

# Evolveum

First Steps Methodology

Ivan Noris, Expert Identity Engineer  
November 2023

# | Agenda

- First Steps Methodology
- Live demo
- Conclusion



# First Steps Methodology: Introduction

- “Guide to quick midPoint deployment of simple midPoint configurations”
  - But can be used with more complex environments as well
- **Safe deployment** heavily utilizing **simulations** and **account marks**
  - Prevents unexpected changes or deletes in target systems
  - **Increases confidence** even with low-quality data



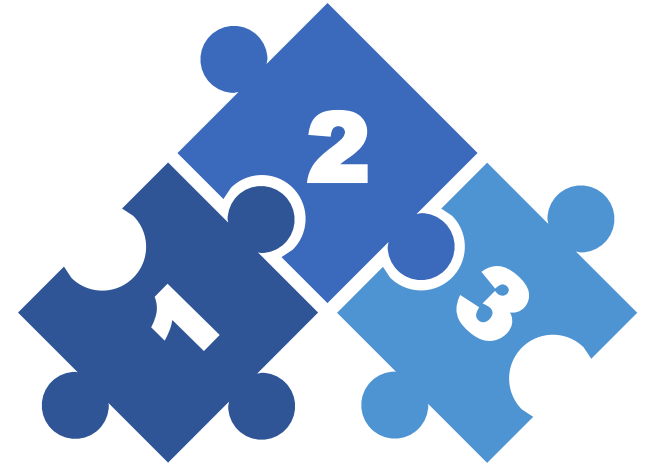
# First Steps Methodology: Introduction (2)

- GUI-based (No XML!)
- **Goal: Start using midPoint by connecting your first source and target system**
- Available [online](#)



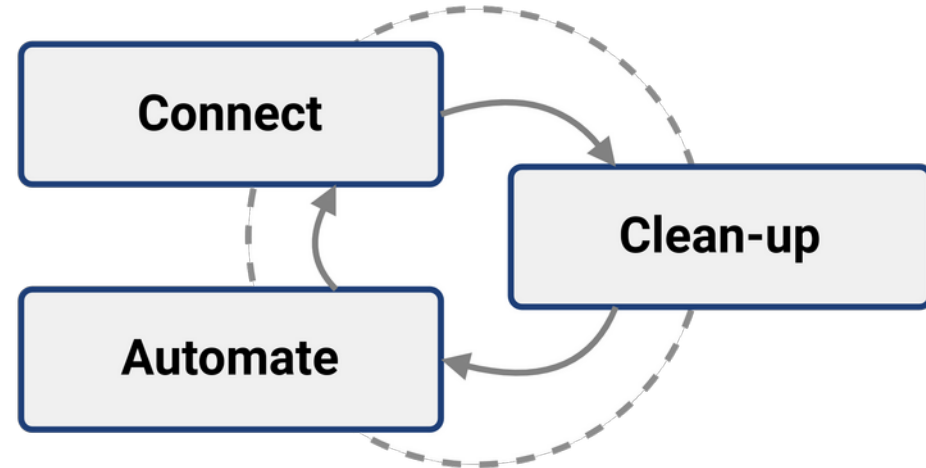
# First Steps Methodology: History

- 2022: started methodology, weekly brainstormings including developers
- 4/2023: midPoint 4.7 released, support for simulations
- 10/2023: midPoint 4.8 LTS
- 11/2023 (planned): first delivery of First Steps training course



# 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**

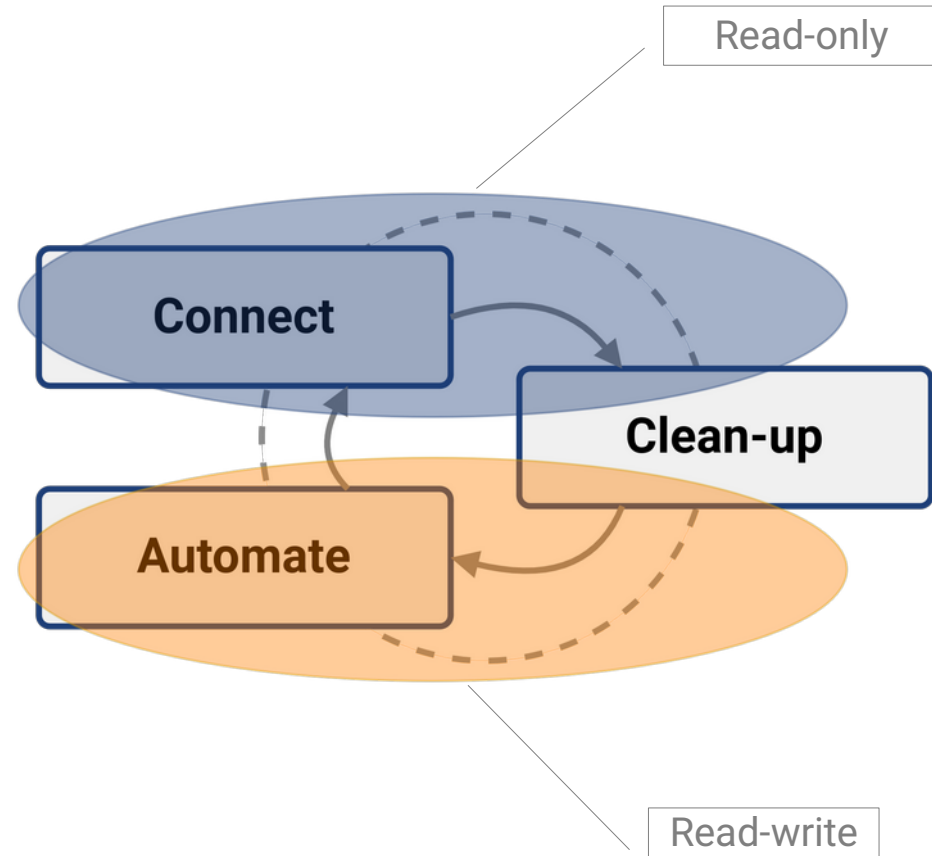
- Connect new system(s) to the solution.  
Read/analyze data

- **Clean-up**

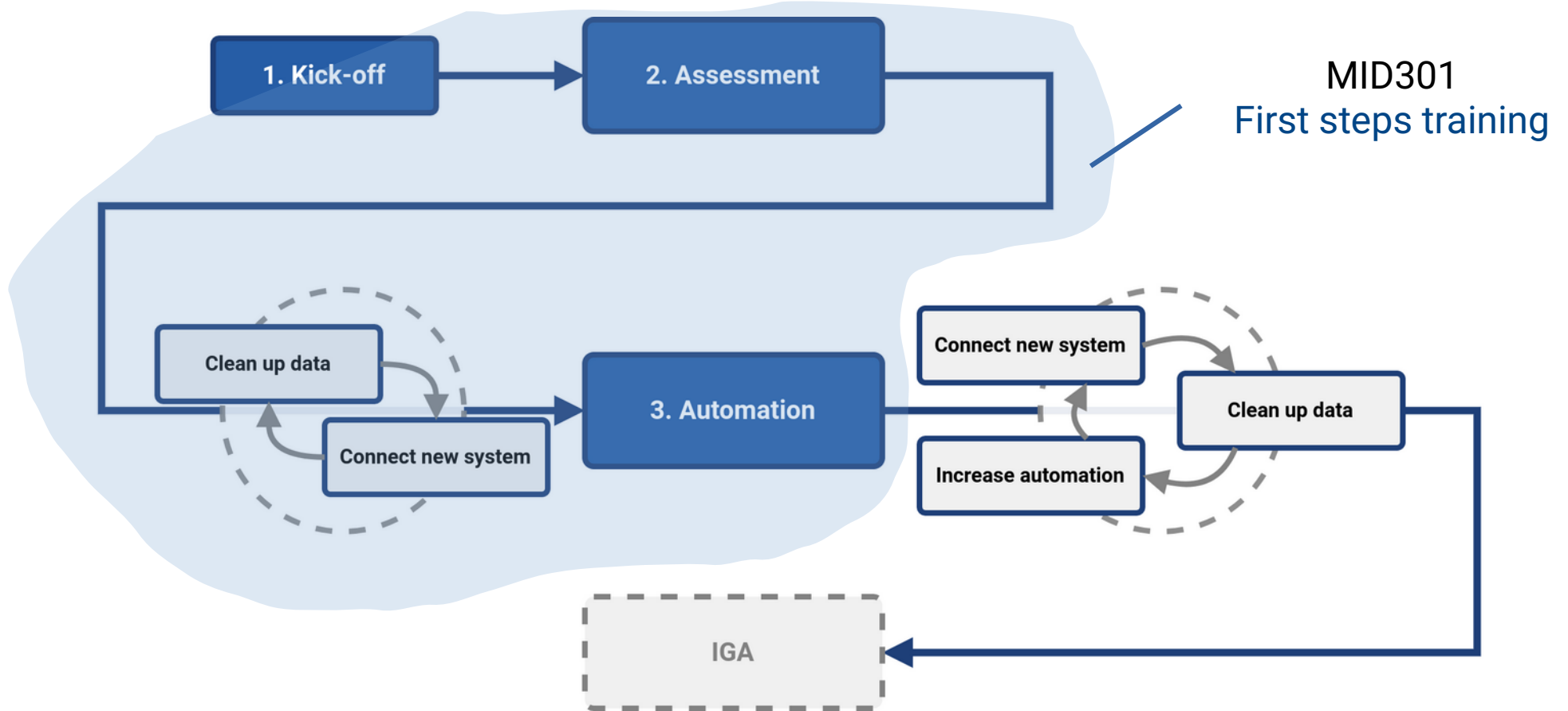
- Improve data quality. Correlate, resolve orphaned accounts, identify data errors

- **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	Plan Your Deployment	Identify data sources, targets, plan resources, timing and money
2	Connect Source System (HR)	Connect the source system using CSV file and preview data
3	Import Source Data	Import data from source system, create users in midPoint
4	Connect Target System	Connect the target system (AD) using a resource template and preview data
5	Target System Integration	Correlate existing accounts to midPoint users (representing HR data)
6	Import Usernames	Import usernames from AD to midPoint

## Utilizing First Steps Methodology (2)

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

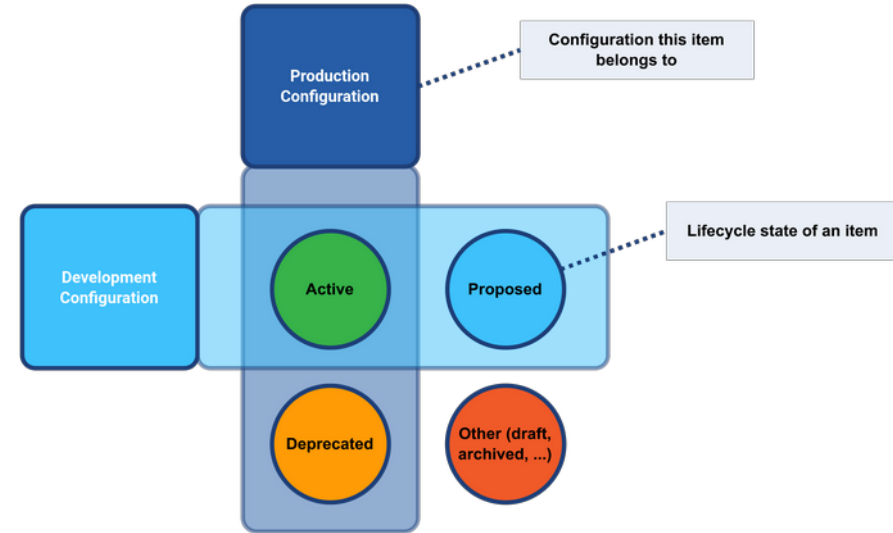
# First Steps Methodology Utilizes Simulations

- Configuration is seldom correct for the first time
- Data can be unexpectedly deleted or modified by incorrect configuration or if target system data is inconsistent
- Incremental adding of new features is **safer** with simulations



# Simulations in midPoint











- MidPoint allows to simulate actions using simulations (“**what would be done**”)
- Actions are only reported, not actually executed
- Lifecycle state of midPoint configuration items
- Execution mode (Preview) – configured in task
- Configuration to use (Development, Production) – configured in task



# Simulation Result: List (Import From Source)

← Back Processed objects

Event mark *i* Undefined ▾ State *i* Undefined ▾ × More... ▾ 🔍 Basic ▾

<input type="checkbox"/>	^ Name	Type	State	Changes	 
<input type="checkbox"/>	 1001 Focus activated	User	Added	 8 Additions of total 8	 
<input type="checkbox"/>	 1001 (Account 1001 (default) on HR)	Shadow	Modified	 2 Edits of total 2	 

Rows per page 20 ▾ 1 to 2 of 2 << < 1 > >>

# Simulation Result: Details (Import From Source)



← Back

1001 (Simulation result: 2023-09-14T08:25:51.246Z)

## Processed object details

Type	User
State	Added
Marks	Focus activated
Projections	1

## Related objects

 1001	User
 1001 (Account 1001 (default) on HR)	Shadow

## Changes

Simple Advanced

### Add User 1001

Item	Value
Name	+ 1001
Lifecycle state	+ active
Given name	+ Geena
Family name	+ Green
Personal Number	+ 1001
Locality	+ Small Red Rock City
Projections	+ 1001 [Default]

User was **enabled**.

# Simulation Result: Summary (Connecting Target System For Provisioning)

[← Back](#) Simulation result: Reconciliation with AD - development simulation, 2023-09-07T12:52:43.032Z

<b>Simulation task details</b>		<b>Event marks</b>		
Start timestamp	September 7, 2023 at 12:52:43 PM UTC	Focus activated 0 <a href="#">More info</a>	Focus deactivated 0 <a href="#">More info</a>	Focus renamed 0 <a href="#">More info</a>
End timestamp	September 7, 2023 at 12:52:49 PM UTC	Focus archetype changed 0 <a href="#">More info</a>	Focus parent organization reference ... 0 <a href="#">More info</a>	Focus role membership changed 0 <a href="#">More info</a>
Finished in	6 seconds	Projection deactivated <b>2</b> <a href="#">More info</a>	Projection renamed <b>5</b> <a href="#">More info</a>	Projection identifier changed <b>5</b> <a href="#">More info</a>
Task	<a href="#">Reconciliation with AD - development simulation</a>	Projection password changed 0 <a href="#">More info</a>	Resource object affected <b>10</b> <a href="#">More info</a>	
Status	<b>Finished</b>			
Configuration	Development			
Added objects	0			
Deleted objects	0			
Modified objects	20			
Unmodified objects	100			
All processed objects	120			





# Demo Environment Introduction


(Existing organization with source/target systems provisioned manually or by scripts, tickets etc.)

# Source System Data (Demo HR Application/CSV File)

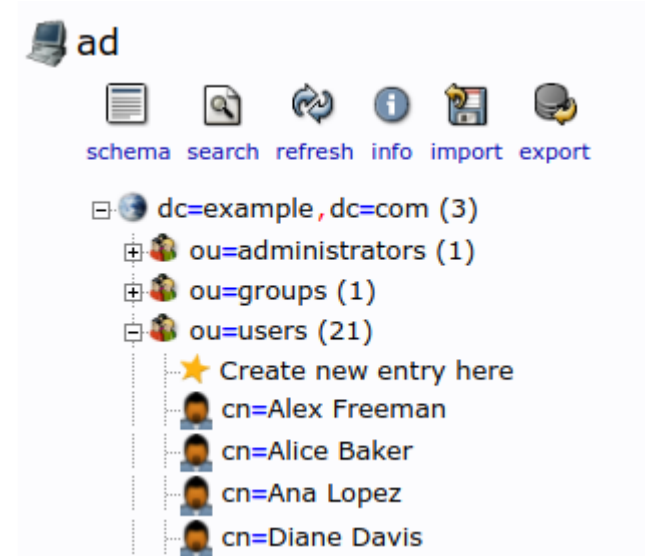
- Attributes exported: **empnum**, `firstname`, `surname`, `artname`, `emptype`, `job`, `status`, `locality`, `country`

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

# Target System Data (AD/LDAP)

- **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



# AD/LDAP: Data Content “Errors”

DN: cn=Alex Freeman,ou=users,dc=example,dc=com	
Attribute Description	Value
<i>objectClass</i>	<i>inetOrgPerson (structural)</i>
<b>cn</b>	<b>Alex Freeman</b>
<b>sn</b>	<b>Freeman</b>
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
<i>objectClass</i>	<i>inetOrgPerson (structural)</i>
<b>cn</b>	<b>Geena Green</b>
<b>sn</b>	<b>Green</b>
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

# Live Demo

(adapted from MidPoint Deployment: First Steps training materials)

# Conclusion

- We have demonstrated midPoint deployment in iterations using First Steps Methodology
- We have used only GUI, no XML
- We have cleaned up orphaned accounts in AD, marked exceptions and set the policy to detect orphaned accounts in the future



## Conclusion (2)

- We have automated the provisioning from HR to AD (accounts)
- We have corrected AD data to correspond to HR data
- We have used simulations to **prevent unexpected changes and deletions** in AD



# Next Steps

- Which steps should be “next” – well, it's up to you
- Continue with connecting other target systems (one by one)
- Continue with connecting other source system for different population
- Import AD groups as roles and start managing them (and their membership) from midPoint





# Do You Want To Know More?

- **MidPoint Deployment: First Steps training** is based on this methodology
- You will learn **how** to do all this in details and more (not all scenarios were presented in this webinar)
- Contact Evolveum if you would like to attend



# Do You Want To Know Even More? (Next Webinars)

- **Resource Wizard**, November 21, 2023
- Navigating the Access Control Maze, December 5, 2023
- **Simulations**, December 7, 2023
- Upgrade with Ninja, January 25, 2024
- **More webinars coming in 2024**



# | ... Yet Yet More? Meet Us at TIIME!

- Jan 29 - Feb 01, 2024, Copenhagen, Denmark
- MidPoint Working Group (Jan 29 - 30)
  - **First Steps Workshop**
- See the [agenda](#)
- Call for speakers
  - Contact us at [marketing@evolveum.com](mailto:marketing@evolveum.com)
- Register here: <https://tiime-unconference.eu/>



# | Q & A



# Thank you for your attention

Do you have any **questions**? Feel free to contact us at [info@evolveum.com](mailto:info@evolveum.com)

**Follow us** on social media or **join us** at GitHub or Gitter!



**Evolveum**

© 2023 Evolveum s.r.o. All rights reserved.