



MidPoint Community Meetup 2025

How to Manage Entitlements via MidPoint's User Interface

Agenda

- But... why?
- Demo (Environment) Introduction
- Group Synchronization Concepts
- Live Demo
- Conclusion



Wait a Minute...

- Didn't we cover *this* before? I remember seeing a *webinar*...
- Is this some kind of mistake?
- Is this a déjà vu?
- *You are trying to fool us!*



Wait a Minute...

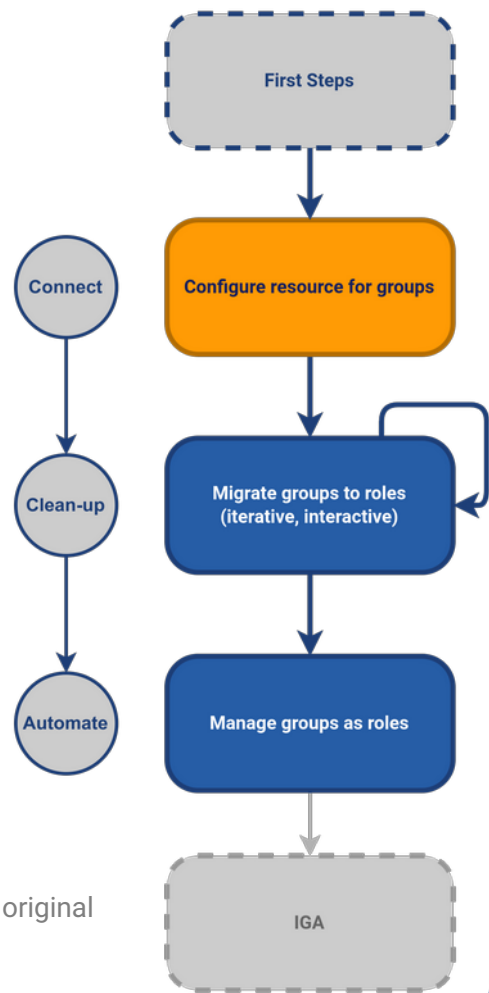
- Didn't we cover *this* before? I remember seeing a *webinar*...
- Is this some kind of mistake?
- Is this a déjà vu?
- *You are trying to fool us!*

Not really, no.

Yes, there was a webinar,
but we have a good reason to do this demo.

Prequel / Sequel

- This demo is a **prequel** to [Group Management with MidPoint webinar \(2024\)](#), where we focused on the actual *entitlement management migration* to midPoint
- Some of our users did not believe that the configuration for webinar was solely possible using midPoint GUI, after so many years with XML configuration.
- In this demo, we will focus on the “**Configure resource for groups**” step

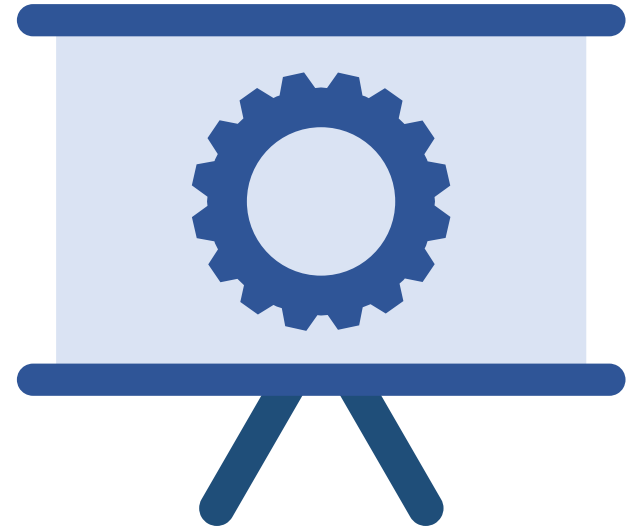


Content of the original
webinar










































Demo (Environment) Introduction


- Based on Evolveum's [Group Synchronization Methodology](#)
- Based on MidPoint Deployment: Group Synchronization training*
- Initial state: MidPoint Deployment: First Steps training final state*
- **Goal:** configure midPoint for group and membership import
- MidPoint 4.9 (because of the webinar)


*) with a reduced set of data





Environment Introduction: Users & AD Accounts

| <input type="checkbox"/> | ^ Name | Personal Number | Full name | Email | Accounts |    |
|--------------------------|--|-----------------|-------------------|-------|----------|---|
| <input type="checkbox"/> |  afreeman | 1010 | Alexander Freeman | | 2 |    |
| <input type="checkbox"/> |  alopez | 1002 | Ana Lopez | | 2 |    |
| <input type="checkbox"/> |  ddavis | 1007 | Diane Davis | | 2 |    |
| <input type="checkbox"/> |  emason | 1008 | Elisabeth Mason | | 2 |    |
| <input type="checkbox"/> |  eyoung | 1005 | Emanuel Young | | 2 |    |
| <input type="checkbox"/> |  ggreen | 1001 | Geena Green | | 2 |    |
| <input type="checkbox"/> |  hboss | 1013 | Hugh Boss | | 2 |    |
| <input type="checkbox"/> |  jtaylor | 1003 | Jimmy Taylor | | 2 |    |
| <input type="checkbox"/> |  jzimmer | 1009 | Josef Zimmer | | 2 |    |
| <input type="checkbox"/> |  mknight | | | | | |
| <input type="checkbox"/> |  phunter | | | | | |

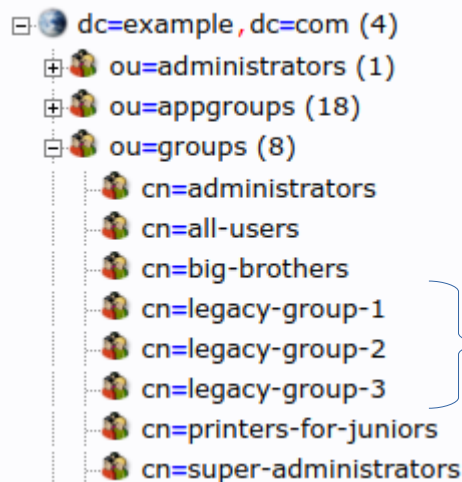
☐  AD

☐  HR

| <input type="checkbox"/> | ^ Name | Connector type |
|--------------------------|--|---|
| <input type="checkbox"/> |  AD | com.evolveum.polygon.connector.ldap.LdapConnector |
| <input type="checkbox"/> |  HR | com.evolveum.polygon.connector.csv.CsvConnector |

| | |
|---|----------------------------------|
|  | dc=example,dc=com (4) |
|  | ou=administrators (1) |
|  | ou=appgroups |
|  | ou=groups (8) |
|  | ou=users (15) |
|  | Create new entry here |
|  | cn=Alexander Freeman |
|  | cn=Ana Lopez |
|  | cn=Diane Davis |
|  | cn=Elisabeth Mason |
|  | cn=Emanuel Young |
|  | cn=Geena Green |
|  | cn=Hugh Boss |
|  | cn=Jimmy Taylor |
|  | cn=Josef Zimmer |
|  | cn=Mail Service Account |
|  | cn=Martin Knight |
|  | cn=Peter Hunter |
|  | cn=Spam Assassin Service Account |
|  | cn=Test123 |
|  | cn=WWW Service Account |

Environment Introduction: AD Groups & Legacy Groups



Managed outside
MidPoint

cn=legacy-group-1

Server: **ad** Distinguished Name: **cn=legacy-group-1,ou=groups,dc=example,dc=com**
Template: **Default**

businessCategory

legacy-group
(add value)

cn required, rdn

legacy-group-1 *

(add value)
(rename)

description

Legacy group 1
(add value)

member required

✗ cn=dummy,o=whatever ⚙

➡ cn=Hugh Boss,ou=users,dc=example,dc=com ⚙

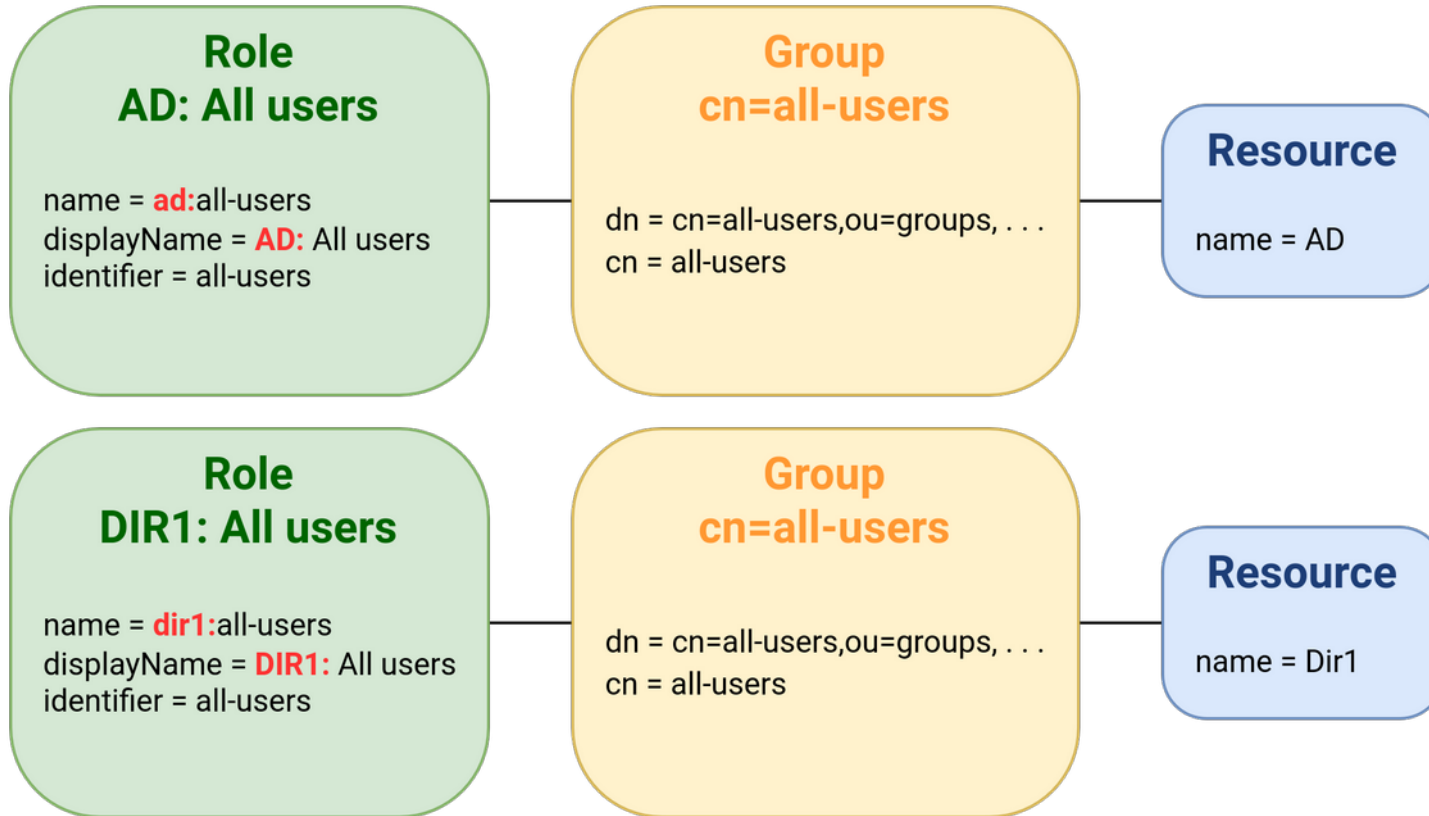
➡ cn=Geena Green,ou=users,dc=example,dc=com ⚙

Group Synchronization Concepts

















- **Roles are equivalents of resource groups**, require a unique naming convention
- **Role assignments are equivalents of group memberships** (associations)
- MidPoint supports roles with different archetypes for different types of resource groups (not used in this demo)
- **Simulations will be used to avoid unexpected group and membership modifications or deletions during the process**



AD Groups and Roles: Naming Conventions



Schema Handling and Object Types (Screenshot)

| Display name | Kind  | Intent  | Default  | Description | Lifecycle state  |   |
|---|--|--|---|--------------------|---|---|
| Normal Account | ACCOUNT 1 | | true | | Active (production)  |    |
| AD Group | ENTITLEMENT 2 | ad-group | true | Internal AD Groups | Active (production)  |    |
|  Add object type | | | | | | Rows per page 20  1 to 2 of 2 << < 1 > >> |

Roles vs Groups (Screenshot)

| Display Name ⓘ Identifier ⓘ Name ⓘ More... 🔍 Basic 📄 | | | | | |
|--|---------------------------|--------------------------|---|----------------------|-------------|
| <input type="checkbox"/> | ^ Name | Display Name | Description | Identifier | Projections |
| <input type="checkbox"/> | 👤 ad:administrators | AD: Administrators | Allows administrator access for group members. Standard AD management tasks are permitted. | administrators | 1 |
| <input type="checkbox"/> | 👤 ad:all-users | AD: All users | Allows basic access for group members. | all-users | 1 |
| <input type="checkbox"/> | 👤 ad:legacy-group-1 | AD: Legacy group 1 | Legacy group 1 | legacy-group-1 | 1 |
| <input type="checkbox"/> | 👤 ad:legacy-group-2 | AD: Legacy group 2 | Legacy group 2 | legacy-group-2 | 1 |
| <input type="checkbox"/> | 👤 ad:legacy-group-3 | AD: Legacy group 3 | Legacy group 3 | legacy-group-3 | 1 |
| <input type="checkbox"/> | 👤 ad:super-administrators | AD: Super administrators | Only privileged administrators might be members, based on CEO approval. Access to all AD management is permitted. | super-administrators | 1 |

Rows per page 20 1 to 6 of 6 << < 1 > >>

| <input type="checkbox"/> | ^ Name | Display Name |
|--------------------------|---------------------|--------------------|
| <input type="checkbox"/> | 👤 ad:administrators | AD: Administrators |
| <input type="checkbox"/> | 👤 ad:all-users | AD: All users |

- 👤 ou=groups (8)
- 👤 cn=administrators
- 👤 cn=all-users
- 👤 cn=big-brothers
- 👤 cn=legacy-group-1
- 👤 cn=legacy-group-2
- 👤 cn=legacy-group-3
- 👤 cn=printers-for-juniors
- 👤 cn=super-administrators

Role Assignments vs Associations vs Group Memberships (Screenshot)

The screenshot displays the Evolveum user interface. On the left, a sidebar menu includes 'Basic', 'Projections' (2), 'All accesses', 'Assignments' (4), 'All', 'Role', 'Organization', and 'Service'. The 'Assignments' section is active, showing a list of roles: 'AD: All users', 'AD: Legacy group 1', 'AD: Legacy group 2', and 'AD: Legacy group 3'. Each role has a checkbox and a person icon. A blue arrow points from 'AD: Legacy group 1' to the 'Associations' tab of the user's profile.

The user profile for 'cn=Geena Green,ou=users,dc=example,dc=com' is shown on the right. The 'Associations' tab is selected, displaying a search bar and a list of objects. The 'adGroup' object is selected, and a blue arrow points from it to the 'memberOf' section below.

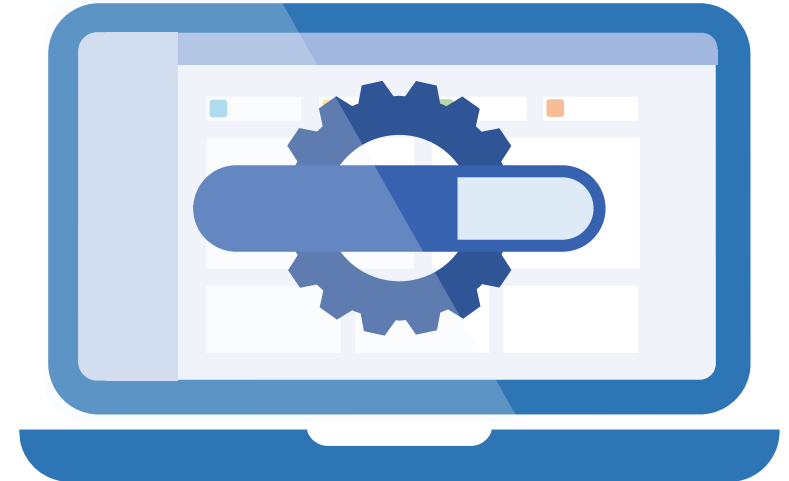
The 'memberOf' section lists the groups the user belongs to:

- cn=all-users,ou=groups,dc=example,dc=com
- cn=legacy-group-2,ou=groups,dc=example,dc=com
- cn=big-brothers,ou=groups,dc=example,dc=com
- cn=legacy-group-3,ou=groups,dc=example,dc=com
- cn=legacy-group-1,ou=groups,dc=example,dc=com

Live Demo Content

- Configure AD resource for AD Group import
- Import AD Groups (to create roles)*
- Add an object collection view
- Configure AD resource for AD Group memberships import
- Import AD Group memberships (to assign the roles to the users)*

*) This step was also part of the webinar



! We are simulating AD with OpenLDAP

Live Demo

(Based on MidPoint Deployment: Group Synchronization training materials)

... And the Rest is History

- This demo is a prequel to **Group Management with MidPoint Webinar 2024**

Configure resource for groups



Conclusion

- You can use midPoint GUI to create configuration for entitlement management quite easily
- Now you can continue the migration of groups/memberships to midPoint and start managing them from midPoint (covered by our [webinar](#))
- Trainings:
 - [MidPoint Deployment: First Steps \(self-paced\)](#) - now available free of charge to everyone
 - [MidPoint Deployment: Group Synchronization \(self-paced\)](#) - now available free of charge to all subscribers
 - [MidPoint Deployment: Intermediate Configuration \(self-paced\)](#) - now available free of charge to all subscribers that have been subscribed for 2+ years
 - See how you can [access our learning portal](#)





Thank you for your attention

Feel free to ask your questions now!



MidPoint Community Meetup 2025