MID301: MidPoint Deployment: First steps

Evolveum, s.r.o.
2023

Introduction & Course Goals

What you can expect

Course Goals

- **Understand** how “First Steps Methodology” helps you to deploy midPoint
- **Learn in iterations**, try and extend previous knowledge
- Start using midPoint by connecting your first source and target system

Course Goals (2)

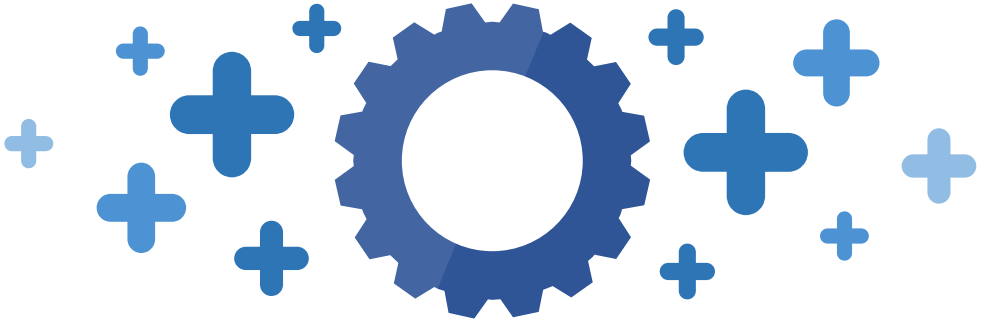
- Use simulations to allow safe configuration deployment
- Understand the concept of Resources and Connectors
- Configure resources using GUI and wizard

Course Goals (3)

- Import data from resource
- Use Reconciliation with resources
- Clean-up data in resources (orphaned accounts etc.)
- Automate the provisioning from source system to target system through midPoint
- Prepare exceptions and data override for incorrect source system data

What's Not Included

- No midPoint installation
- No container configuration
- No XML configuration language
- No version management
- **Will be covered in other courses**



What's Not Included (2)

- No migration from earlier versions, starting with 4.8
- Migration from 4.4 might require additional work (e.g. resource migration)

Course Map

Module 1

Planning Your Deployment Project

Module 2

Connecting Source System

Module 3

Importing Source Data

Module 4

Connecting Target System

Module 5

Target System Integration

Module 6

Importing Usernames From Target System

Course Map (2)

Module 7

Enabling Provisioning to Target System

Module 8

Automating Integration

Module 9

Overriding Incorrect Data

Module 1

Planning Your Deployment Project

Evolveum

Methodology: Planning Your Deployment Project

- Identify data source
- Identify data target
- (Discuss security)
- (Discuss other data targets)
- (Discuss resources, timing, rough plan, money)
- (Talk to your management)

Existing Situation: ExAmPLE, Inc.

- Provisioning is currently partially implemented using a home-grown solution for some target systems
- Source system: HR application (exported CSV file); includes non-IT personnel
- Some target systems are managed by their administrators using tickets
- Usernames are created by AD administrators (`jsmith` convention, appending number if not unique, manually)
- AD username is used in all other systems

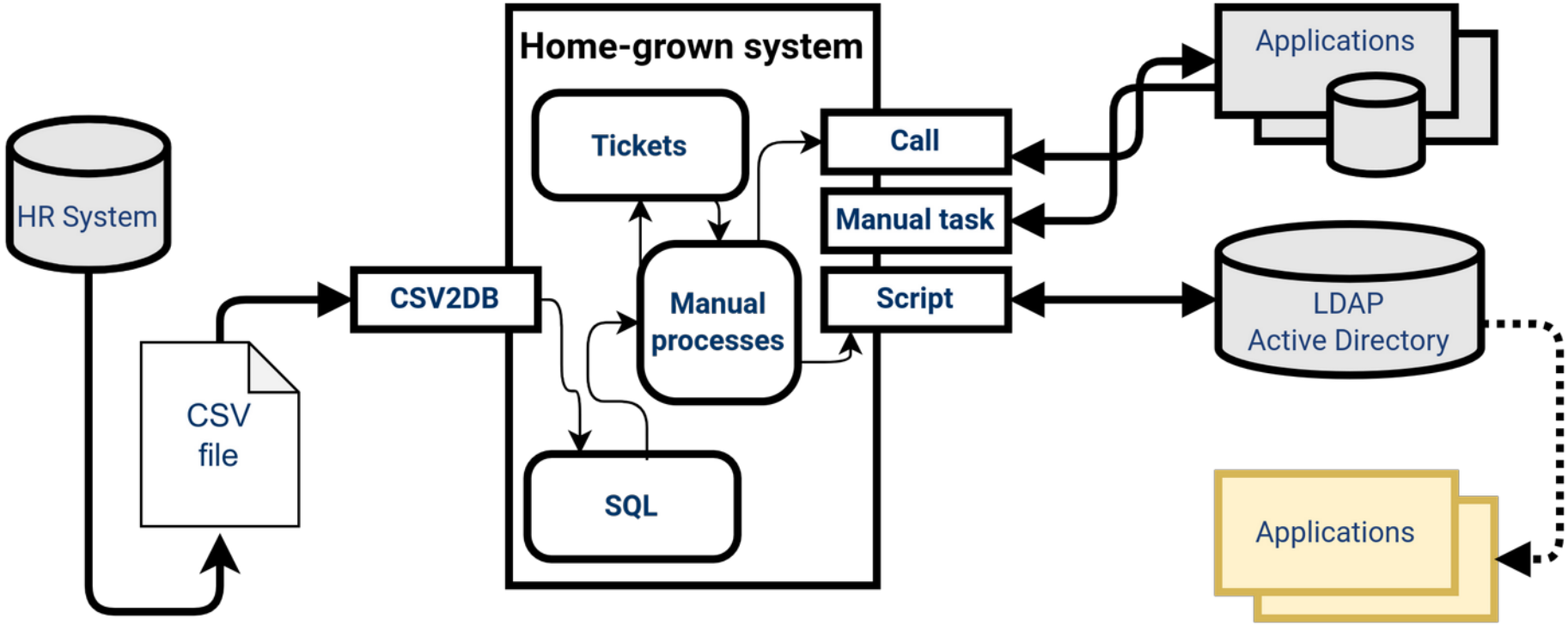
Existing Situation: ExAmPLE, Inc. (2)

- No self-service, no roles, no role request process
- AD groups are used in AD for access control
- Most target systems use AD for authentication
  - ⓘ No SSO configuration within this training
- Home-grown solution … has grown out of control
  - “Do not touch mode”, (original author retired)

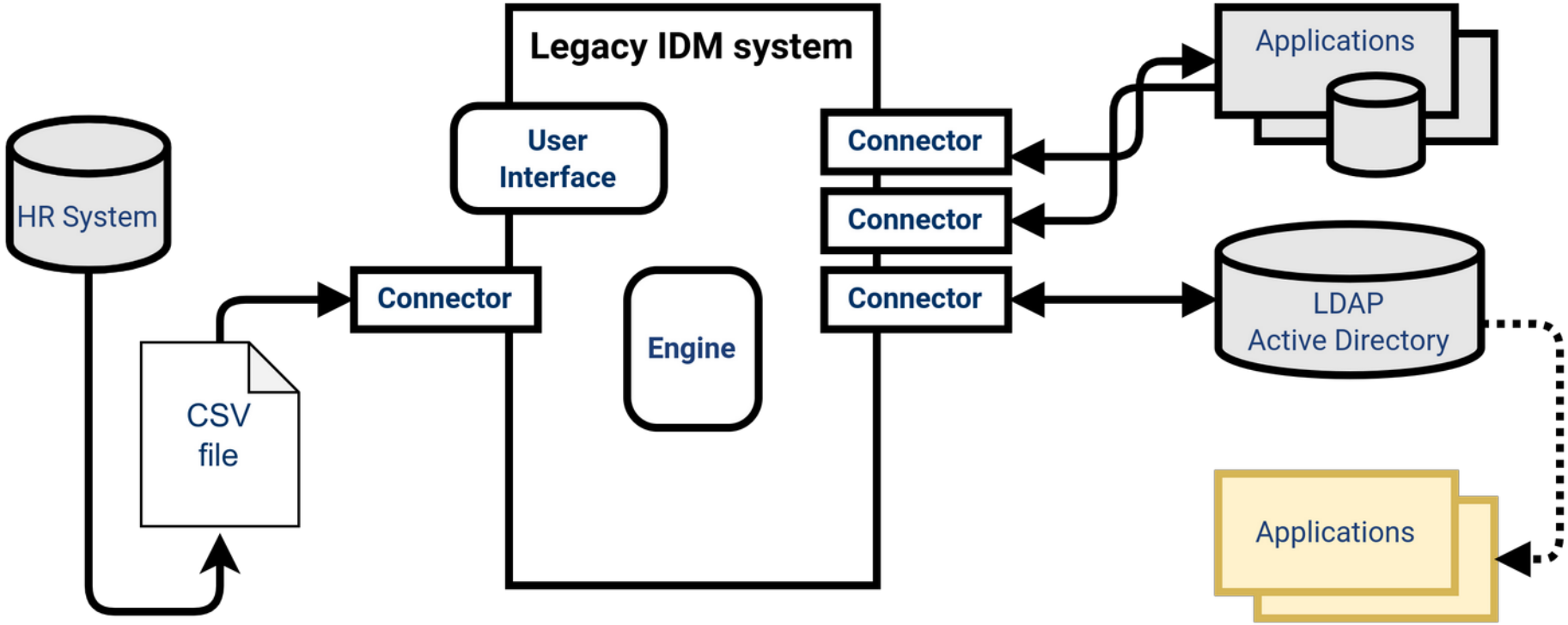
Existing Situation: Alternative

- First Steps methodology can be used also with other existing situations
  - e.g.legacy IDM solution where roles may be already present
- Steps and go live transition can be adapted
- Both midPoint and legacy IDM can coexist as long as needed if the legacy IDM can stop provisioning accounts
- Out of scope of this training

Existing Situation: Architecture (Home-grown System)



Existing Situation: Architecture (Legacy IDM System)



HR Application: Show Users

- List of HR records with ability to modify

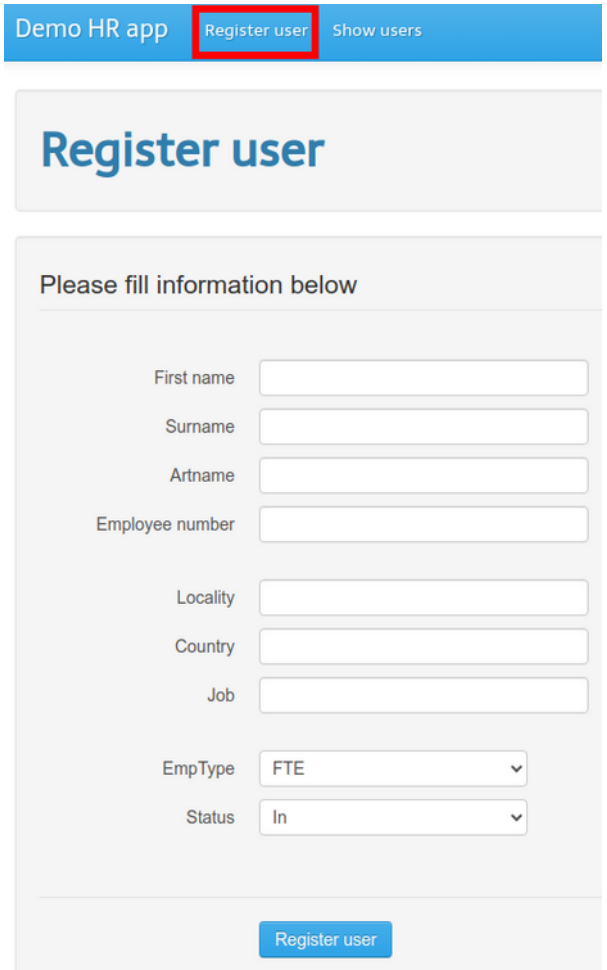
Demo HR app Register user Show users Monday, October 9, 2023 at 5:54:26 AM PDT

Show users

id	First name	Surname	Art name	Emp type	Job	Employee number	Locality	Country	Status	Action
1	Geena	Green		FTE	124#CEO	1001	Small Red Rock City	_loc:Rocky State	In	Modify
2	Ana	Lopez		FTE	125#CFO	1002	Hot Lava City	_lcl:Lava State	In	Modify

HR Application: Register User

- Register (new) record
- Some fields are mandatory



HR Application: Export to CSV File

- HR data can be exported to CSV file
- File is stored in application server, available to midPoint using docker volume

HR Application: Export to CSV File (2)

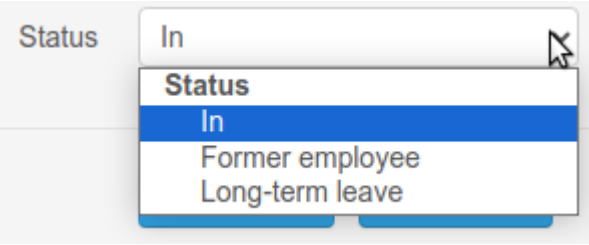
- Attributes exported: **empnum**, firstname, surname, ~~artname~~, emptype, job, status, locality, country

empnum	firstname	surname	artname	emptype	job	status	locality	country
1001	Geena	Green		FTE	124#CEO	In	Small Red Rock City	_loc:Rocky State
1002	Ana	Lopez		FTE	125#CFO	In	Hot Lava City	_lcl:Lava State
1003	Jimmy	Taylor		FTE	107#Junior Consultant	Former employee	Small Red Rock City	_loc:Rocky State
1004	Peter	Hunter		FTE	910#HR Consultant	In	White Stone City	_ilo:Stone State
1005	Emanuel	Young		FTE	120#Senior Specialist	Former employee	Hot Lava City	_lcl:Lava State
1006	Martin	Knight		FTE	121#Junior Specialist	In	Hot Lava City	_lcl:Lava State
1007	Diane	Davis		FTE	107#Junior Consultant	In	Hot Lava City	_lcl:Lava State
1008	Elisabeth	Mason		FTE	191#Accountant	In	Small Red Rock City	_loc:rocky state

HR Application: Data Content

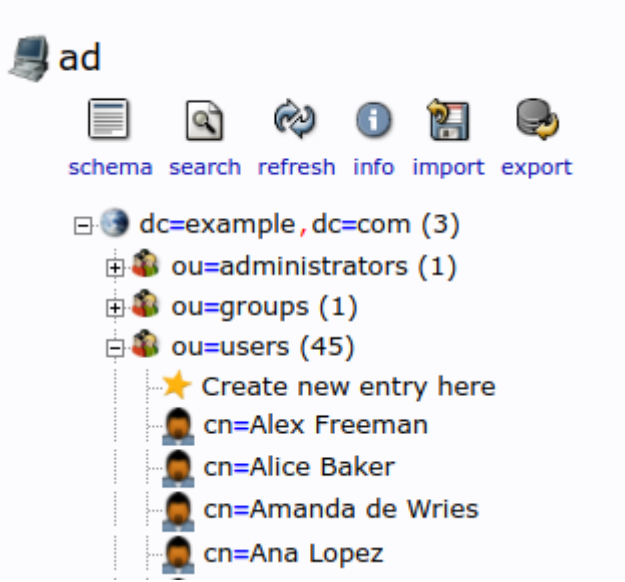
- Employees only (no contractors)
- Non-IT personnel included (should not have IT accounts)
- Attribute **`status`**: In / Long-term leave / Former employee (should be reflected in target system accounts statuses – only “In” having *active* accounts)

empnum	firstname	surname	artname	emptype	job	status	locality	country
8000	Janet	Garner		PTE	899#Cleaning & Maintenance Specialist	In	Hot Lava City	_lcl:Lava State
8001	Ben	Goosehead		PTE	899#Cleaning & Maintenance Specialist	In	Hot Lava City	_lcl:Lava State
8002	Maria	Alvarez		PTE	899#Cleaning & Maintenance Specialist	In	Small Red Rock City	_loc:Rocky State
8003	Monica	Mendez		PTE	899#Cleaning & Maintenance Specialist	In	Fast River City	_rlc:Two River State



Active Directory: Data Content

- `cn` of DN is created manually as user's Given Name + Family Name (but must be unique)
- `uid` (*`sAMAccountName`*) is created manually in `jsmith` convention (but must be unique)
- ⓘ Some accounts (deliberately) don't match the convention



ⓘ We are simulating AD with OpenLDAP

Active Directory: Data Content “Errors”

DN: cn=Alex Freeman,ou=users,dc=example,dc=com

Attribute Description	Value
objectClass	***inetOrgPerson (structural)***
cn	**Alex Freeman**
sn	**Freeman**
displayName	Alex Freeman
employeeNumber	1010
givenName	Alex
l	Fast River City
st	Two River State
uid	afreeman
userPassword	SSHA hashed password

DN: cn=Geena Green,ou=users,dc=example,dc=com

Attribute Description	Value
objectClass	***inetOrgPerson (structural)***
cn	**Geena Green**
sn	**Green**
displayName	Geena Green
employeeNumber	1001
givenName	Geena
l	Small Red Rock City
st	Rocky State
uid	geena
userPassword	SSHA hashed password

ⓘ We are simulating AD with OpenLDAP

Main Goals

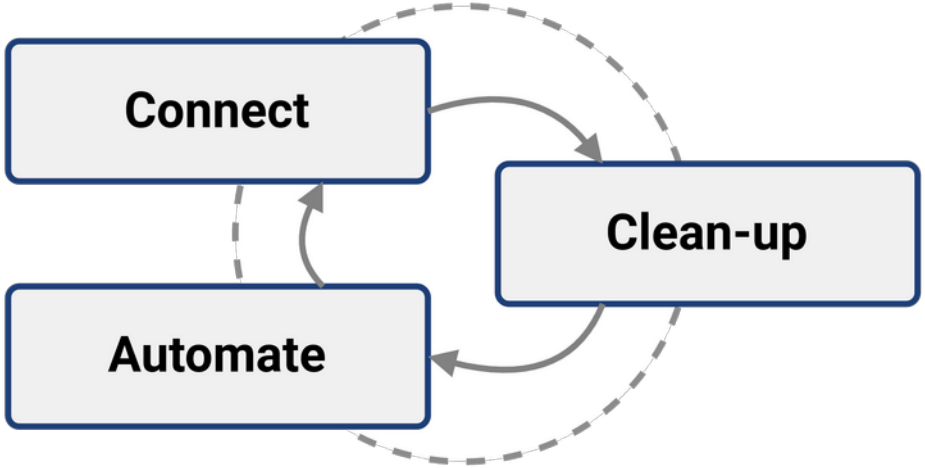
- **Switch from home-grown solution for provisioning target systems using scripts to open-source provisioning and governance system (midPoint)**
- Connect more target systems
- Centralize IdM and IGA

Approach for Main Goals

- Safe migration from existing solution
- No unexpected data deletion or modification in target systems
- Smaller steps, iterations
- Use GUI whenever possible
- Utilize midPoint Simulations

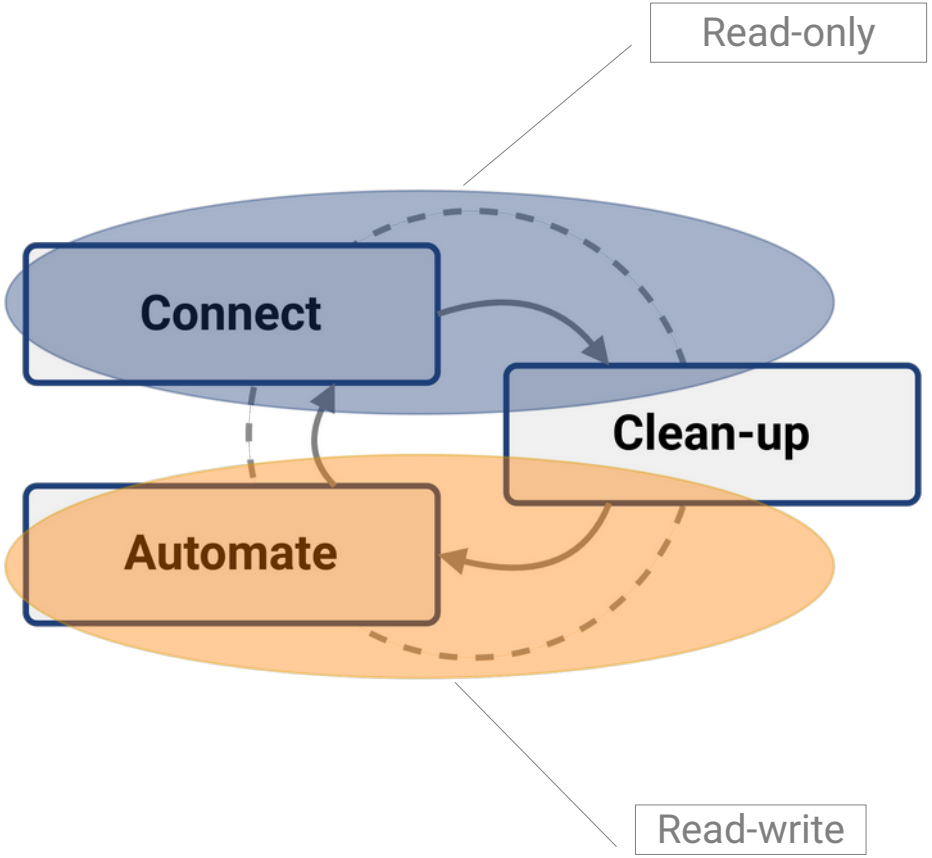
First Steps Methodology

- Simplified midPoint deployment methodology
- Quick deployment of simple midPoint configurations
- *Iterative* identity management program
- Docs: First Steps Methodology

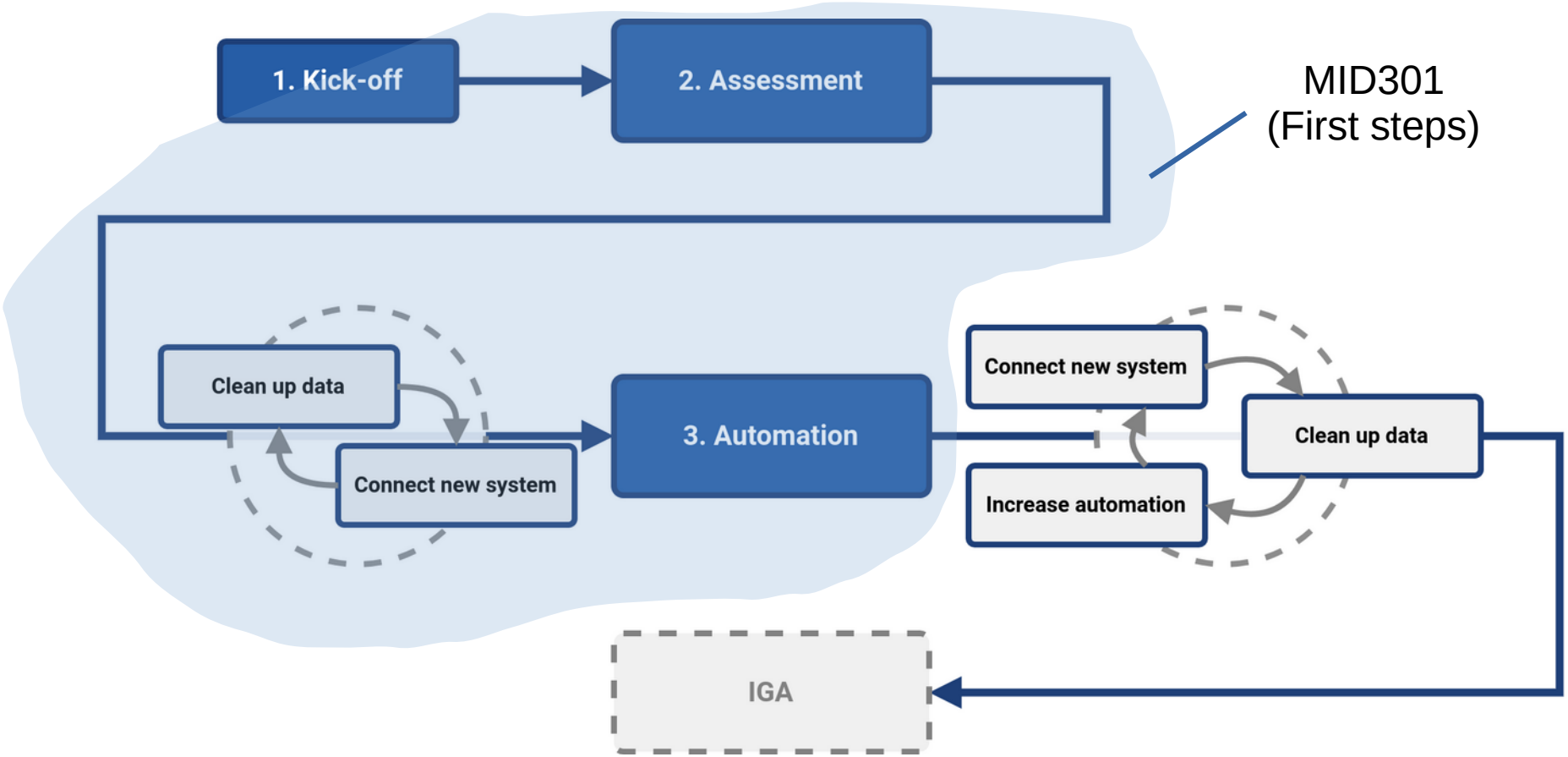


First Steps Methodology (2)

- **Connect**
  - Connect new system(s) to the solution. Read/analyze data
- **Clean-up**
  - Improve data quality. Correlate, resolve orphaned accounts, identify data errors
- **Automate**
  - Speed up the processes, improve efficiency. On-boarding, data updates, off-boarding



First Steps Methodology vs First Steps Training



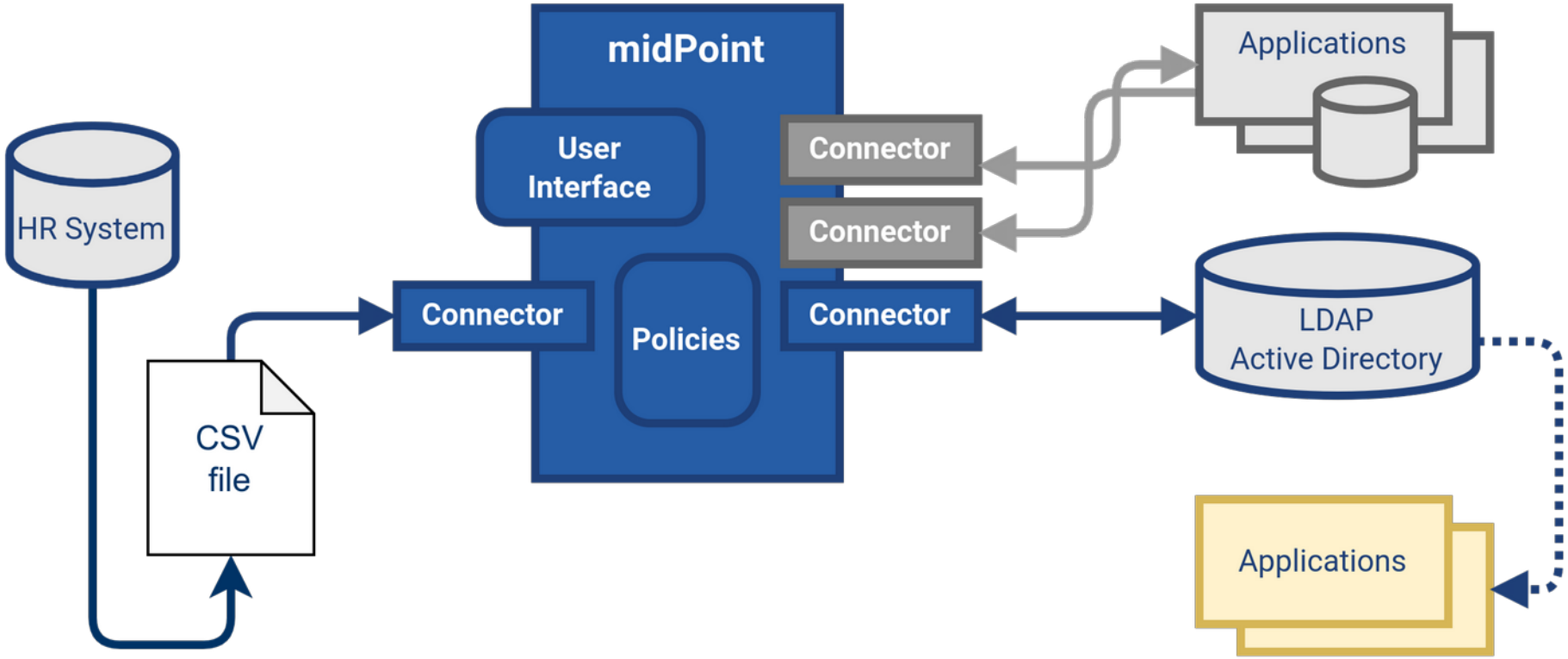
Utilizing First Steps Methodology

#	Step	Description, goals
1	Connect Source System (HR)	We will connect the source system using CSV file and preview data
2	Import Source Data	We will import data from source system, create users in midPoint
3	Connect Target System	We will connect the target system (AD) using a resource template and preview data
4	Target System Integration	We will correlate existing accounts to midPoint users (representing HR data)
5	Import Usernames	We will import usernames from AD to midPoint as they are used for all other applications

Utilizing First Steps Methodology (2)

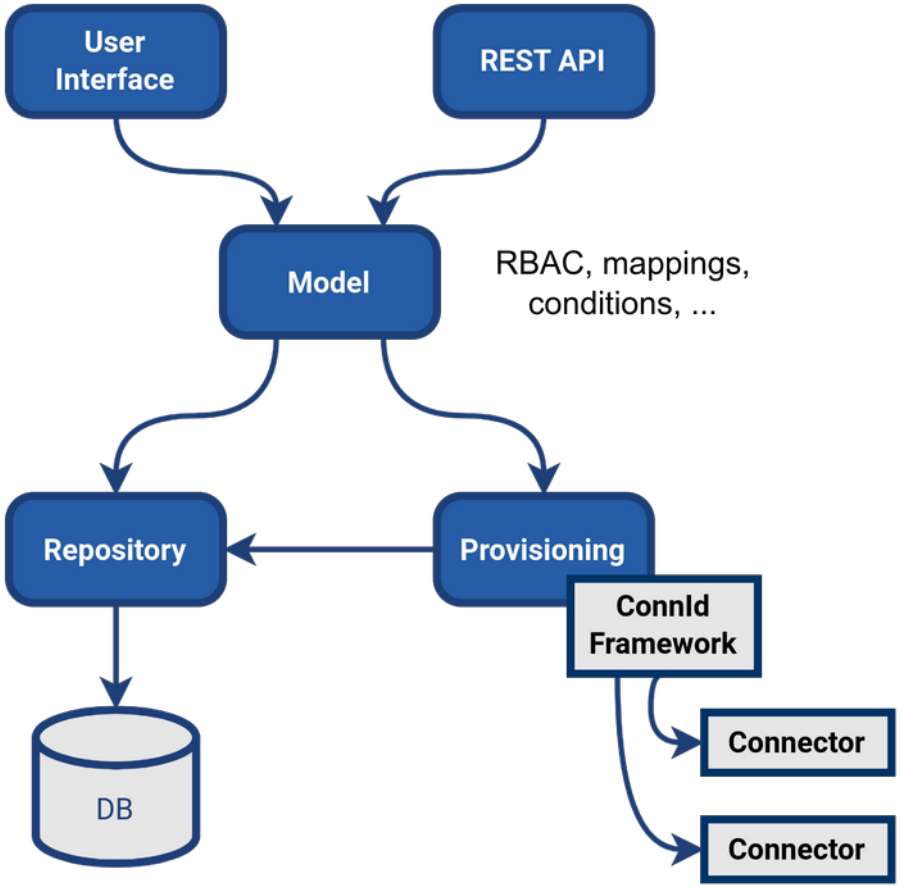
#	Step	Description, goals
6	Enable Provisioning to Target System	We will prepare AD resource for provisioning from midPoint, checking what would be done using simulations
7	Automate Integration	We will automate the AD account provisioning based on HR data in regular intervals. We will start generating midPoint usernames on our own. On-boarding, off-boarding and modifications will be automated.
8	Override Incorrect Data	We will make sure we can override incorrect data from HR if needed

Migration to midPoint: New Architecture



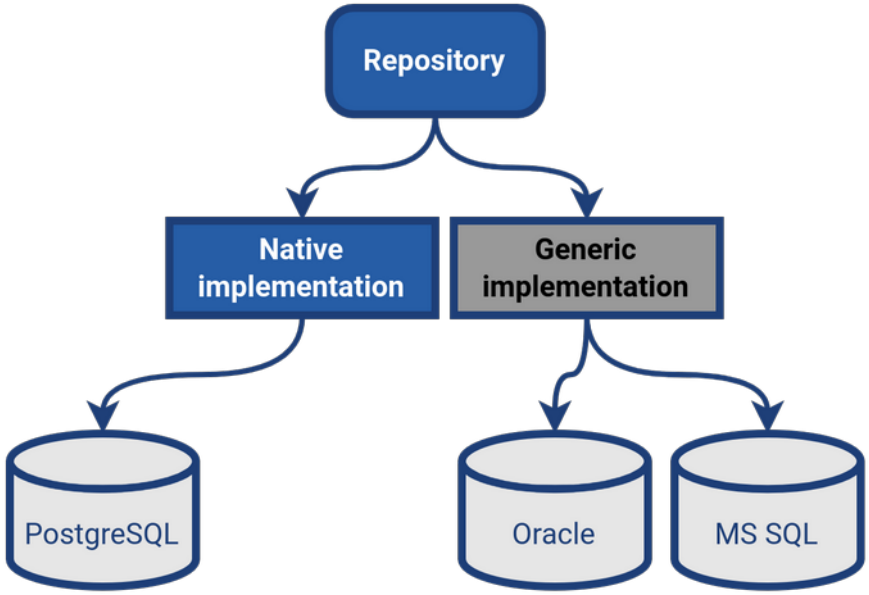
midPoint: Basic Architecture

- Java web application
- Embedded Tomcat, runs as a standalone process
- Small number of components
- Uses XML/JSON to represent internal data
  - ⓘ We will not use this during the training



midPoint Repository

- MidPoint needs a DB repository to store its configuration and identities
- Audit log is by default stored in the same repository
- Native repository (PostgreSQL)
- Generic repository (Oracle, MS SQL)
  - Deprecated, limited features



Newer implementation (currently limited to PostgreSQL)

Older implementation (DEPRECATED)

Does not support all features (e.g. simulation)

Containerized Environment Introduction

- The training is based on docker containers
  - Not just midPoint!
- Lightweight (vs virtual machine)
- Reproducible
- Isolated
- Each container serves one purpose

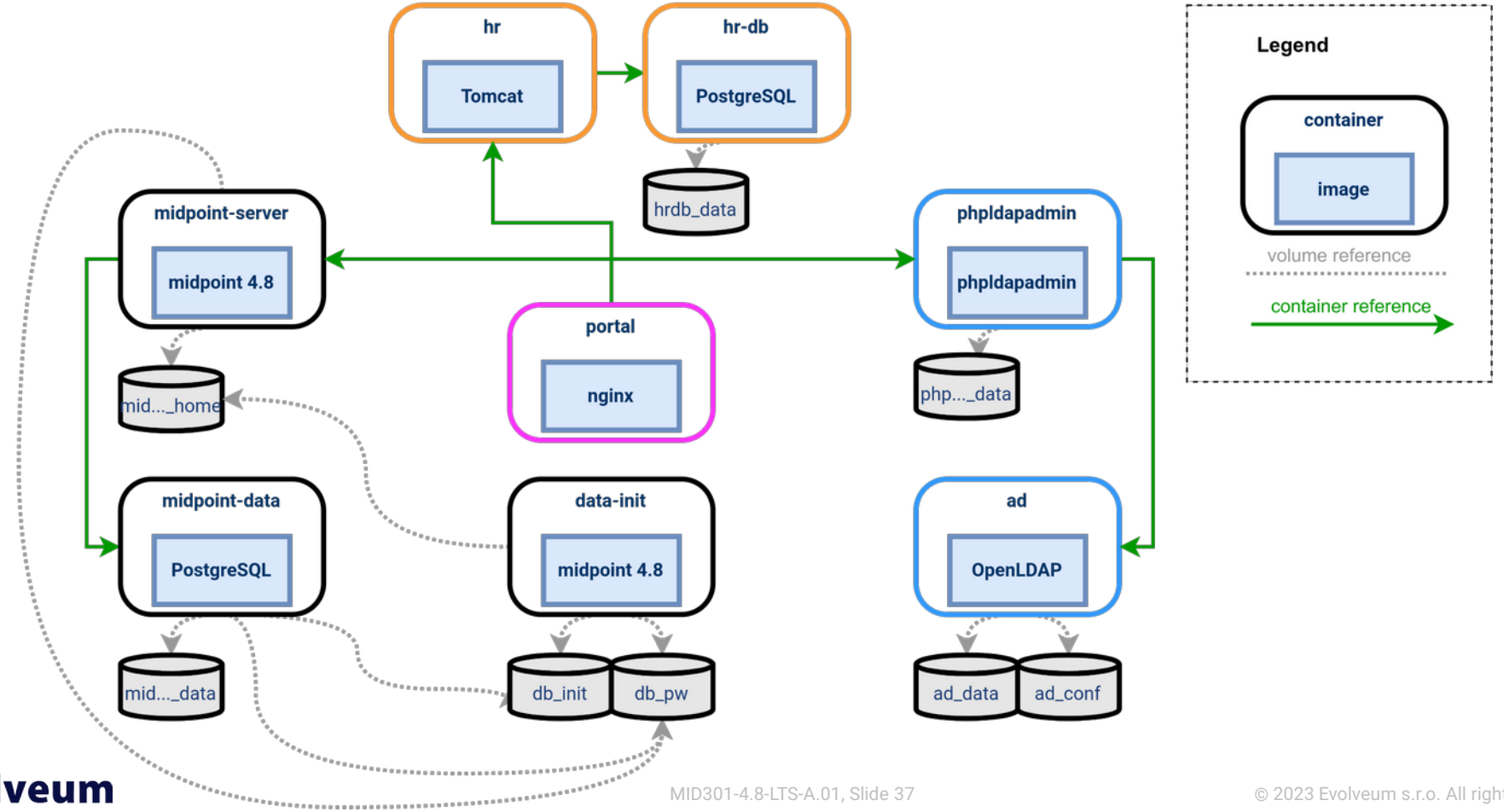
Containerized Environment Introduction (2)

- Docker image: equivalent of OS/applications
- Docker container: running instance of docker image
- Docker volume: persistent storage accessible between containers and host
- ⓘ We will not install the environment

1) MidPoint server 4.8 LTS
2) MidPoint DB repository (PostgreSQL)
3) “AD” (simulated by OpenLDAP)
4) LDAP browser (phpLdapAdmin)
5) HR application (Tomcat)
6) HR DB repository (PostgreSQL)
7) Portal (Nginx)

+ 2 more data initialization containers

Containerized Environment Architecture



Module 1: Labs

LAB 1-1: Inspect Your Environment

Module 1: Self-assessment

- What are the three main steps of First Steps Methodology?
- Name at least two midPoint components...

Module 1: Summary

- Utilizing First Steps Methodology will allow iterative and safe midPoint deployment
- This training will utilize docker containers

Module 1

End of module