

# Evolveum

Group Management with MidPoint Webinar

Ivan Noris, November 2024  
Expert Identity Engineer

# Agenda

- From identities to accesses
- Group synchronization approach & concepts
- Live demo
- Conclusion



## From Identities to Accesses: The Problem

- We started with [First Steps methodology](#) (▶) for users and accounts, now we need access rights management, e.g. groups
- **Complexity of group management:** there are *existing groups*, but there is typically no single authoritative source of groups
- Even if there is an authoritative source, it contains groups representing business roles
- **Target systems are actually authoritative for their own (application) groups**



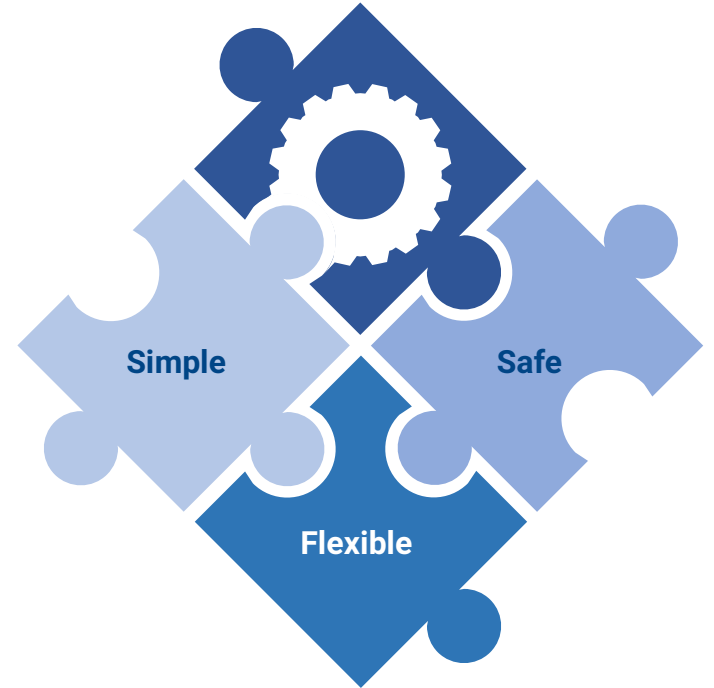
## From Identities to Accesses: The Approach

- **Gradual** migration of the group management including cleanup helps to achieve partial results immediately without any negative impact on end users
- Working on production data with simulations increases deployment speed & confidence
- Increase in configuration flexibility allows to manage some objects by midPoint while others are managed externally
- Synchronizing groups into midPoint even when they are managed externally allows using of midPoint IGA features, e.g. role mining, role engineering
- Reducing the technical complexity and streamlining the process allows even less experienced engineers to execute the process safely



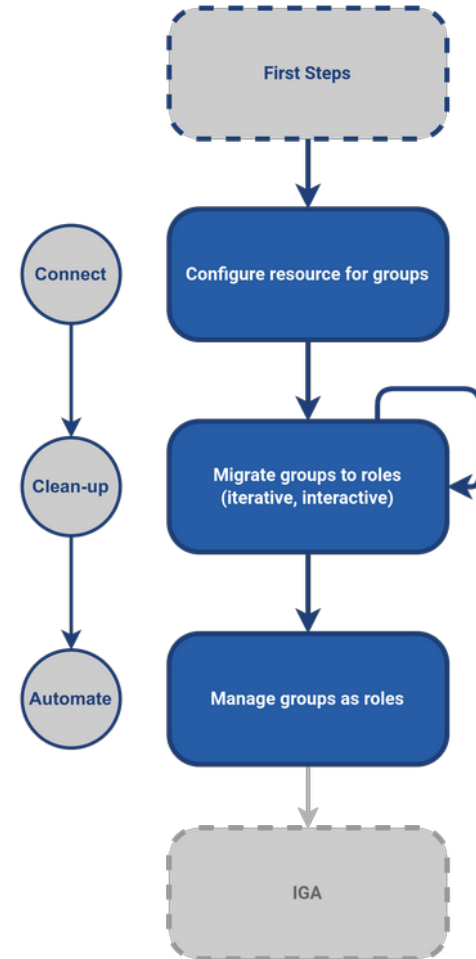
## Group Synchronization in MidPoint: Simple, Safe, Flexible

- **Simple:** easy to configure (GUI, wizards)
- **Safe:** allowing small steps and migration of group management even when in production (lifecycle status, marks, simulations)
- **Flexible:** configurable for different needs (multiple object types, multiple association types)
- Available [online](#)



# Group Synchronization: Iterative Approach

- **Goal: Migration of management of *existing* groups to midPoint**
- Usually, not all groups can be migrated at once, some groups need to be migrated *later* (e.g. groups managed by legacy IDM solution)
- **We need a *mixed* approach:** for some groups and their memberships midPoint is authoritative; for others it is not
- **Connect, clean-up, automate**
  - Connect: extend *First steps* configuration with new object type for groups
  - Clean-up: mark groups for migration and migrate them to midPoint roles; group by group, iterative, interactive
  - Automate: start managing groups as midPoint roles




# Group Synchronization Concepts


- **Roles are equivalents of resource groups**, require a unique naming convention
- **Role assignments are equivalents of group membership** (associations)
- Support for roles with different archetypes for different types of resource groups
- **Simulations will be used to avoid unexpected group and membership modifications or deletions during the process**

### Provisioning from resource wizard


Please choose which aspect of the provisioning from resource you would like to configure



Basic Attributes




Mapping




Synchronization

### Association wizard


Please choose which aspect of the association you would like to configure



Basic Attributes



Subject  
Normal Account



Object  
AD Group






[← Back to association table](#)

© 2024 Evolveum s.r.o. All rights reserved.

**Evolveum**

## Foundation for Easy Migration in MidPoint 4.9

- Protected groups are ignored, cannot be used to create midPoint roles / assignments
- New shadow object marks:
  - **Unmanaged:** resource is authoritative, “inbound-only”
  - **Managed:** midPoint is authoritative, “outbound-only”
- You can mark specific shadows as Unmanaged (exceptions from migration) either **explicitly** or using **Marking rules** (queries)
- New **Default Operation Policy** for object type defining midPoint behavior based on mark
- Different configurations for different group types (not in this webinar)

























<input type="checkbox"/>		cn=all-users,ou=groups,dc=example,dc=com
<input type="checkbox"/>		cn=big-brothers,ou=groups,dc=example,dc=com Protected
<input type="checkbox"/>		cn=legacy-group-1,ou=groups,dc=example,dc=com Unmanaged
<input type="checkbox"/>		cn=legacy-group-2,ou=groups,dc=example,dc=com Unmanaged
<input type="checkbox"/>		cn=legacy-group-3,ou=groups,dc=example,dc=com Unmanaged













## Live Demo vs Training

#	Step	Description
1	Connect resource for groups	Environment initialization, Groups examination
2	<b>Import groups</b>	Configuring AD resource for AD group import, <b>Importing AD groups</b> , Configuring AD resource for AD application group import, Importing AD application groups, Adding object collection views for new roles
3	<b>Import group membership</b>	Configuring AD resource for AD group membership, <b>Importing AD group membership</b> , Configuring AD resource for application group membership, Importing AD application group membership, <b>Reacting on group changes, Reacting on group membership changes</b>
4	<b>Migrate group management to midPoint</b>	Preparing AD groups provisioning, Preparing AD groups membership provisioning, <b>Migrating selected AD groups to midPoint, Migrating non-legacy AD groups to midPoint</b> , Preparing AD application groups provisioning, Preparing AD application groups membership provisioning, Migrating all AD application groups to midPoint
5	<b>Automate group integration</b>	<b>Creating and using roles for new AD groups</b> , Creating and using roles for new AD application groups, <b>Finishing AD group management migration, Detecting unauthorized AD group management</b> , Detecting unauthorized AD application group management, Updating group attributes, <b>Enforcing group membership, Using Person archetype for automating role assignment</b>
6	Manage roles	Renaming role display names, Creating and using applications, Decommissioning roles and groups, Creating business roles, Role reports

# Screenshot: Roles vs Groups

<input type="checkbox"/>	^ Name	Display Name	Description	Identifier	Projections	  
<input type="checkbox"/>	 <a href="#">ad:administrators</a>	AD: Administrators	Allows administrator access for group members. Standard AD management tasks are permitted. This group is now managed by midpoint	administrators	1	 
<input type="checkbox"/>	 <a href="#">ad:all-users</a>	AD: All users	Allows basic access for group members.	all-users	1	 
<input type="checkbox"/>	 <a href="#">ad:legacy-group-1</a>	AD: Legacy group 1	Legacy group 1. Migrated to midpoint.	legacy-group-1	1	 
<input type="checkbox"/>	 <a href="#">ad:legacy-group-2</a>	AD: Legacy group 2	Legacy group 2	legacy-group-2	1	 
<input type="checkbox"/>	 <a href="#">ad:legacy-group-3</a>	AD: Legacy group 3	Legacy group 3	legacy-group-3	1	 
<input type="checkbox"/>	 <a href="#">ad:printer-administrators</a>	AD: Printer administrators		printer-administrators	1	 
<input type="checkbox"/>	 <a href="#">ad:super-admins</a>	AD: Super admins	Only privileged administrators permitted. To be used with ca	AD management is super-admins	1	 

 **ou=groups (9)**

-  **cn=administrators**
-  **cn=all-users**
-  **cn=big-brothers**
-  **cn=legacy-group-1**
-  **cn=legacy-group-2**
-  **cn=legacy-group-3**
-  **cn=printer-administrators**
-  **cn=printers-for-juniors**
-  **cn=super-admins**

Rows per page  1 to 7 of 7 << < 1 > >>

# Screenshot: Role Membership vs Associations vs Group Membership

Basic

Projections **2**

All accesses

Assignments **4** ▾

**All**

Role

Organization

Service

<input type="checkbox"/>	^ Name
<input type="checkbox"/>	AD: Administrators
<input type="checkbox"/>	AD: All users
<input type="checkbox"/>	AD: Printer administrators
<input type="checkbox"/>	AD: Super admins

**cn=Alexander Freeman,ou=users,dc=example,dc=com** ↗

Resource: AD  
Normal Account

Basic Associations

Search

**adGroup**

**Objects \***

- cn=super-admins,ou=groups,dc=example,dc=com
- cn=administrators,ou=groups,dc=example,dc=com
- cn=printer-administrators,ou=groups,dc=example,dc=com
- cn=all-users,ou=groups,dc=example,dc=com
- cn=big-brothers,ou=groups,dc=example,dc=com  
Protected

## memberOf

cn=super-admins,ou=groups,dc=example,dc=com  
cn=all-users,ou=groups,dc=example,dc=com

cn=administrators,ou=groups,dc=example,dc=com  
cn=big-brothers,ou=groups,dc=example,dc=com

cn=printer-administrators,ou=groups,dc=example,dc=com

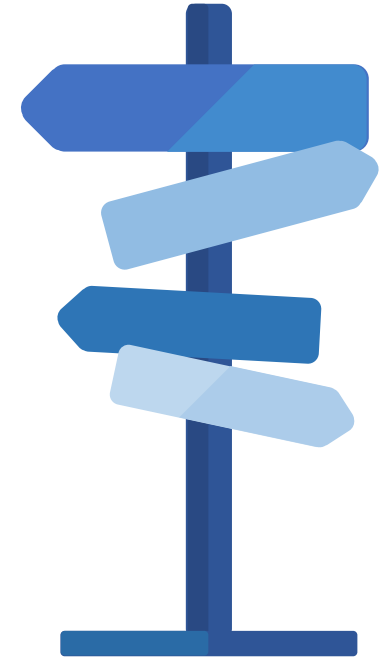
# Live Demo

(adapted from MidPoint Deployment: Group Synchronization training materials)

**Disclaimer:** This is not a training but a real-time demonstration. The configuration has been prepared in advance.

## Conclusion

- From identities to accesses
- You have reached centralized visibility of access rights
- Methodology for migrating the group management to midPoint is fully supported since midPoint v4.9
- Simple, safe, flexible
- Group-by-group approach allows midPoint to start managing specific groups even when group management migration has not been finished yet
- You have taken first steps into a larger world of IGA (role engineering, role mining)



## Do You Want to Know More?

- **NEW** 🖱️ **MidPoint Deployment: Group Synchronization training** is based on this methodology
  - You can register for training [here](#)
- You will learn **how** to use the Group synchronization methodology using many hands-on labs (not all scenarios were presented in this webinar)



# 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



@Evolveum



/Evolveum



/Evolveum



/Evolveum

**Evolveum**

© 2024 Evolveum s.r.o. All rights reserved.