Vision for Identity Management in Higher Education

Slavek Licehammer
slavek@evolveum.com
November 2020

Who am I

- Affiliation: Evolveum, Masaryk University
- Engaged in AAI / IdM for more than 10 years
- Experience with designing, building, and operations of AAI(s)
  - Designing new features based on requirements from different domains
- Focus on higher education and research environments

IdM Evolution

- Zero generation
  - Cron & scripts
  - (Semi-) automatic identity management
- First generation
  - Real IdM and IAM systems
  - Provisioning and deprovisioning
  - Full automation

Evolveum

IdM Evolution

- Second generation
  - Access rights delegation, self-service
  - Governance
  - Policies, Certifications
  - Auditing and reporting
  - Objects life-cycle (not only users)
  - Privacy preserving features
- Hard to draw a line
- It’s still evolving

Where are we now?

- Somewhere between 1st and 2nd generation
- Everyone have different priorities on implementing new features
- (De-)Provisioning is still problematic
  - Lack of widely applicable standards
- Self-service is complicated for users
- Guest/visitors accounts issues
- Scalability
- Infrastructure and operations

Broader scope

- How to collaborate with other organizations
- Identity federations
- Account linking
- Self-service
- Provisioning between IdMs
- Standardization

Evolveum

Vision in IdM

- IdM is not only for managing identities it’s powerful data source
- IdM supporting other systems/use-cases
  - Service catalog
  - Privacy enhancement
  - ...
- Tighter internal integration
- Cross-organizational collaborations
- Identity governance
  - Policy driven IdM

Evolveum

Small steps

- Focus on automation
- Clean your data
- Unified IdM and Access management for all services
- Empower your users
  - IdM team have to focus on improvements, not support

Evolveum

Examples with midPoint

- Let’s examine some IdM features
- Let’s see midPoint’s approach to deal with them

Evolveum

IdM as central system

Evolveum

Other IdM and IdM-related components

- IdM have wide reach but will never handle everything
- Integration with other components are crucial
- Access management (SSO)
- Other systems for managing groups and attributes
- Legacy IdM components
- External IdM systems

Evolveum

Provisioning, deprovisioning

- Solved using service connectors/configurations
- SCIM often needs custom schema
  - Specialized configuration per service
- Speed might be crucial
  - In reality often isn’t
- Need for full synchronization from time to time
- Messaging often complicates operations

Evolveum

Provisioning, deprovisioning

midPoint

- ConnId – open-source identity connectors framework
- Bi-directional
- Using delta updates
  - Speed
- Live-sync for inbound synchronization
- Updates from IdM are immediately provisioned
- Full-sync supported simultaneously

Evolveum

Rights delegation, self-service

- IdM engineers should only integrate new services
  - Design representation in IdM
  - Hide technical complexity from users
- Day to day operations should be delegated
  - Add/remove role to users
  - Approvals
  - Setting expiration and other manual part of life-cycle

Rights delegation, self-service

midPoint

- Smart roles (archetypes)
- Internal roles
  - Managed by IdM engineers, otherwise hidden
  - Contains all technical complexity
- User-facing roles
  - Available for selected users
  - Well described
  - Can be assigned only to correct object
- Result: users can manage access rights on their own

Evolveum

Archetypes – problem statement

- Objects in IdM can represent various things
  - Employees, students, contractors, service accounts, org. units, projects, groups, classes, entitlements, roles, privileges, services, devices, ...
- IdM manages attributes and relations between objects
- How to organize this?

Archetypes

- Archetypes are used for categorization (sub-type)
- midPoint doesn’t restrict individual objects
  - Any IdM object can represent anything
- Archetypes can have own visualization
- Archetypes can carry limitations, policies, extensions

Relations

- Basic relations are simple
  - User has a role, user is in a group, group has a role, ...
- It will get complicated
  - User can be student or employee of a faculty
  - … or both
- Relation can have internal usage in IdM
  - e.g. owner or approver
  - … but no reason not not use them in provisioning

Evolveum

Relations

midPoint

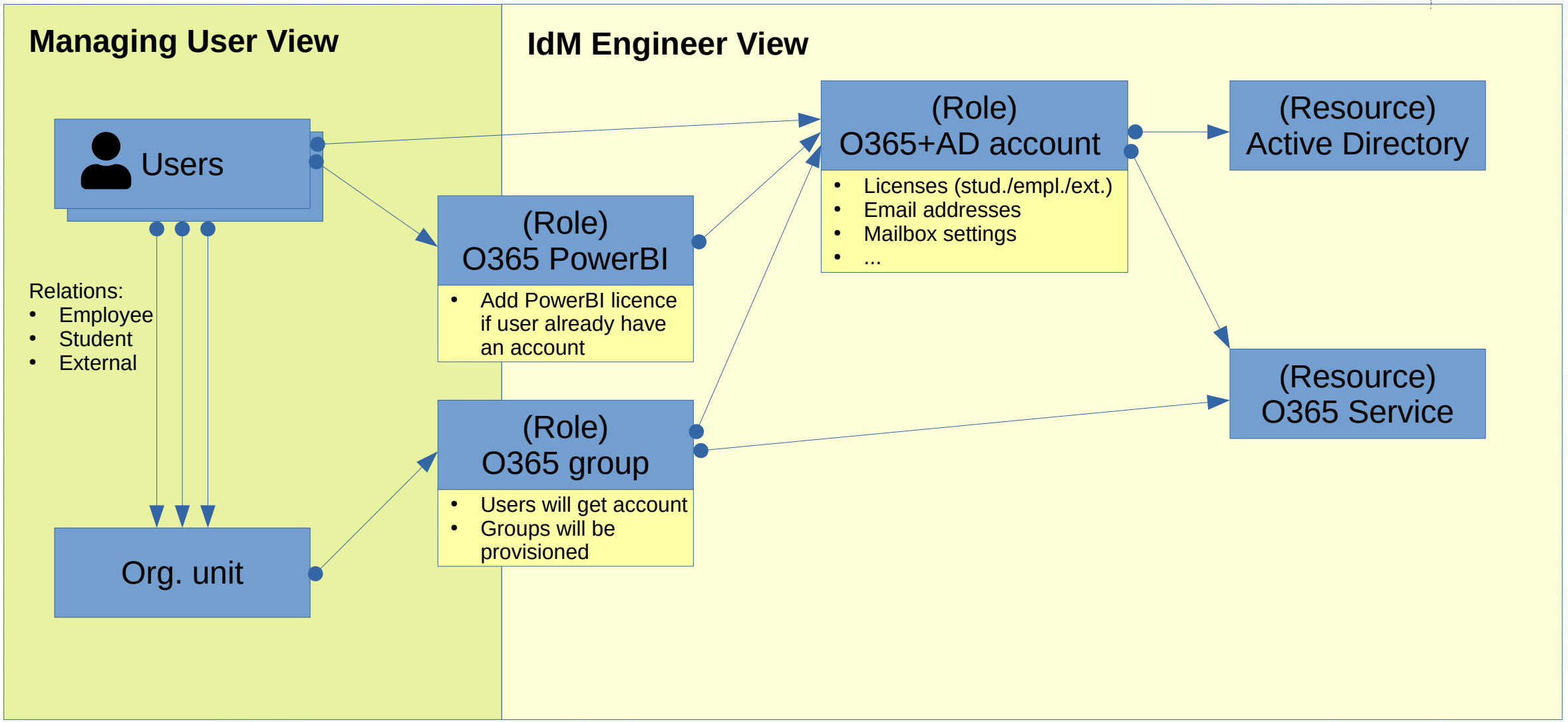
- Different types of relations are supported
- Allowed relation types are configurable per object
  - Can be fine-tuned using Archetypes
- Provisioning rules are fully configurable
- Internal interpretation of relations are fully configurable
- Complexity can (and should) be hidden from users

Smart roles and relations

midPoint

- Complexity is hidden from users
  - In configuration and objects available only to IdM Engineers
- midPoint allows only valid operation (e.g. assignments)
- Roles and other objects are distinguishable and clearly labeled
- Can be combined with other features
  - Policies, approval processes, …
  - Usually hidden from users

Smart roles example



Demo

Smart roles – future plans

- Parametric roles and relations
  - Going further beyond RBAC
  - Preventing role explosions
- User experience improvements
- Configuration options improvement

Evolveum

Conclusion

- Future is not that far
  - IdM systems offers more that we are using
  - Lots of features are already available – just try them
- IdM area still have huge potential
- Evolveum goal is to push boundaries
  - Focus on higher education and research environment
  - Join the discussion with us

Evolveum

Useful links

- midPoint mailing list
  - https://lists.evolveum.com/mailman/listinfo/midpoint
- midPoint in higher education blog series
  - https://evolveum.com/midpoint-in-higher-education-introduction/
  - https://evolveum.com/midpoint-in-higher-education-archetypes/
  - https://evolveum.com/midpoint-in-higher-education-orgs-roles-and-relations/
- #incommon-midpoint channel on Internet2 Slack
- slavek@evolveum.com

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