MidPoint Deployment: First Steps [MID301]

Student Lab Guide - Module 5

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 5: Target System Integration

LAB 5-1: Simulated Correlation With Active Directory

Estimated Time: 10 min.

In this lab, we will run a simulated reconciliation task with Active Directory to correlate the existing accounts. Orphaned accounts will be detected as well.

In your browser with midPoint:

1. go to **Resources › All resources** unless you are already displaying AD resource accounts
2. edit **AD** resource
3. click **Accounts**
4. click **Tasks**, then click **Create task** item in the context menu to open a simple task creation wizard for AD accounts
   a. click **Reconciliation Task** tile
   b. toggle **Simulate task** to **ON**
   c. click **Create task** and fill in the following details:
      i. **Name**: `Reconciliation with AD - development simulation`
   d. click **Next: Resource objects**
   e. click **Next: Execution**
   f. in **Execution options** page, set the following:
      i. select **Mode**: `Preview`
      ii. select **Predefined**: `Development`
   g. click **Next: Schedule**
   h. click **Next: Distribution**
   i. click **Save & Run**

Running simulated reconciliation task with `Development` configuration will evaluate all `Active` and `Proposed` configuration items, but there will be no permanent effects on data; we are only simulating.

1. click **Defined Tasks** menu item
2. edit the task **Reconciliation with AD - development simulation**

3. click **Operation statistics** menu item to check correlation results
4. scroll down to **Synchronization situation transitions** section. Here you can see how the resource accounts were classified before/after the task execution. **Please note the operations were not actually executed as we have run the reconcilition in simulation mode.**
    a. 39 accounts previously not linked are now linked to midPoint users; final situation is **Linked**
    b. 5 accounts previously not linked are still not linked to midPoint users; final situation is **Unmatched** - these are orphaned accounts
    c. 1 account is **protected** (within the configuration of resource copied from resource template)
5. click **Show simulation result**
6. the Simulation results show:
    a. 5 deactivated accounts (to be deleted) including **Ana Lopez** (company CFO, we need to be careful here!)
    b. 78 modified objects, where:
        i. midPoint users indicate added Projection (as a result of correlation of the account and linking it to its owner)
        ii. AD accounts indicate metadata changes (in midPoint repository only)

The results of simulation indicate some inconsistency in target system accounts. We need to correct their states and/or make exceptions in the following labs. No harm has been done yet.

LAB 5-2: Marking Accounts

Estimated Time: 10 min.

In this lab, we will create exceptions for some orphaned accounts to prevent midPoint from modifying or deleting them.

In your browser with midPoint, in simulation results for **Reconciliation with AD - development simulation** task:

1. click **Projection deactivated** tile
2. mark the accounts using **Mark** or **Protect** buttons

Account	Mark
cn=Ana Lopez,ou=users,dc=example,dc=com **This is CFO, we definitely don't want to delete this account.**	Correlate later
cn=Mail Service Account,ou=users,dc=example,dc=com	Protected
cn=Secret Admin,ou=users,dc=example,dc=com	do not set any mark, we want to delete this account
cn=Spam Assassin Service Account,ou=users,dc=example,dc=com	Protected
cn=Test123,ou=users,dc=example,dc=com	Do not touch

3. the processed object list immediately refreshes to show the marks
4. (also **Resource** › **Accounts** page now shows the marks)
5. edit and run **Reconciliation with AD - development simulation** task again using **Run now** and wait for the task completion (task status: closed)
6. click **Show simulation result**
7. the Simulation results show:
    a. 1 deactivated accounts (to be deleted) - this is the `cn=Secret Admin,ou=users,dc=example,dc=com` account (no more CFO deletion - good!)
    b. 78 modified objects, where:
        i. midPoint users indicate added Projection (as a result of correlation of the account and linking it to its owner)
        ii. AD accounts indicate metadata changes (in midPoint repository only)

midPoint won't delete protected accounts from now on. **Ana Lopez** will be ignored from automatic synchronization from now on and will not be even correlated (yet).

LAB 5-3: Ignoring Orphaned Accounts

Estimated Time: 10 min.

In this lab, we will reconfigure synchronization to temporarily ignore orphaned accounts. We will keep them in the system (most of them already marked in the previous steps). This way we can continue deployment and still do it safely.

In your browser with midPoint:

1. go to **Resources › All resources**
2. edit **AD** resource
3. in resource's **Lifecycle state** toolbar, select `Active (Production)`
4. click **Schema handling** menu item
5. switch **Lifecycle state** for **Normal Account** object type to `Active (Production)`
6. click **Save**
7. edit **AD** resource
8. click **Accounts**
9. click **Configure**, then click **Synchronization** item in the context menu
    a. for all situations **except Unmatched** switch **Lifecycle state** to `Active (Production)`
10. click **Save synchronization settings**

Reaction for **Unmatched** is not active, it will be only executed during simulations. No orphaned accounts will be automatically deleted (yet).

In your browser with midPoint, in **Accounts** panel for **AD** resource:

1. click **Tasks**, then click **Create task** item in the context menu to open a simple task creation wizard for AD accounts
    a. click **Reconciliation Task** tile
    b. toggle **Simulate task** to **ON**
    c. click **Create task** and fill in the following details:
        i. **Name**: `Reconciliation with AD - production simulation`
    d. click **Next: Resource objects**
    e. click **Next: Execution**
    f. in **Execution options** page, set the following:
        i. select **Mode**: `Preview`

ii. select **Predefined**: `Production`

g. click **Next: Schedule**

h. click **Next: Distribution**

i. click **Save & Run**

Running simulated reconciliation task with `Production` configuration will evaluate only `Active` (and `Deprecated`, which we do not use) configuration items, but there will be no permanent effects on data; we are only simulating.

In your browser with midPoint, in **Accounts** panel for **AD** resource:

1. click **Defined Tasks** menu item
2. open **Reconciliation with AD - production simulation**
3. click **Operation statistics** menu item and check correlation results
4. scroll down to **Synchronization situation transitions** section. Here you can see how the resource accounts were classified before/after the task execution. **Please note the operations were not actually executed as we have run the reconciliation in simulation mode.**
   a. 39 accounts previously not linked are now linked to midPoint users; final situation is **Linked**
   b. 1 account previously not linked is still not linked to midPoint users; final situation is **Unmatched** - this is orphaned account
   c. 4+1 accounts are **protected** (4 using marks including **Ana Lopez**, one from the configuration of resource copied from resource template)
5. click **Show simulation result**
6. the Simulation results show:
   a. 0 deactivated accounts (because the configuration to delete orphaned accounts is in `Proposed` lifecycle state and not evaluated now)
   b. 78 modified objects, where:
      i. midPoint users indicate added Projection (as a result of correlation of the account and linking it to its owner)
      ii. AD accounts indicate metadata changes (in midPoint repository only)

AD resource is ready for a safe correlation. No AD accounts are going to be deleted. Even if there would be new AD accounts created meanwhile, they would not be automatically deleted by midPoint. The orphaned accounts will be resolved later to not stop us from continuing the deployment.

LAB 5-4: Real Correlation With Active Directory

Estimated Time: 10 min.

In this lab, we will finally correlate the existing AD accounts to their midPoint owners. Based on the previous steps with simulations, we are sure that no unexpected actions are going to happen in Active Directory. CFO **Ana Lopez**'s account will not be correlated at this time.

In your browser with midPoint:

1. go to **Resources › All resources**
2. edit **AD** resource
3. click **Accounts** menu item
4. click **Tasks**, then click **Create task** item in the context menu to open a simple task wizard for AD accounts
   a. click **Reconciliation Task** tile
   b. keep **Simulate task** value **OFF**
   c. click **Create task**
      i. enter the task name: `Reconciliation with AD (real)`
   d. click **Next: Resource objects**
   e. click **Next: Schedule**
   f. click **Next: Distribution**
   g. click **Save & Run**
5. click **Defined Tasks** menu item
6. edit task **Reconciliation with AD (real)**
7. click **Operation statistics** menu item and check correlation results. The results are the same as during the simulations.
8. go to **Users › Persons**
   a. all linkable AD accounts are linked to their owners, 2 accounts are reported for all users (except `1002` - Ana Lopez)
   b. edit any user, e.g. **1006** (Martin Knight)
   c. click **Projections** menu item
   d. click **AD** account to display user's AD account attributes
9. go to **Resources › All resources**
10. edit **AD** resource

11. click **Accounts**
12. search for `Unmatched` accounts using the search panel:
    a. select **Situation**: `Unmatched`
    b. click **Basic**
13. All `Unmatched` accounts except `cn=Secret Admin,ou=users,dc=example,dc=com` are already marked from earlier steps
14. Any new `Unmatched` accounts (created meanwhile in AD) would have no marks
15. **Ana Lopez** will be resolved later

We have successfully correlated the vast majority of Active Directory accounts to their midPoint owners.

This concludes the Module 5 labs.