



MidPoint Deployment: First Steps [MID301]

Student Lab Guide - Module 6

Evolveum, s.r.o.

Revision 4.8-LTS-A.01, 2023-11-06

This lab guide is not a standalone document and should be used only for the purpose of this training. If there are any questions during the course related to the content of the training or this lab guide itself, do not hesitate to ask the instructor.

If there are any errors, typos or typographic convention mistakes, please report them to the instructor as well. Thank you.

All labs were tested with the midPoint version used during the training.

We assume you have already installed the prerequisites before this training (if there were any).

Disclaimer

The names, organizations and places portrayed in this training course are fictitious. No identification with actual persons (living or deceased), organizations, places or events is intended or should be inferred.

Table of Contents

Module 6: Importing Usernames From Target Systems **3**

 LAB 6-1: Preparing Configuration For Username Import 3

 LAB 6-2: Username Import Simulation..... 5

 LAB 6-3: Username Import From Active Directory 7

 LAB 6-4: Deleting Orphaned Active Directory Accounts 8

 LAB 6-5: Finalize Correlation 10

Module 6: Importing Usernames From Target Systems

LAB 6-1: Preparing Configuration For Username Import

Estimated Time: 10 min.

In this lab, we will prepare the configuration for username import from Active Directory. We want to achieve that users in midPoint will re-use their AD usernames which they are used to. This configuration is temporary, as Active Directory will not be a source of usernames once we start generating the usernames in midPoint in later labs.

We will update the username "generator" in HR resource first to use it only as a "last resort" for users that don't have Active Directory account.

In your browser with midPoint:


1. go to **Resources** › **All resources**
2. edit **HR** resource
3. click **Accounts** menu item
4. click **Configure**, then click **Mappings** item in the context menu
 - a. edit inbound mapping **empnum-to-name** using **Edit** and set:
 - i. **Strength**: **weak**
 - ii. click **Next: Optional**
 - iii. click **Done**
5. click **Save mappings**

If there was an ongoing synchronization between HR and midPoint, new users would still get usernames as personal numbers as before. But there is no synchronization with HR (yet).

Now we will add a new inbound mapping for AD resource.

In your browser with midPoint:

1. go to **Resources** › **All resources**
2. edit **AD** resource
3. click **Accounts** menu item
4. click **Configure**, then click **Mappings** item in the context menu

- a. do not modify the existing mappings used **only for the correlation** (indicated by )
- b. click **Add inbound** to create a new inbound mapping:

Name	From resource attribute	Expression	Target	Lifecycle state
mapping-inbound-username-to-name-for-import	uid	As is	name	Proposed (simulation)

5. click **Save mappings**

The new mapping will be evaluated for all users with linked AD accounts when we run the reconciliation task. The new mapping's strength is automatically set as strong by resource wizard and will override existing midPoint username for such users.



With real Active Directory, **sAMAccountName** attribute is likely to be used for "as is" mapping.

LAB 6-2: Username Import Simulation

Estimated Time: 5 min.

In this lab, we will run a simulated reconciliation task to see if/how the usernames would be imported from Active Directory.

We will start with a single account simulation.

In your browser with midPoint:

1. go to **Resources** › **All resources**
2. edit **AD** resource
3. click **Accounts** menu item
4. click context menu for AD account **cn=Geena Green** and select **Import preview**
5. in **Select task execution mode** select: **Simulated development** and click **Select**



Simulated development mode will evaluate all **Active** and **Proposed** configuration items, but there will be no permanent effects on data; we are only simulating.

We have set the new inbound mapping for username import with lifecycle state: **Proposed**. Using **Simulated production** mode would not indicate any rename; the new mapping *would be ignored*.

- a. the simulation result will indicate username (**Name** property) to be renamed

Now we will run the simulation for all AD accounts.

In your browser with midPoint:

1. go to **Resources** › **All resources**
2. edit **AD** resource
3. go to **Defined Tasks**
4. edit and run **Reconciliation with AD - development simulation** using **Run now** and wait for the task completion (task status: closed)
5. click **Show simulation result**
6. the Simulation results show:
 - a. 39 users to be renamed (click **More info** in **Focus renamed** tile for more details)
 - b. there is still 1 account to be deactivated - this is still the very same **cn=Secret Admin,ou=users,dc=example,dc=com** account. The synchronization reaction for **Unmatched** it

still in **Proposed** lifecycle state, therefore it is evaluated now.

The simulated reconciliation results look promising, the usernames for all users with linked AD accounts are going to be renamed in midPoint.

LAB 6-3: Username Import From Active Directory

Estimated Time: 5 min.

In this lab, we will finally rename midPoint users by importing their Active Directory usernames.

In your browser with midPoint:

1. go to **Resources** › **All resources**
2. edit **AD** resource
3. click **Accounts**
4. click **Configure**, then click **Mappings** item in the context menu
 - a. switch the inbound mapping **mapping-inbound-username-to-name-for-import** lifecycle state to **Active (production)**
 - b. click **Save mappings**
5. click **Defined Tasks** menu item
6. edit and run **Reconciliation with AD (real)** task for AD using **Run now** and wait for the task completion (task status: closed)
7. go to **Users** › **Persons**
8. users with linked AD accounts have renamed usernames in midPoint

All users with linked AD account are now renamed in midPoint. The only exception is user **1002 (Ana Lopez)** for whom the correlation has failed and does not have a linked AD account. Her AD account is still **Unmatched** and marked **Correlate later**. We will resolve this in later labs. We wanted to emphasize that we can continue the deployment using *First steps methodology* even if the data is not ideal.

LAB 6-4: Deleting Orphaned Active Directory Accounts

Estimated Time: 10 min.

In this lab, we will get rid of the orphaned AD accounts that we have not marked as protected.



This step could be done later, even after turning automated provisioning, if the priority is to do the provisioning for new users.

1. go to **Resources** › **All resources**
2. edit **AD** resource
3. click **Accounts** menu item
4. click **Configure**, then click **Synchronization** item in the context menu
 - a. switch the **Unmatched** → **Delete resource object** reaction's lifecycle state to **Active (production)**
 - b. click **Save synchronization settings**

We can run an additional simulation once again after we have switched the reaction to **Active**.

In your browser with midPoint:

1. go to **Resources** › **All resources**
2. edit **AD** resource
3. click **Defined Tasks** menu item
4. edit and run **Reconciliation with AD - production simulation** using **Run now** and wait for the task completion (task status: closed)
5. click **Show simulation result**
 - a. make sure the simulation indicates that only **cn=Secret Admin,ou=users,dc=example,dc=com** account will be deleted
 - b. the protected accounts set earlier will not be deleted nor modified

Now run the real reconciliation task to really delete the orphaned accounts.

In your browser with midPoint:

1. get back to **Defined tasks** menu item
2. edit and run **Reconciliation with AD (real)** task using **Run now** and wait for the task completion (task status: closed)

- click **Operation statistics** menu item and scroll down to **Actions executed (all actions)** section. You should see the following entry representing the orphaned account deletion in the table (some content is excluded for brevity):

Object type	Operation	Channel	Count (OK)	Last (OK)
Shadow	Delete	Reconciliation	1	cn=Secret Admin,ou=users,dc=example,dc=com (ACCOUNT - default - inetOrgPerson)

- click **Back**
- click **Accounts** menu item
- search for **Unmatched** accounts using the search panel:
 - select **Situation: Unmatched**
 - click **Basic**
- check the resulting accounts and their marks:

Account	Mark
cn=Ana Lopez,ou=users,dc=example,dc=com	Correlate later
cn=Mail Service Account,ou=users,dc=example,dc=com	Protected
cn=Secret Admin,ou=users,dc=example,dc=com	Does not exist anymore
cn=Spam Assassin Service Account,ou=users,dc=example,dc=com	Protected
cn=Test123,ou=users,dc=example,dc=com	Do not touch

You can also check the account presence in AD resource using LDAP browser.

In your browser with AD LDAP browser:

- expand **dc=example,dc=com**
- expand **ou=users**
- account **cn=Secret Admin** should not be present

We could repeat these steps also for account **cn=Test123** which is currently marked as **Do not touch**. By removing that mark and running reconciliation with Active Directory, the account would be deleted. (We will show how to remove mark in the following lab.)

Active Directory resource is now configured to delete any orphaned accounts. If there was a scheduled reconciliation task, midPoint would make sure no orphaned accounts exist. Of course, the protected/marked accounts won't be affected.

LAB 6-5: Finalize Correlation

Estimated Time: 10 min.

In this lab, we will resolve the previously uncorrelated accounts by introducing an alternative correlation mechanism based on other attributes than employee number. This configuration is already prepared in the resource template, we need just to enable it.

Account `cn=Ana Lopez,...` was not correlated, because her AD attribute `employeeNumber` has (deliberately, for the purpose of this training) incorrect value `2` instead of `1002` from HR.

We will enable an additional correlation for such cases, using Given Name, Family Name and Locality attributes, with manual administrator confirmation (using midPoint approval mechanism).

In your browser with midPoint:

1. go to **Resources** > **All resources**
2. edit **AD** resource
3. click **Accounts** menu item
4. Search for **Lopez** using basic search or display only accounts with **Unmatched** situation
5. click **Configure**, then click **Correlation** item in the context menu
 - a. For **last-resort-correlation** correlation rule set:
 - i. **Enabled: True**
6. click **Save correlation settings**

As `cn=Ana Lopez` is marked with **Correlate later** mark, any import/correlation would completely ignore her. We need to unmark the account first.

1. for `cn=Ana Lopez` in the list of accounts, click the context menu and select **Remove marks**
2. select **Correlate later** mark to be removed
3. click **Remove Marks**
4. click **Defined Tasks** menu item
5. edit and run **Reconciliation with AD (real)** task using **Run now** and wait for the task completion (task status: closed)
6. click **Back**
7. click **Accounts** menu item again
8. `cn=Ana Lopez` is in **DISPUTED** situation, for which we do not have yet any configuration. This situation is used if midPoint is not sure who the owner should be, but there are some candidates. But we know she is not unmatched anymore.

9. click **Configure**, then click **Synchronization** item in the context menu
 - a. click **Add reaction**

Name	Situation	Reaction	Lifecycle state
disputed-create-case	Disputed	Create correlation case	Active

- b. click **Save synchronization settings**
10. click **Defined Tasks** menu item
11. edit and run **Reconciliation with AD (real)** using **Run now** and wait for the task completion (task status: closed)

A correlation case should be created to resolve the **DISPUTED** situation, user **administrator** needs to act (e-mail notification would be sent in real deployments).

1. go to **Cases › My workitems**
2. click the only work item (**Correlation of account 'cn=Ana Lopez,ou=users,dc=example,dc=com' on AD**)
3. in the table of correlation candidates, look at the **Correlation candidate 1** column (Ana Lopez)
 - a. notice the Personal number difference (default correlator didn't match), but all other correlation attributes (from second correlator) match
4. click **Correlate** for **Correlation candidate 1** (Ana Lopez) to select this user as owner of the uncorrelated account
5. go to **Users › Persons**
6. user **alopez** (formerly **1002**, now renamed) has her AD account linked and visible in **Projections** panel. AD's **employeeNumber** is still incorrect, but will be fixed when we enable provisioning to AD in later labs

We have seen how midPoint can use several correlators with one or more attributes, with exact or "approximate" matching and how human factor can be used to resolve the undecided cases.

This concludes the Module 6 labs.