MidPoint Deployment Fundamentals

MID-101

revision 4.4-LTS-E

(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

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

(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Course Goals (2)

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

(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Course Goals (3)

- Create authorization roles in midPoint
- Understand associations between accounts and entitlements (groups)
- Create and maintain password and security policies

(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Course Goals (4)

- Backup, restore and upgrade midPoint
- Manage connectors in deployed solution
- Understand deployment best practices
- Troubleshooting introduction

(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Course Map

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

(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

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

(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

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

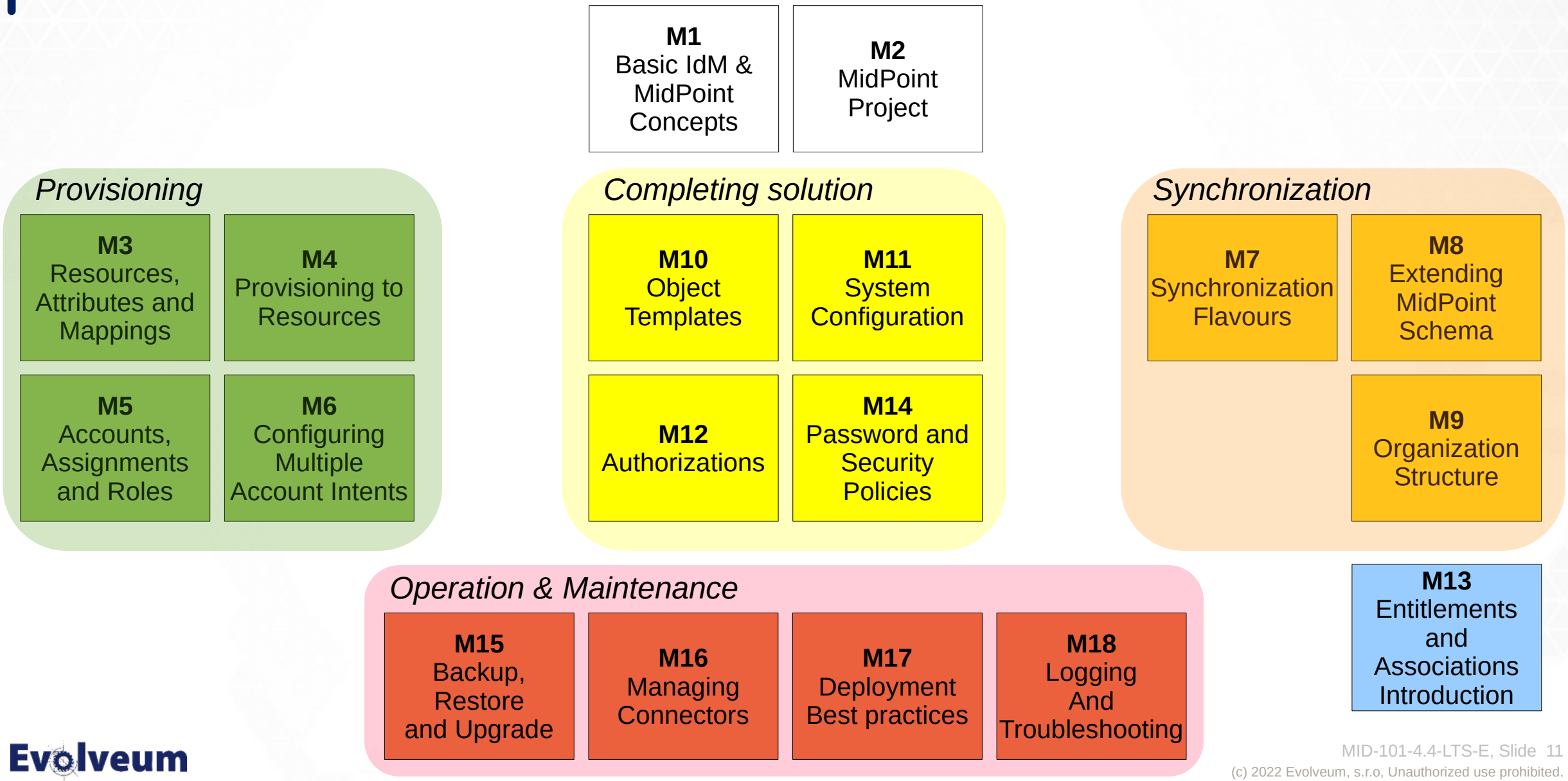
Deployment Best Practices

Module 18

Logging and Troubleshooting

(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Course Map Relations



(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Note

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

(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Accounts, Assignments and Roles

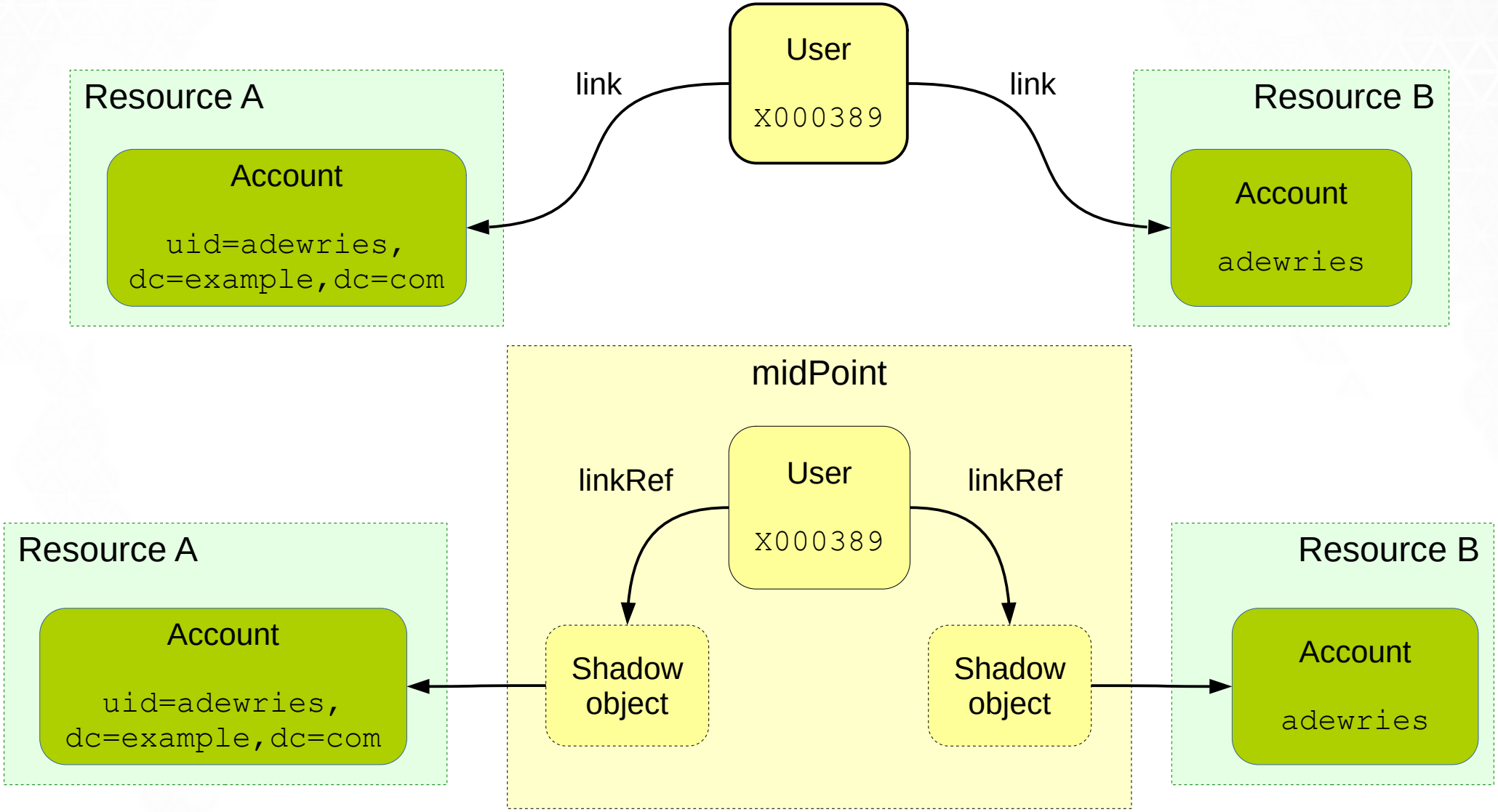
(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

User and Resource 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 vs multiple identifier(s)
  - Syntax of identifier(s) differs (string, integer)
- Integration handled by midPoint

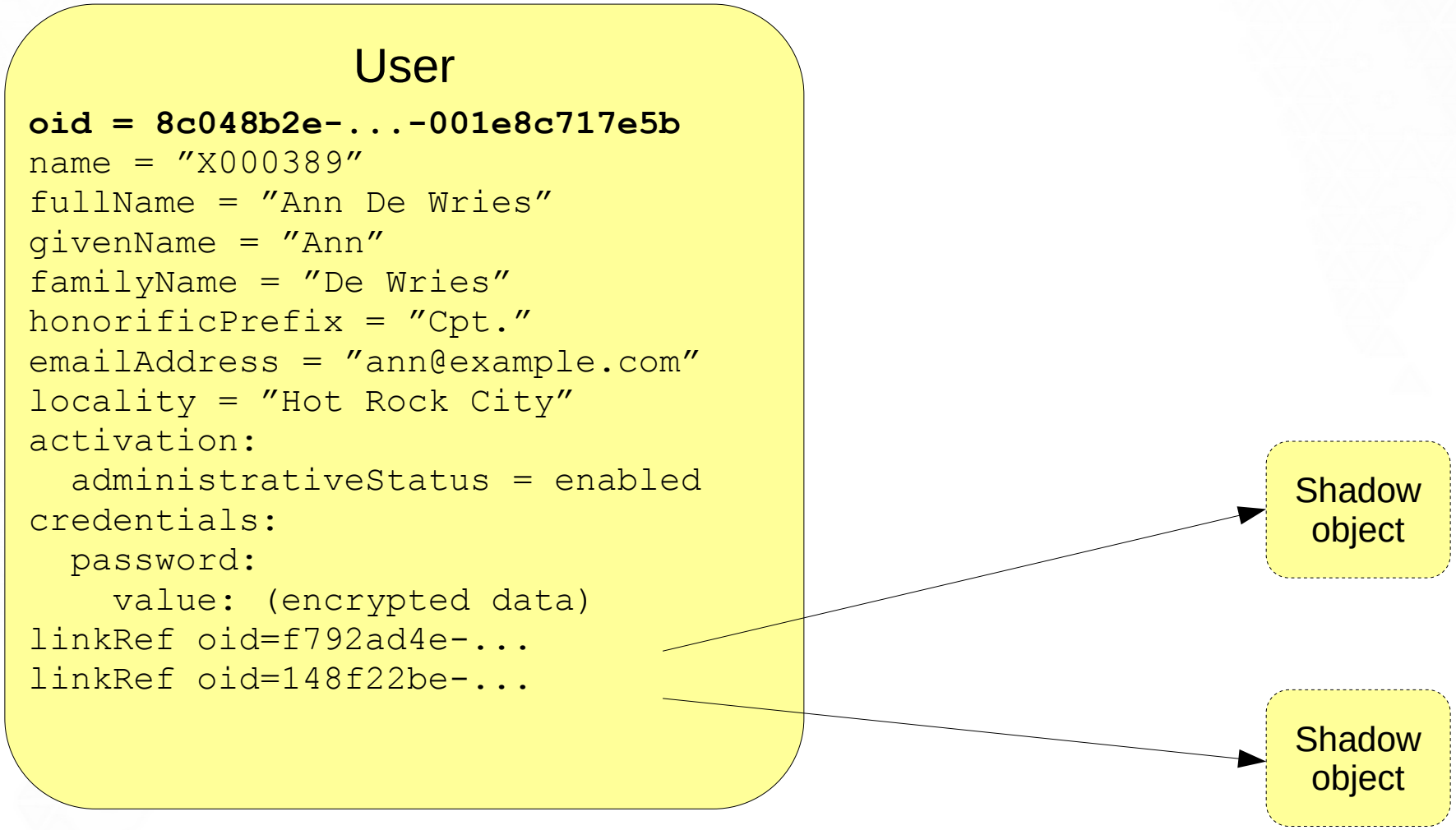
(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

User and Resource Accounts (2)



(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

User and Resource Accounts (3)



(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

User and Resource Accounts (4)

- 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

(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Shadow Object

- Object that connects midPoint world (repository) to the outside world (resource)
- Equivalent of resource object of which midPoint is aware
- Object in repository mirroring some of the account characteristics such as identifier(s) of the account (fixed schema)
- Other data is fetched on demand or cached
- You will probably never need to modify it directly

(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Shadow Object (2)

- Stored identifiers depend on the target system and/or connector

Most connectors	Polygon LDAP connector	Polygon CSV connector*
icfs:name	ri:dn	ri:<custom>
icfs:uid	ri:entryUUID	ri:<custom>

(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Shadow Object In Repository

```
<object ... oid="11001ad7-ca95-4de0-9849-8a42f9c817de" xsi:type="ShadowType">
  <name>uid=adewries,dc=example,dc=com</name>
. . .
   <resourceRef oid="ef2bc95b-76e0-48e2-86d6-a000ff000003"/>
   <objectClass ...>qn792:AccountObjectClass</objectClass>
. . .
   <attributes>
      <ri:dn>uid=adewries,dc=example,dc=com</ri:dn>
   </attributes>
</object>
```


(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Shadow Object in Memory

Shadow object of an account

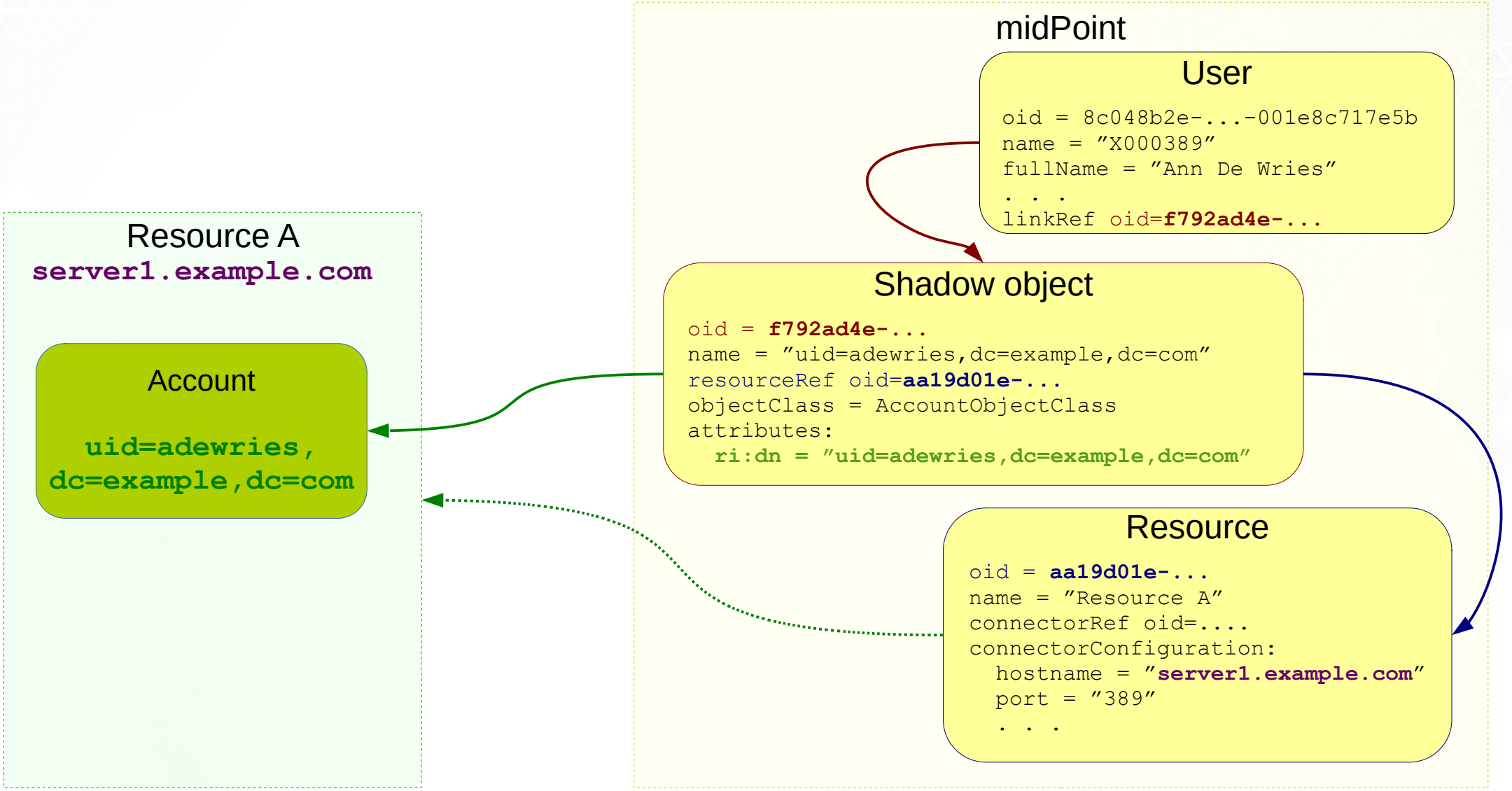
```
oid = f792ad4e-...
name = ”uid=adewries,dc=example,dc=com”
resourceRef oid=aa19d01e-...
objectClass = AccountObjectClass
attributes:
  dn = ”uid=adewries,dc=example,dc=com
  uid = ”adewries”
  cn = ”Ann De Wries”
  sn = ”De Wries”
  givenName = ”Ann”
activation:
  administrativeStatus = enabled
credentials:
  password:
    value: (encrypted data)
```

ConnId special(s)
Stored in repo
(one or more)

Resource object attributes (dynamic; different for each target system)

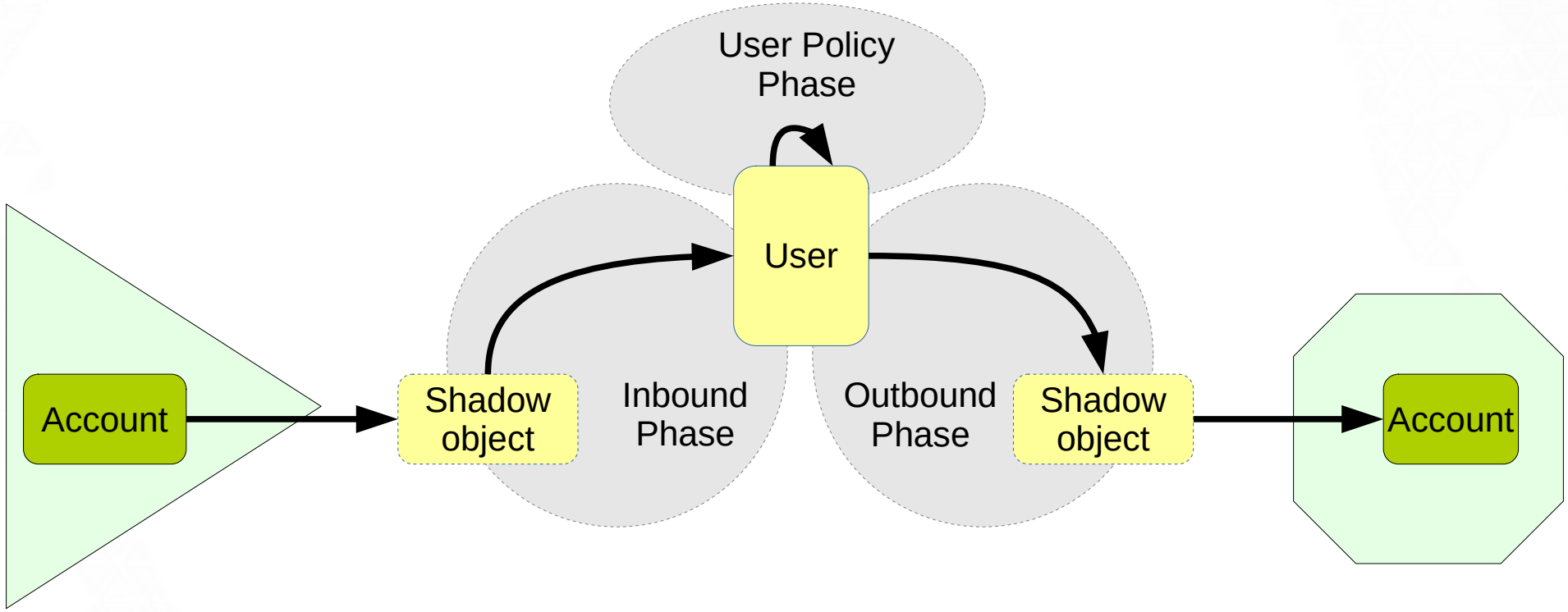
(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

User – Accounts Links Implementation



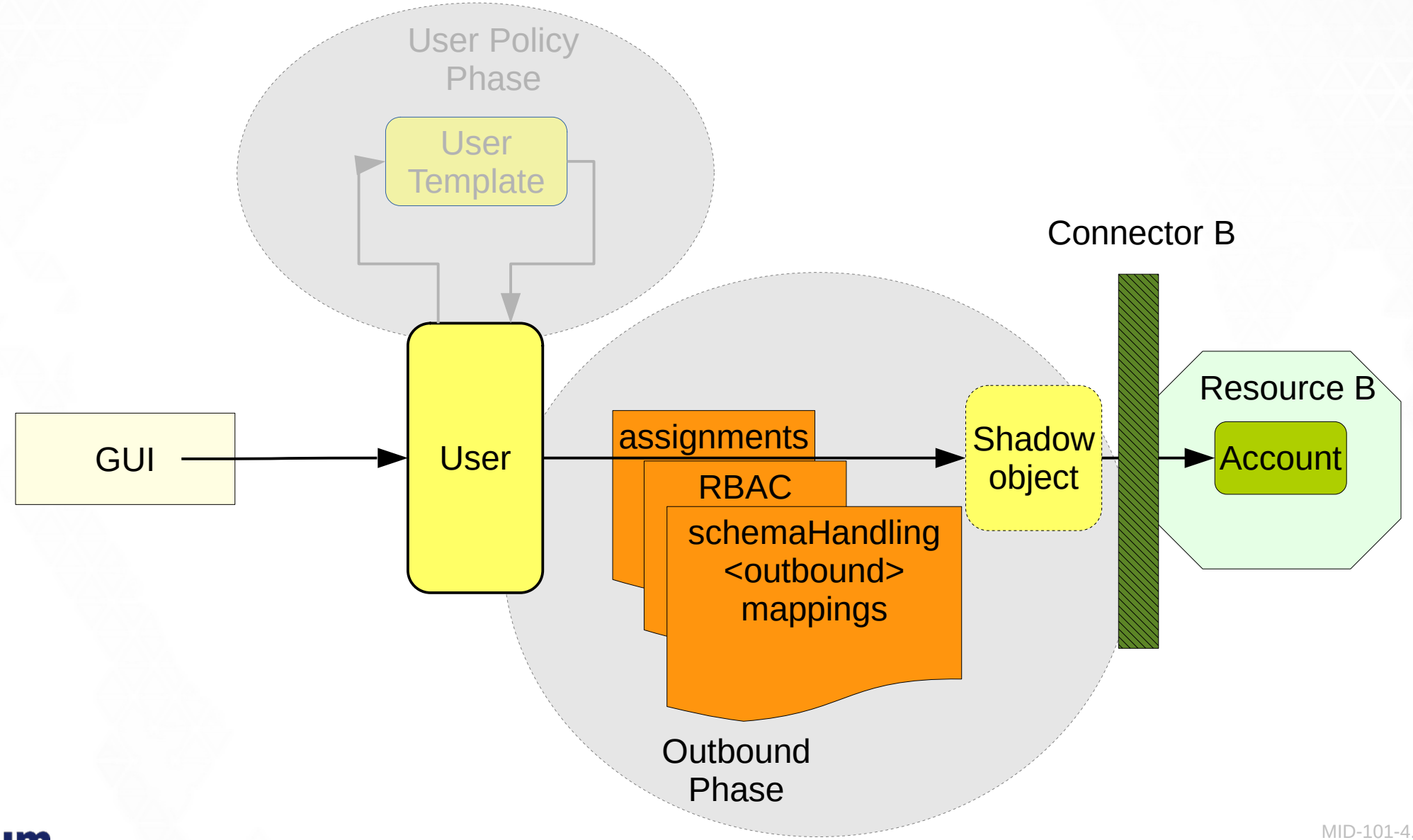
(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

MidPoint User Provisioning Phases



(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Outbound Phase Detail



(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

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)

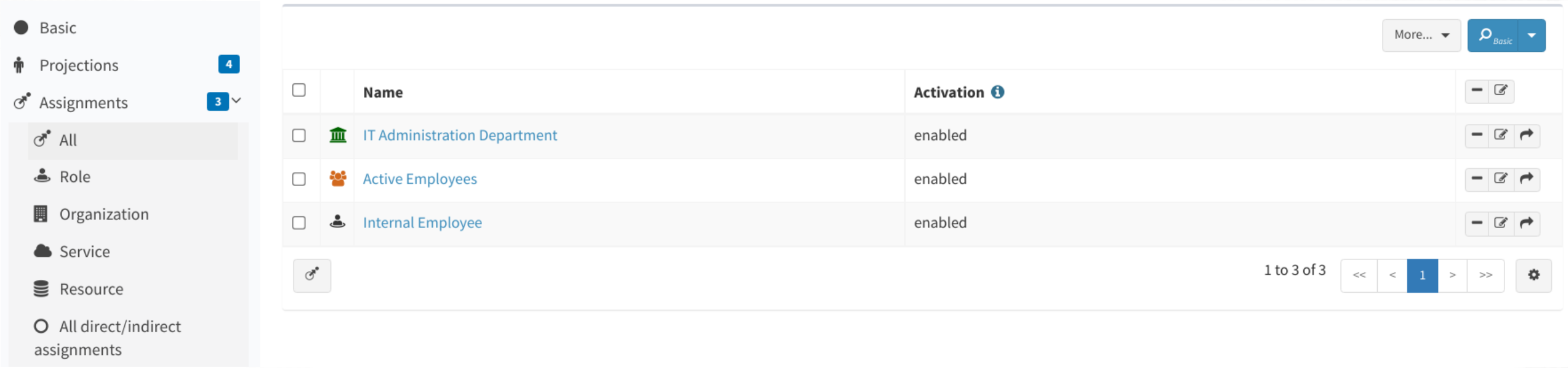
(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Assignment Types

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

(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Assignments in GUI



(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Lab 5-1: Using RBAC

(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Lab 5-2: Segregation of Duties

(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Lab 5-3: Shadows and Projections

(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Lab 5-4: Creating Roles

(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Lab 5-5: Disable on Unassign

(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Lab 5-6: Inactive Assignment

(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Lab 5-7: Archetypes Introduction

(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Module 5: Self-assessment

- (not applicable for sample of the training)

(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Module 5: Summary

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

(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

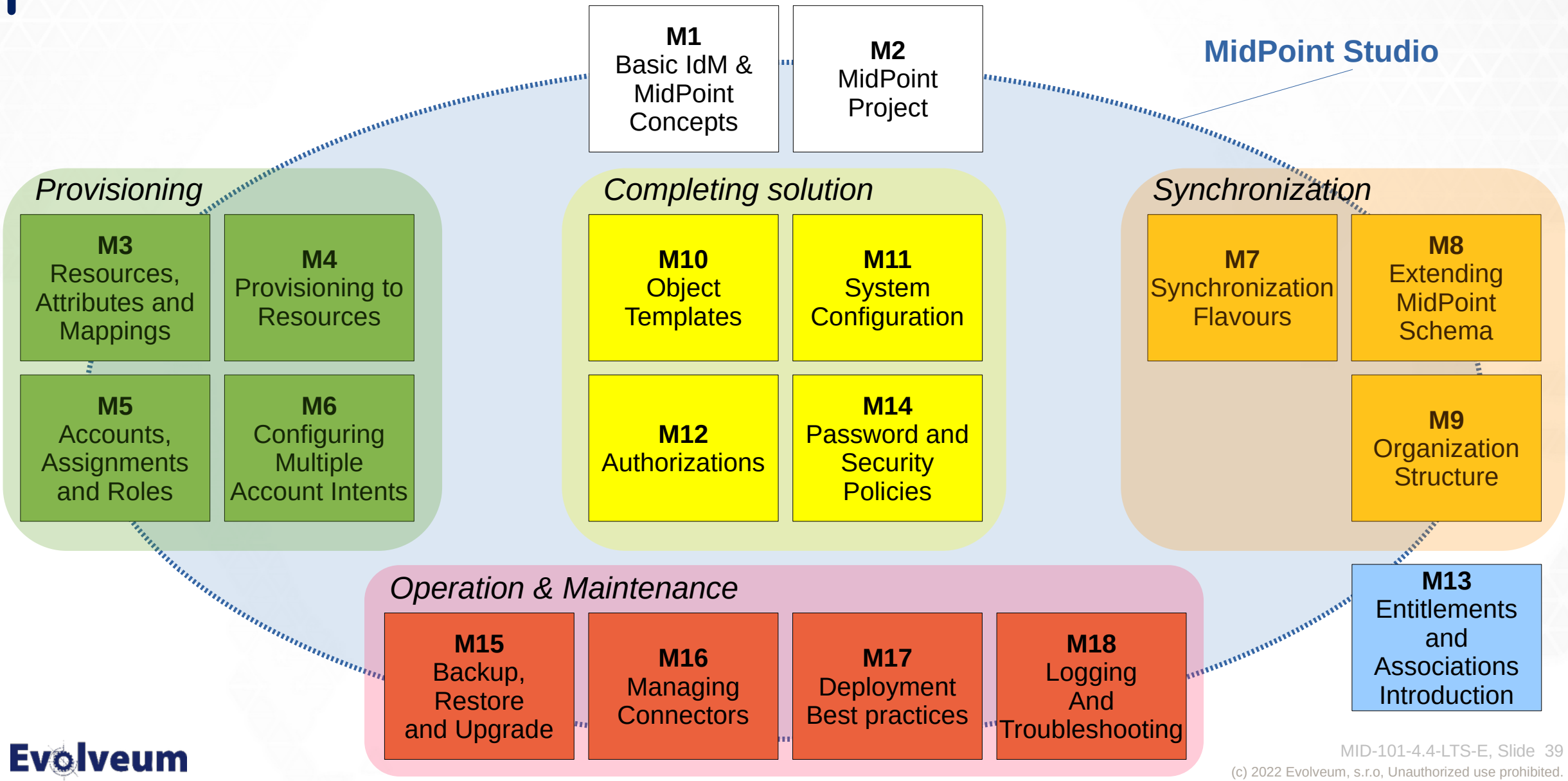
End of Module

(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Course Summary

(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Course Map Relations (Reprise)



(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Questions and Discussion

(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.

Congratulations!
You have just finished the training course!

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

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

 /Evolveum

 /Evolveum

 /Evolveum

 @Evolveum

 /Evolveum

(c) 2022 Evolveum, s.r.o, Unauthorized use prohibited.