, managers, ...
- Access management
  - Authentication, single-sign on
  - Can support federated authentication
  - User-facing component

Building AAI

- Legacy systems
- Various protocols
- Lack of standardization
- Various requirements
- Variety of existing components and solutions

Evolveum

MidPoint Overview

Slavek Licehammer
slavek@evolveum.com
10. 5. 2021

MidPoint

- Identity management
- Provisioning, synchronization
- Identity governance

- MidPoint **is not** access management, SSO

Main principles of midPoint

- Open Source
- MidPoint will adapt to your use-cases and workflows
- Lots of configuration options
  - Might get complex
  - Better than be limited by the tool
- Consistent and integrated features
- Continuous improvement
  - Supporting midPoint community
  - Gathering feedback
  - Easy to upgrade to new versions

Provisioning & integration

- ConnId Framework
- MidPoint will adapt to your use-cases
- Custom attributes mapping, rules, ...
- Synchronization/(de-)provisioning
- Designed to enhance existing environment
  - Dry-run
  - Correlations, tolerant patterns, ...
- REST interface

Identity management

- Hybrid RBAC (roles + parameters)
- Organizational structure (support of multiple roots)
- User life-cycle
- Progressive user profile
- Support different personas on a user
- Self-service
- Approvals
- Privileges delegation

Identity governance

- Policies
  - Global, per object types, per specific objects, …
  - Segregation of duties
  - Managing licenses for external systems
- Policy compliance, remediation
- Life cycle of roles
  - Drafted, proposed, activated, deprecated, archived
  - Customization, approval process, ...
- Re-certifications
- Auditing
- Reporting and data exports

Future plans

- Focus on higher education
- Further improvement of identity governance features
- Identity provenance and privacy enhancing features
- …and more, based on user requirements

MidPoint technical info

- Java application
  - SQL DB (PostreSQL)
- Distributed with embedded tomcat
  - Docker image also available
- Scaling to million of managed objects
  - Improvements in progress
- Supports clustering
- Long term support versions (LTS)

Evolveum

- Company developing midPoint, providing support, training and consultations
- Subscription based support
- Stable team (developers, identity engineers, …)
  - Approximately 27 people
- Partners network
  - Approximately 28 partners
- Collaboration with Internet2
- Focus on automation, innovation and added value

MidPoint summary

- Open-source
- Identity management
- Identity governance
- Designed to be flexible
- Wide configuration options
- Pushing boundaries in IdM area

Thank you for your time

If any questions occur, feel free to ask at slavek**@evolveum.com**

Also **follow us** on our social media for further information!

/Evolveum

/Evolveum

/Evolveum

@Evolveum

/Evolveum

Evolveum