MidPoint Deployment Fundamentals

MID-101

revision 4.0-LTS-C

Course Goals

- Deploy and configure midPoint in enterprise environment
- Configure resources
- Create mappings for resource attributes
- Create and maintain role definitions (RBAC)
- Use initial import, LiveSync and reconciliation

Course Goals (2)

- Extend XML Schema
- Create organizational structure
- Enforce policies using Object Templates and mappings
- Configure notifications
- Admin GUI configuration

Evolveum®

Course Goals (3)

- Create authorization roles in midPoint
- Understand associations between accounts and entitlements (groups)
- Create and maintain password and security policies
- Manage connectors in deployed solution
- Troubleshoot, backup and restore the system

Evolveum®

Course Map

Module 1 **Basic IdM & midPoint Concepts**	**Module 2** **Managing Your Customizations**	**Module 3** **Resources, Attributes and Mappings**
Module 4 **Provisioning to Resources**	**Module 5** **Accounts, Assignments And Roles**	**Module 6** **Configuring Multiple Account Intents**

Course Map (2)

Module 7

Synchronization Flavours

Module 8

Extending midPoint Schema

Module 9

Organization Structure

Module 10

Object Templates

Module 11

System Configuration

Module 12

Authorizations

Evolveum®

Course Map (3)

Module 13

Entitlements and Associations Introduction

Module 14

Password and Security Policies

Module 15

Backup, Restore and Upgrade

Module 16

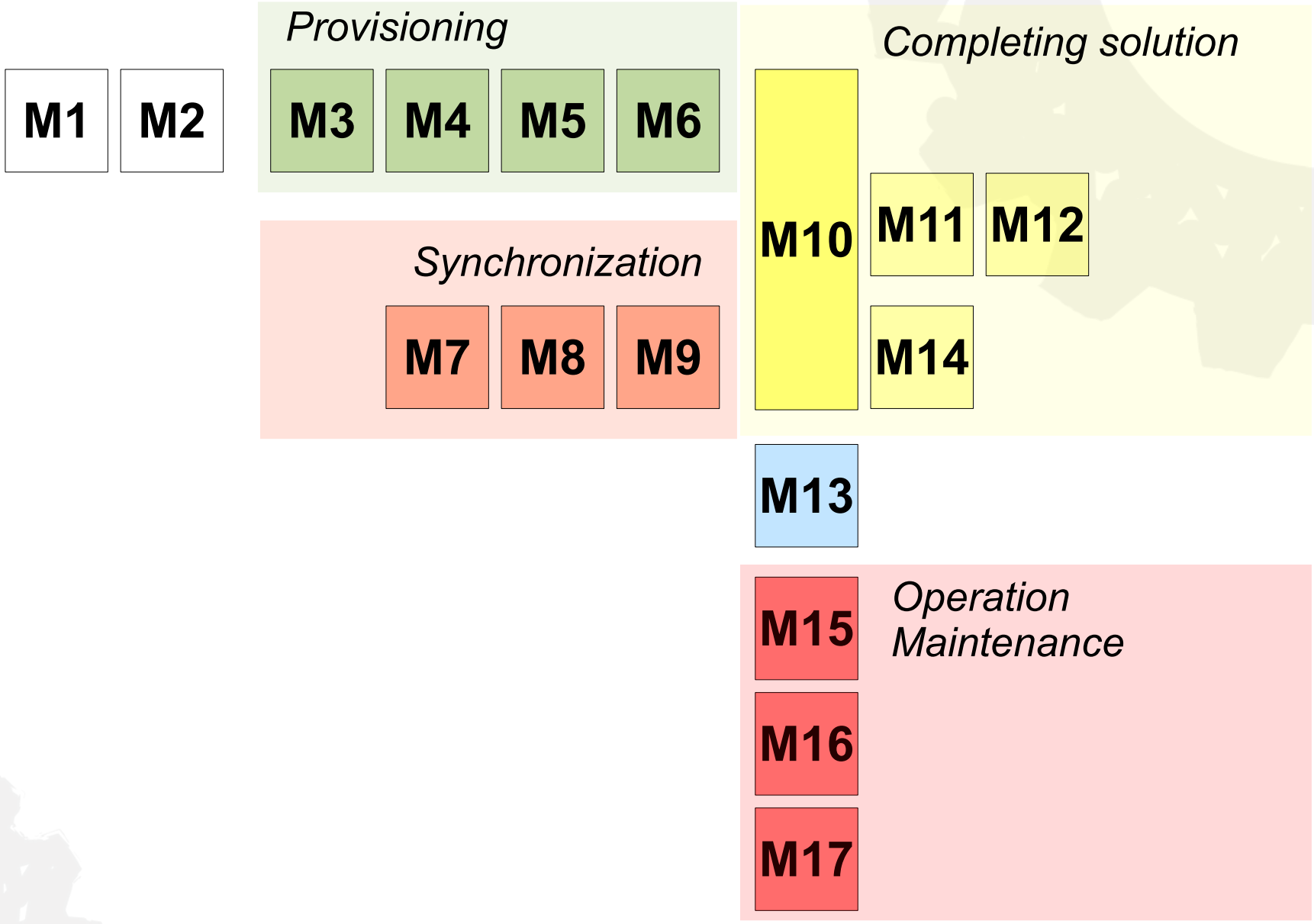
Managing Connectors

Module 17

Logging and Troubleshooting

Evolveum®

Course Module Relations



Note

- This is a **sample** of our training materials
- Please contact **sales@evolveum.com** to order a real training course session

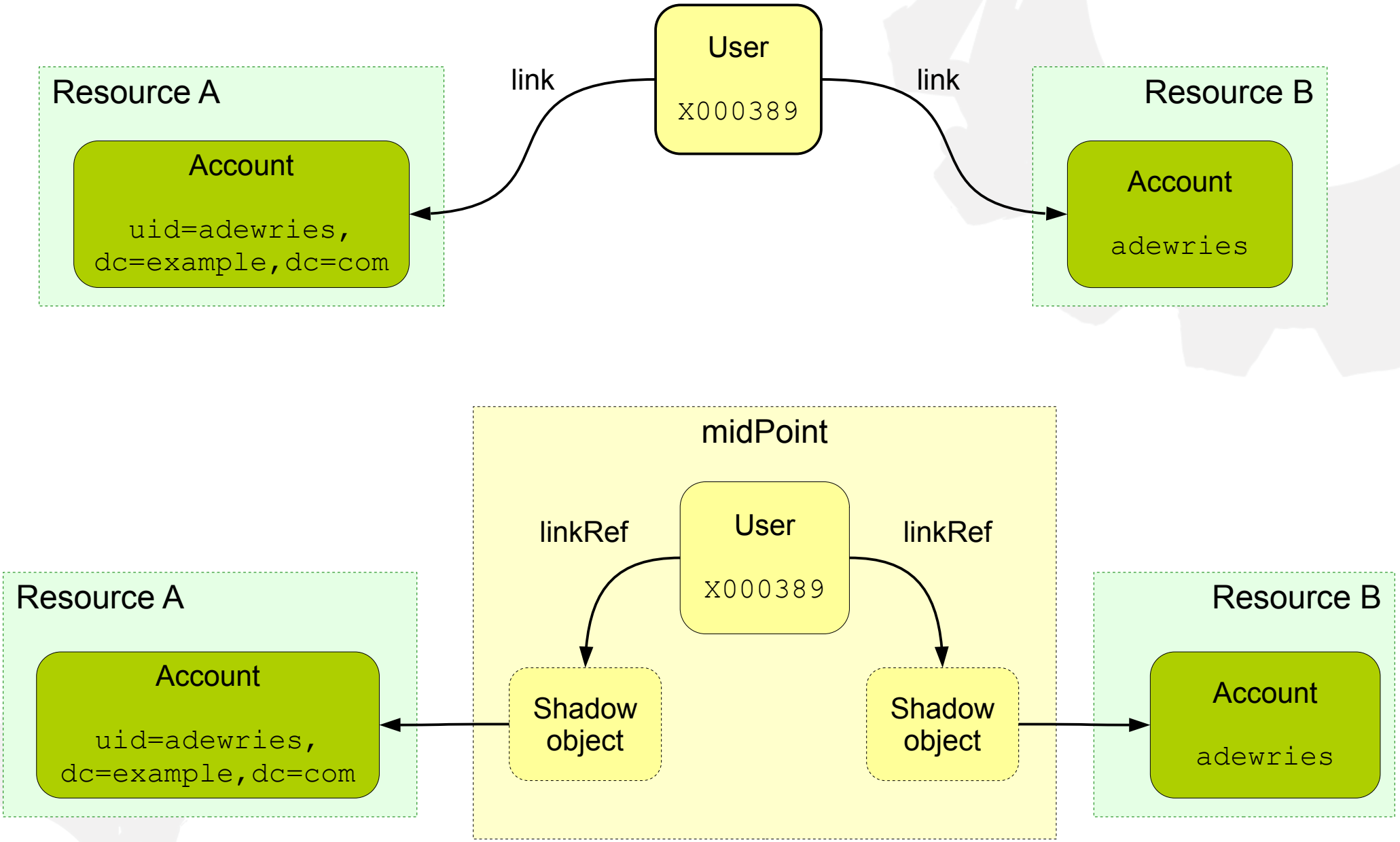
Module 5: Accounts, Assignments and Roles

User and Accounts

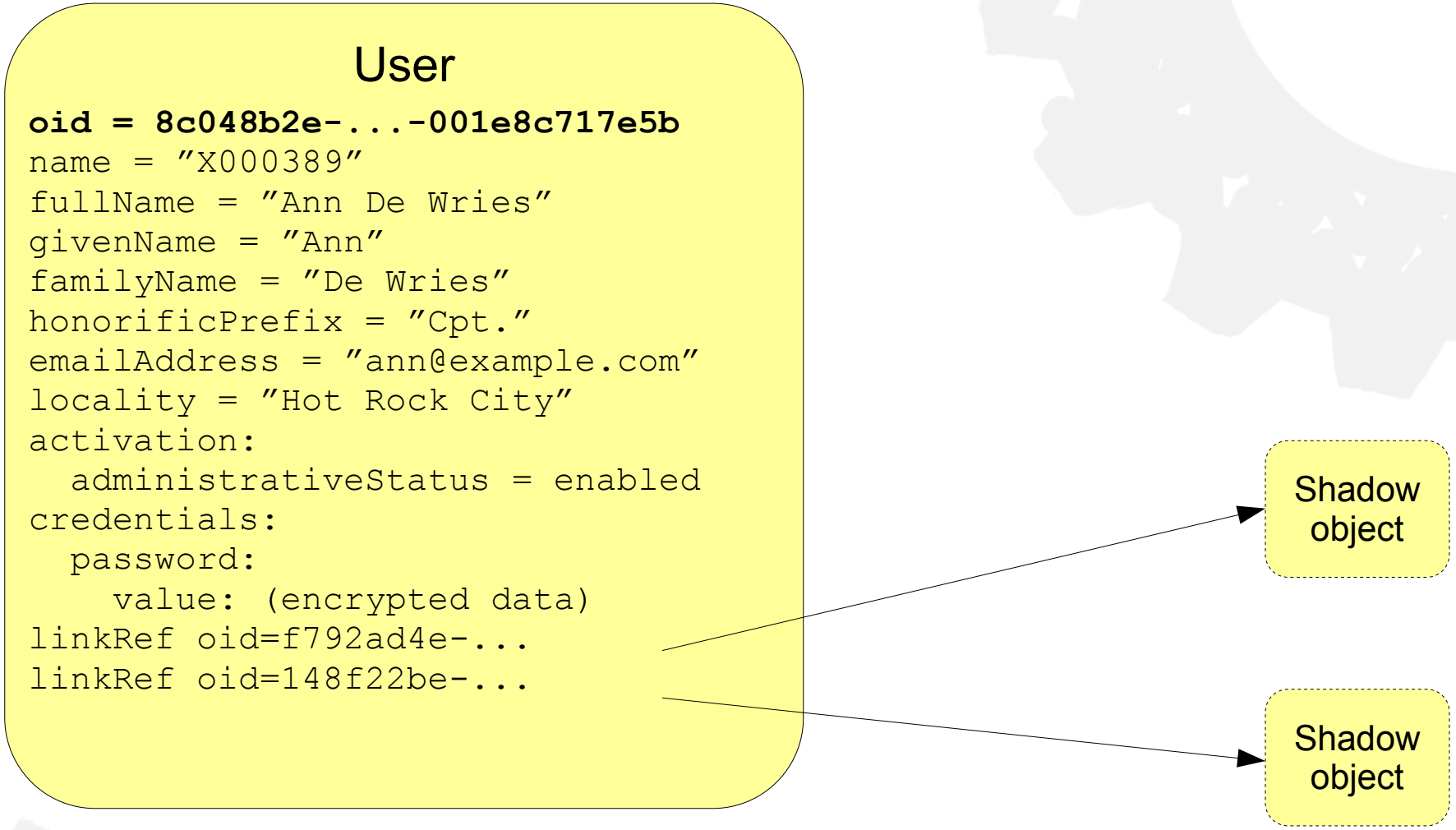
- User represents the identity (employee, contractor etc.), it resides in midPoint
- Accounts reside on target systems
- Accounts have variable attributes, their meaning and representation
  - One identifier vs multiple
  - Syntax of identifier(s) differs (string, integer)
- Integration handled by midPoint

Evolveum®

User and Resource Accounts



User



User and Resource Accounts (2)

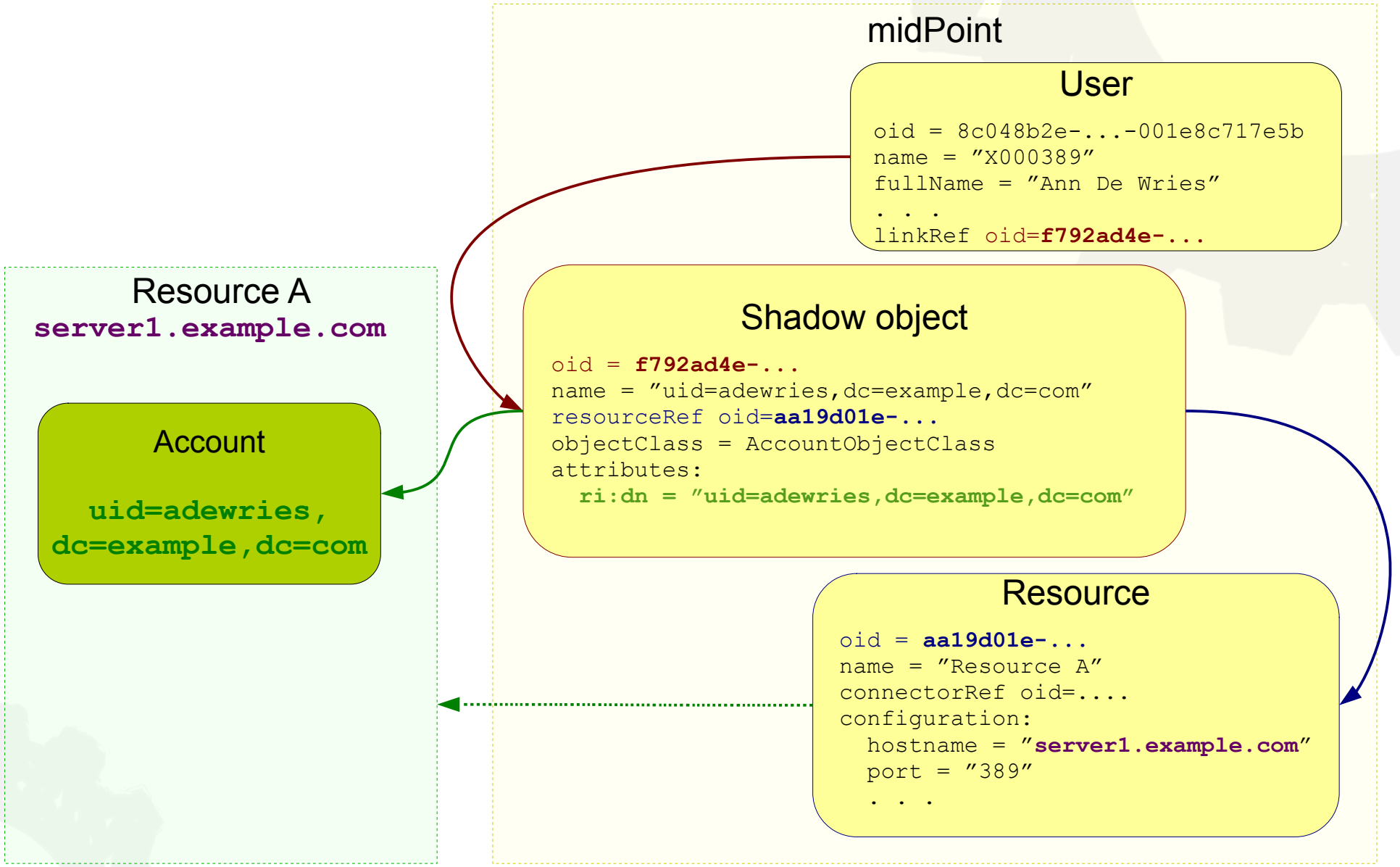
- Attributes (schema) and account identifiers differ between target systems
- Account resides on the resource, it is not a midPoint object but a projection (no oid)
- MidPoint maintains the link user → account
  - Intermediate Shadow objects are used
  - Static schema

Evolveum®

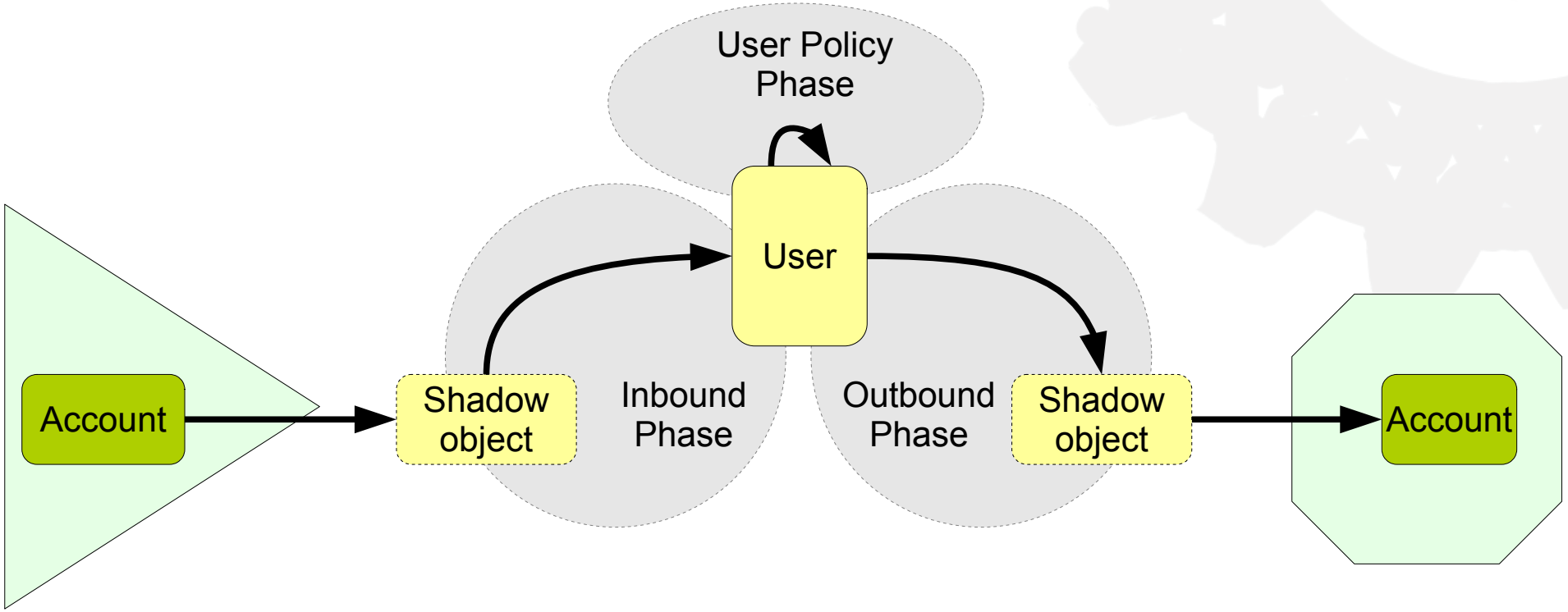
Shadow Object

- Object that connects midPoint world (repository) to the outside world (resource)
- Object in repository mirroring some of the account characteristics such as identifier(s) of the account (fixed schema)

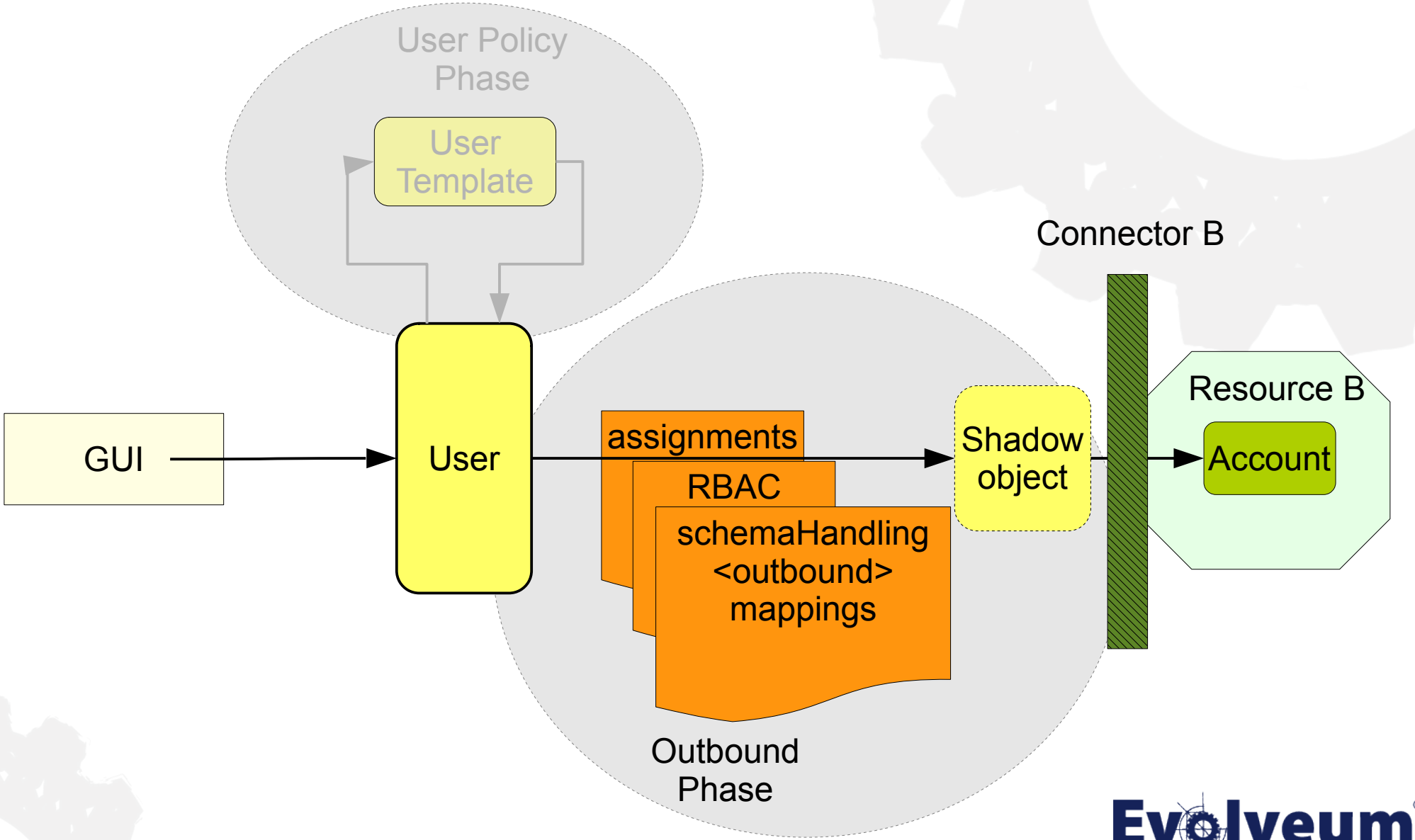
Users-Accounts Links Implementation



MidPoint User Provisioning Phases



Outbound Phase Detail



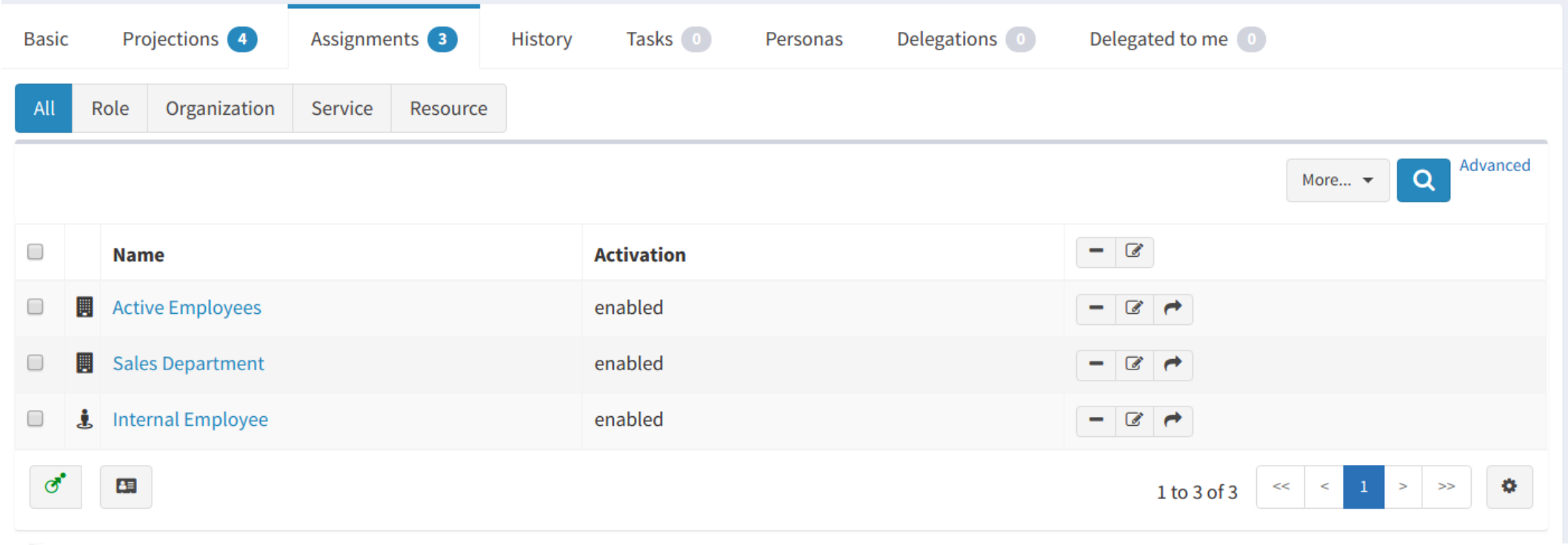
Linked Accounts vs. Assignments

- Link: User-account relationship
  - What IS on the resource
- Assignment: User-assignment-account(s) relationship
  - What SHOULD be on the resource(s)

Assignment Types

- Account Assignments
  - Roles not required
- Role Assignments
  - Create roles first, assign them to users
- Organization Structure Assignments
  - OU membership
- Archetypes

Assignments in GUI



Lab 5-1: Using RBAC

Lab 5-2: Segregation of Duties

Lab 5-3: Shadows and Projections

Lab 5-4: Creating Roles

Lab 5-5: Disable on Unassign

Lab 5-6: Inactive Assignment

Lab 5-7: Archetypes Introduction

Module Summary

- *Should be* vs. *Is*
- Assignment types
- Shadows and linkRefs
- RBAC, Assignments and Inducements
- Disable instead of delete
- Assignment Activation
- Archetypes

Evolveum®

End of Module 5

Conclusion

Questions and Answers

Follow Evolveum

- **Web**: www.evolveum.com
- **Blogs**: https://evolveum.com/blog/
- **Twitter**: https://twitter.com/evolveum
- **FB**: https://www.facebook.com/evolveum