MidPoint: First Steps [MID301]

Student Lab Guide

Evolveum, s.r.o.

Revision 4.8-LTS-A.01, 2023-10-26

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.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

Table of Contents

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

Module 1: Planning Your Deployment Project

LAB 1-1: Inspect Your Environment

Estimated Time: TODO

In this lab, we will check the existing source and target systems and midPoint and access them using web browser. We do this in order to introduce the existing environment and to check the connections.

We have prepared a single point of access in a form of a simple static web page. A reverse proxy server is configured to limit the access.

In your browser:

1. go to `http://AWS_workstation_IP`

List of links to training containers is provided.

> For training courses delivered on publicly accessible machines (e.g. in cloud), training password `e=mc2` may be required for all services protected by the reverse proxy server.

Let's try **HR application** first. It is a simple application for HR data management for *demo* purposes. We are using it in this training as our HR system.

In your web browser with main navigation page:

1. click **HR application** link

   > As an alternative, you may go directly to `http://AWS_workstation_IP/hr/`

2. there is no authentication in this demo application
3. click **Show users**
4. list of HR records is displayed. These HR records will be imported to midPoint in later labs

> The data is sorted by `Id` column. No searching other than using web browser is possible in the Demo HR application at the moment.

Use page navigator under the table of HR records to move to previous/next pages.

To create a new person record (will be needed in future labs), you can click **Register user**.

To update existing person record (will be needed in future labs), you can click **Modify** button.

To export data from HR to a CSV file (will be needed in future labs), you can click **Export users to csv file**.

> Please do not do any modifications in HR data at this time.

Let's show our **Active Directory** (simulated by OpenLDAP server) now.

In your web browser with main navigation page:

1. click **AD LDAP browser**

> As an alternative, you may go directly to `http://AWS_workstation_IP/phpldapadmin/`

2. there is no authentication in the LDAP browser
3. expand the LDAP tree for `dc=example,dc=com` by clicking `+` button
4. expand `ou=users` container by clicking `+` button

You can click on any account in the left tree to display its details.

> Please do not do any modifications in AD/LDAP data at this time.

> We will simulate Active Directory using OpenLDAP. This is not a complete simulation, i.e. attribute names do not match real Active Directory, but the structure of the tree and usernames/distinguished names is similar to real Active Directory environment.

Finally, let's log in to **midPoint**.

In your web browser with main navigation page:

1. click **midPoint**

> As an alternative, you may go directly to `http://AWS_workstation_IP/midpoint/`

2. login to midPoint as:
   - **Username**: `administrator`
   - **Password**: `1st3ps`
3. go to **Users › All users** to display the list of midPoint users
   a. only user `administrator` is listed

This concludes the Module 1 labs.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

Module 2: Connecting Source System

LAB 2-1: Create HR Resource

Estimated Time: TODO

In this lab, we will configure midPoint to connect to HR data exported as CSV file.

In your browser with HR application:

1. click **Show users**
2. click **Export users to csv file**

HR application should display the following message next to the button:

```
Successfully exported
```

Data is exported to a file in HR application server. The file is available for midPoint server using docker *volume*.

In your browser with midPoint:

1. go to **Resources › New resource**
2. click **From scratch** tile
3. click **CSV Connector**
4. configure the resource **Basic information**:
   a. **Name**: `HR`
   b. **Lifecycle state**: `Proposed`
5. click **Next: Configuration** button to open **Establish the connection** configuration
   a. **File**: `/opt/midpoint/var/resources/export.csv`
6. click **Next: Discovery** button to open **MidPoint Discovery** configuration:
   a. **Unique attribute**: `empnum`
7. click **Next: Schema** button to open **Schema** configuration:
   a. keep defaults
8. click **Create resource** button
9. click **Preview resource data** tile to list existing accounts in HR
10. click **Back**

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

We have succeeded in connecting the HR export file. Now we need to create object type configuration in midPoint. As the HR export file contains only one type of records (employees), we will need only one object type definition.

1. click **Configure Object Types** tile
2. click **Add object type** button to create new object type
3. configure Basic information:
   a. **Display name**: `HR Person`
   b. **Kind**: `account`
   c. **Intent**: (keep it empty)
   d. **Default**: `True`
4. click **Next: Resource data** button
5. configure Resource data:
   a. **Object class**: make sure `AccountObjectClass` is selected. This is the only object class supported by the CSV connector (represents CSV rows as accounts)
6. click **Next: MidPoint Data**
7. configure MidPoint data: by this configuration we specify, to which midPoint objects this object type corresponds (and will create in midPoint)
   a. **Type**: select `User`
   b. **Archetype**: do not set yet, we will do it later
8. click **Save settings** button
9. click **Preview data**

At this moment, we have prepared a basic configuration of object type. While previewing HR data, you will notice that there are also non-IT employees (their HR employee numbers start with `8xxx`) - and we wish to ignore such employees.

One possibility would be to modify the HR export mechanism to not include such employees in the export file.

In our case, we will do the configuration in midPoint to show its flexibility (changes in HR export mechanism could take some time).

1. click **Back**
2. click **Basic Attributes** tile
3. click **Next: Resource data**
4. in **Specify the resource data** page, enter the following:
   a. **Filter**: paste the following query:

Skip HR accounts starting with 8 (non-IT personnel):

```
attributes/empnum not startsWith "8"
```

5. click **Next: MidPoint data**
6. click **Save settings**
7. click **Back to object types**
8. click **Exit wizard**
9. click **Go To Resource** tile
10. click **Resource objects** menu item. All HR accounts are displayed here, regardless of (even potentially multiple) object types.
11. click **Reclassify** button and confirm **Yes**
12. reclassification task will be executed in background, processing all HR accounts and update midPoint metada for them
13. click **Accounts** menu item to list all accounts after reclassification
14. accounts starting with `8` should be now hidden from the list as they no longer match the classification filter. midPoint is aware of them, but they are no longer considered "HR Person" (they will not have intent `default` but `kind=unknown` and `intent=unknown`)

We have successfully configured midPoint to connect to the CSV file exported from HR system and even to ignore certain HR records.

The object type definition is by default in `Active` lifecycle state, but the whole resource is still in `Proposed`, which overrides the object type lifecycle state. TODO can I have more about this - maybe in slides. Can't find doc. Slide about hierarchy, overrides etc. for lifecycle state for configuration items... We will continue the resource configuration and prepare for simulations in the following lab.

LAB 2-2: Configure HR Resource

Estimated Time: TODO

In this lab, we will configure HR resource for data import.

In your browser with midPoint:

1. edit **HR** resource
2. click **Accounts** menu item
3. click **Configure**, then click **Synchronization** item in the context menu
   a. use **Add reaction** to fill this configuration:

Name	Situation	Action	Lifecycle state
unmatched-add	Unmatched	Add focus	Active
linked-synchronize	Linked	Synchronize	Active

   b. click **Save synchronization settings**
4. The synchronization configuration items are in `Active` lifecycle state, but the whole resource is still in `Proposed`, which overrides the synchronization configurations lifecycle states.
5. click **Configure**, then click **Mappings** item in the context menu
   a. for each attribute, click **Add inbound** button

Name	From resource attribute	Expression	Target	Lifecycle state
empnum-to-name	empnum	As is	name	Active
empnum-to-persNumber	empnum	As is	personalNumber	Active
firstname-to-givenName	firstname	As is	givenName	Active
surname-to-familyName	surname	As is	familyName	Active

6. click **Save mappings**
7. The mappings are in `Active` lifecycle state, but the whole resource is still in `Proposed`, which overrides the mappings' lifecycle states.

As the last step, we will disable any write attempt to the CSV file using resource capabilities, as a precaution.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

We will configure the capabilities on the resource level (global). It is also possible to configure the capabilities on object-type level, but we will not use this option now.

1. click **Details** menu item
2. click **Create** to disable the `Create` operation for this resource
3. click **Update** to open **Update objects** popup, then update the following to disable the `Update` operation for this resource:
   a. **Enabled**: `False`
   b. click **OK**
4. click **Delete** to disable the `Delete` operation for this resource
5. click **Save** to save resource

From now on, HR resource is now considered read-only. Any attempt to issue create, update or delete operation on the resource would fail with **Operation not supported** error.

This concludes the Module 2 labs.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

Module 3: Importing Source Data

LAB 3-1: Single Source System Entry Import Simulation

Estimated Time: TODO

In this lab, we will simulate a single source system account import and improve the resource configuration based on the results of simulation. This is how the usual midPoint deployment works: we are improving the configuration in iterations. Thanks to the simulations, we can do it without any consequences.

In your browser with midPoint:

1. go to **Resources › All resources**
2. edit **HR** resource
3. click **Accounts** menu item
4. click context menu for account `1001` 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.

6. **1001** user is indicated to be *activated* (created and/or enabled)
7. click **1001** user entry in the list of processed objects to display the details
   a. notice which user properties are being populated from HR by the import and that **Locality** and **Lifecycle status** attribute values are not being populated
8. click **Back** to get to the list of processed objects
9. click **Back** to get to the list of HR accounts
10. click **Configure**, then click **Mappings** item in the context menu
    a. use **Add inbound** button to create two additional mappings:

Name	From resource attribute	Expression	Target	Lifecycle State
locality-to-locality	locality	As is	locality	Active

Name	From resource attribute	Expression	Target	Lifecycle State
status-to-lifecycle-state	status	Script	lifecycleState	Active

b. click **Show script** for the `status` attribute mapping

   i. paste the following code:

```
switch (input) {
    case 'In':
        'active'
        break

    case 'Long-term leave':
        'suspended'
        break

    case 'Former employee':
        'archived'
        break

    //default:
       //'suspended'
       //break
}
```

   ii. click **Done**

c. click **Save mappings**

11. click context menu for account (1001) and select **Import preview**
12. in **Select task execution mode** select: **Simulated development** and click **Select**
13. click **1001** user entry in the list of processed objects to display the details
    a. notice which user properties are being populated from HR by the import and that **Locality** (`Small Red Rock City`) and **Lifecycle state** (`active`) are now being populated as well
14. click **Back** to get to the list of processed objects
15. click **Back** to get to the list of HR accounts
16. in resource's **Lifecycle state** toolbar, select `Active (Production)`

We have finished the HR resource configuration. We have simulated the import and validated the attribute mappings. Resource is ready to be used for data import to midPoint.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

LAB 3-2: Source System Data Import

Estimated Time: TODO

In this lab, we will import data about users from HR resource.

In your browser with midPoint:

1. edit **HR** resource
2. click **Accounts** menu item
3. click **Tasks**, then click **Create task** item in the context menu to open a simple task creation wizard
   a. click **Import Task** tile to select it
   b. keep **Simulate task** value **OFF**
   c. click **Create task**
   d. keep the task name empty and midPoint will generate its own task name
   e. click **Next: Resource objects**
   f. keep defaults.

      If you are wondering why the `intent` is set to `default`, it is because we have not set any intent when creating the object type definition - that corresponds to an intent named `default`.

   g. click **Next: Distribution**
   h. keep defaults
   i. click **Save & Run**

A new import task has been created and started in background. We will check the import progress and status.

In your browser with midPoint:

1. display the tasks by using either:
   a. go to **Server tasks › Import tasks** ; or
   b. click **Tasks** and click **View import tasks** item in the context menu ; or
   c. click **Defined Tasks** menu item
2. click the task **Import task: HR: HR Person** to open task details
   a. click **Operation statistics** to watch the task progress
   b. Summary of processed objects and Synchronization situation transitions are displayed.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

This allows to understand what just happened. We can see 40 (1+39) accounts are now linked to their corresponding midPoint owners (users) - which have been created during the process.

3. go to **Users › All users** and check if users are imported.
4. edit user **1001** and notice which user properties are populated in user's **Basic** panel (displayed by default)
5. click **Back**

Only IT-related users should be imported because classification filter we have defined in the resource. Users with personal number starting with 8 were not imported to midPoint.

You may have noticed that no full names are filled (yet). Also, we have created just "ordinary" users. We will improve the situation by introducing archetypes.

You may think of archetype as an object *category*. It helps administrators to distinguish between objects visually, but later we can define specific behavior for each archetype. We will use midPoint built-in archetype `Person` and reimport users from HR.

In your browser with midPoint:

1. go to **Users › Persons** and check there are no entries
2. go to **Resources › All resources**
3. edit **HR** resource
4. click **Accounts** menu item
5. click **Configure**, then click **Basic attributes** item in the context menu
6. click **Next: Resource data**
7. click **Next: MidPoint data**
   a. **Archetype**: click **Choose**, then click **Person**
8. click **Save settings**
9. click **Exit wizard**
10. click **Defined Tasks** menu item
11. click the task **Import task: HR: HR Person** to display task details
12. click **Operation statistics** to watch the task progress
13. click **Run now** button and wait for the task completion (task status: closed)
14. go to **Users › Persons** and check if users are imported

You may have noticed that users now have full names populated! This is a direct consequence of assigning `Person` archetype. We will explain this later in the course.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

This concludes the Module 3 labs.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

Module 4: Connecting Target system

LAB 4-1: Creating Active Directory Resource From Template

Estimated Time: TODO

In this lab, we will create a new resource for Active Directory target system. Unlike in previous labs, we will not create it from scratch. We will use a predefined resource template and copy the new resource from it. This way our resource will not depend on the template after it is created.

> For simplicity and to allow using docker on any operating system, we use OpenLDAP instead of Active Directory. The directory structure and account naming conventions are made *similar* to real Active Directory.

In your browser with midPoint:

1. go to **Resources › New resource**
2. click **Copy From Template** tile
3. click **Training Active Directory Resource Template**
4. set Basic information:
   a. **Name**: `AD`
   b. **Description**: `ExAmPLE, Inc. AD resource`
   c. **Lifecycle state**: keep `Proposed`
5. click **Next: Configuration** to display **Establish a connection** section:
   a. **Host**: `ad`
   b. **Port**: `389`
   c. **Bind DN**: `cn=idm,ou=Administrators,dc=example,dc=com`
   d. **Bind password**: `secret`
6. click **Next: Discovery** to open **MidPoint Discovery** section
   a. **Base context:** make sure `dc=example,dc=com` is displayed
7. click **Next: Schema** to display **Schema** configuration
   a. keep defaults
8. click **Create resource**
9. click **Preview Resource Data** tile

   a. select `inetOrgPerson` object class to display the existing account in your AD resource

10. click **Back**
11. click **Go To Resource** tile

We have successfully created a new resource from resource template. The configuration is already present; we will review and/or update it to our needs in the following labs.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

LAB 4-2: Reviewing Active Directory Resource Synchronization Configuration

Estimated Time: TODO

In this lab, we will review the synchronization configuration of AD resource which has been copied from the resource template.

The resource and all object types are in `Proposed` lifecycle states, so the resource is ready for simulations but not for normal use.

We will review synchronization configuration first.

> Please do not change any resource configuration while reviewing it.

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 **Configure**, then click **Synchronization** item in the context menu

Synchronization configuration is already in place from the resource template.

All synchronization reactions are in `Proposed` lifecycle state, so they can be used for simulations. The configuration is typical for a target system. Notice the reaction for **Unmatched** (orphaned) accounts is **Delete resource object** rather than **Add focus** which we have used for HR resource.

Click **Exit wizard** to get back to account list.

We will review correlation configuration now.

> Please do not change any resource configuration while reviewing it.

1. click **Configure**, then click **Correlation** item in the context menu
2. There are two correlation rules:
   a. rule `personalNumber-correlation` to correlate by user's personal number vs AD's `employeeNumber` attribute is in place and active (not disabled)
   b. rule `last-resort-correlation` to correlate by other attributes is currently not active (will be used later)
3. you can click **Edit** for any correlation rule to display its details

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

Correlation configuration is already in place from the resource template.

Click **Exit wizard** to get back to account list.

We will review inbound mappings now.

1. click **Configure**, then click **Mappings** item in the context menu
2. there are several inbound mappings, all of them are active, but used **only for the correlation** (indicated by icon)

Click **Exit wizard** to get back to account list.

The resource created from resource template is ready to be used for simulations.

This concludes the Module 4 labs.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

Module 5: Target System Integration

LAB 5-1: Simulated Correlation With Active Directory

Estimated Time: TODO

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.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

LAB 5-2: Marking Accounts

Estimated Time: TODO

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).

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

LAB 5-3: Ignoring Orphaned Accounts

Estimated Time: TODO

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.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

LAB 5-4: Real Correlation With Active Directory

Estimated Time: TODO

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

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

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.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

Module 6: Importing Usernames From Target Systems

LAB 6-1: Preparing Configuration For Username Import

Estimated Time: TODO

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 for `empnum → 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

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

a. do not modify the existing mappings used **only for the correlation** (indicated by icon)

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: TODO

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 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.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

LAB 6-3: Username Import From Active Directory

Estimated Time: TODO

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-import-to-name` 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 `Do not correlate`. 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.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

LAB 6-4: Deleting Orphaned Active Directory Accounts

Estimated Time: TODO

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 account` 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)

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

3. 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)

4. click **Back**
5. click **Accounts** menu item
6. search for `Unmatched` accounts using the search panel:
   a. select **Situation**: `Unmatched`
   b. click **Basic**
7. 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:

1. expand **dc=example,dc=com**
2. expand **ou=users**
3. 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.

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.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

LAB 6-5: Finalize Correlation

Estimated Time: TODO

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 **Reconcile with AD (real)** task using **Run now** and wait for the task completion (task status: closed)
6. blick **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.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

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 `emploeeNumber` 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.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

Module 7: Enable Provisioning to Target Systems

LAB 7-1: Reviewing Active Directory Resource Provisioning Configuration

Estimated Time: TODO

In this lab, we will review the provisioning configuration of AD resource which has been copied from the resource template.

The provisioning configuration is either in `Proposed` or `Draft` lifecycle states, so the resource is not yet ready for normal use.

> Please do not change any resource configuration while reviewing it.

In your browser with midPoint:

1. go to **Resources › All resources**
2. edit **AD** resource
3. click **Accounts**

We will review outbound attribute mappings now. These mappings are already in place from the resource template.

> Please do not change any resource configuration while reviewing it.

1. click **Configure**, then click **Mappings** item in the context menu
2. click **Outbound mappings (to Resource)** to display the outbound mappings
3. there are several outbound mappings prepared for future use, all of them are in `Draft` lifecycle state, so they are effectively disabled. The configuration is typical for a target Active Directory resource

These mappings are already in place from the resource template.

Click **Exit wizard** to get back to account list.

We will review activation outbound mappings now. These mappings are already in place from the resource template.

> Please do not change any resource configuration while reviewing it.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

1. click **Configure**, then click **Activation** item in the context menu
2. click **Outbound**
3. there are three outbound activation mappings, all of them in `Draft` lifecycle state, so they are effectively disabled:
   a. mapping `set-account-status-based-on-midpoint-user` will be later used to enable/disable AD account based on midPoint user status
   b. mapping `Disable instead of delete` will be later used to disable AD account instead of deleting it if the user has no "reason" to have an account there
   c. mapping `Delayed delete` will be later used to delete AD account after it has been disabled for configured time if the user has no "reason" to have an account there.
      i. click **Settings** to display the time configuration for the delayed account deletion (please do not make any changes)
4. click **Exit wizard** to get back to the account list

We will review credentials outbound mappings now. These mappings are already in place from the resource template.

> Please do not change any resource configuration while reviewing it.

1. click **Configure**, then click **Credentials** item in the context menu
2. click **Outbound**
3. there are two outbound credentials mappings, all of them in `Draft` lifecycle state, so they are effectively disabled:
   a. mapping `initial-password-generate` will be later used to generate a random *initial* password (using a *weak* mapping) for AD account (as the account cannot be passwordless). This password won't be stored and will be unknown to the user; we assume the user will activate his/her AD account by visiting the company's helpdesk
   b. mapping `password-change` will be later used to allow password changes from midPoint to Active Directory

> We will not allow end-user access not password changes via midPoint in this training.

Click **Exit wizard** to get back to account list.

The resource created from resource template is ready to be used for provisioning simulations.

LAB 7-2: Active Directory Provisioning Simulation

Estimated Time: TODO

In this lab, we will re-use some of the outbound mappings for Active Directory which were preconfigured in the resource template, and we will simulate the provisioning first. This step is very important as there might be data inconsistencies in Active Directory and midPoint (based on HR data,) and we don't want to have any unexpected attribute changes.

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. click **Outbound mappings (to Resource)**
   b. select the following **outbound** mappings (there are more mappings prepared in the resource template, but we - as in real life - will not need to use all of them):
      i. `mapping-dn`
      ii. `mapping-cn-weak`
      iii. `mapping-displayName`
      iv. `mapping-sn`
      v. `mapping-givenName`
      vi. `mapping-uid`
      vii. `mapping-l`
      viii. `mapping-employeeNumber`
   c. click ❤ button (tooltip: **Change lifecycle state**) in the table header and select `Proposed (simulation)`
   d. click **Apply changes**
   e. click **Save mappings**

We will also update the configuration for activation outbound mapping(s) to see if midPoint is going to change any account's status:

1. click **Configure**, then click **Activation** item in the context menu
   a. click **Outbound**
   b. for all outbound mappings, switch lifecycle in upper right corner to `Proposed (simulation)`

   c. click **Save settings**

We will also update the configuration for credentials (password) outbound mapping(s) to see if midPoint is going to change any account's password:

1. click **Configure**, then click **Credentials** item in the context menu
   a. click **Outbound**
   b. for all outbound mappings, switch lifecycle in upper right corner to `Proposed (simulation)`
   c. click **Save settings**

Now we are ready to run the simulated reconciliation.

1. click **Defined Tasks** menu item
2. edit **Reconciliation with AD - development simulation** task
3. click **Run now** and wait for the task completion (task status: closed)
4. click **Show simulation result**
5. the Simulation results show:
   a. 5 accounts are going to be renamed (DN is being changed) - as AD DN contains user's `fullName` - if users had incorrect DN/CN in AD, they will be now corrected/renamed, e.g. `cn=Ema Jones` instead of `cn=Emma Jones`
   b. 2 users are being deactivated (disabled) because of incorrect data in AD (their accounts should be disabled and are not): `cn=Jane Anderson` and `cn=Laura Shepherd` are enabled in AD, but are on **Long-term leave** in HR
   c. AD `employeeNumber` attribute is being updated for Ana Lopez
   d. no passwords are going to be changed
   e. no accounts are going to be deleted

This is the time to analyze the results of the simulation. Make sure to check all entries in the simulation results. Are the changes expected? Are the changes good or bad? Thanks to the simulation, nothing has been executed yet, we have time to think and fix the situation.

Usually you will either let midPoint to execute the changes in Active Directory, or fix the data in HR. It is also possible to update the mappings to provide some conditional behaviour (outside of scope for this training). You could also mark some AD accounts as "Do not touch" and resolve these exceptions later.

In general, the simulation results show that midPoint is trying to fix the target system data using HR data - which we consider as more authoritative and thus better, at least in this particular lab.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

LAB 7-3: Active Directory Provisioning

Estimated Time: TODO

In this lab, we will turn on provisioning to Active Directory after successful simulation from previous lab.

We will switch all simulated mappings of attributes, activation and credentials to `Active` lifecycle state.

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. click **Outbound mappings (to Resource)**
   b. select the following **outbound** mappings:
      i. `mapping-dn`
      ii. `mapping-cn-weak`
      iii. `mapping-displayName`
      iv. `mapping-sn`
      v. `mapping-givenName`
      vi. `mapping-uid`
      vii. `mapping-l`
      viii. `mapping-employeeNumber`
   c. click 💗 button (tooltip: **Change lifecycle state**) in the table header and select `Active (production)`
   d. click **Apply changes**
   e. click **Save mappings**

We will also update the configuration for activation outbound mapping(s):

1. click **Configure**, then click **Activation** item in the context menu
2. click **Outbound**
   a. for all outbound mappings, switch lifecycle in upper right corner to `Active (production)`
   b. click **Save settings**

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

We will also update the configuration for credentials (password) outbound mapping(s):

1. click **Configure**, then click **Credentials** item in the context menu
2. click **Outbound**
   a. for all outbound mappings, switch lifecycle in upper right corner to to `Active (production)`
   b. click **Save settings**

We will run the simulated reconciliation one last time. All configuration is already in `Active` lifecycle state.

1. click **Defined Tasks** menu item
2. edit and run **Reconciliation with AD - production simulation** task using click **Run now** and wait for the task completion (task status: closed)
3. click **Show simulation result**
4. the Simulation results show:
   a. 8 objects to be updated in AD just like before

Finally, let's run the real reconciliation.

1. click **Back** until you get to **Defined tasks** page
2. edit and run **Reconciliation with AD (real)** task again using **Run now** and wait for the task completion (task status: closed)
3. go to **Audit log viewer** and check what has happened (8 AD accounts modifications should be displayed)

If you want, you can also check the accounts in AD.

In your browser with AD LDAP browser:

1. expand **dc=example,dc=com**
2. expand **ou=users**
3. click any account from the previously updated ones, for example:
   a. `cn=Ana Lopez` should have her `employeeNumber: 1002`
   b. `cn=Jane Anderson` and `cn=Laura Shepherd` should be disabled (simulated by `roomNumber: disabled`)

From now on, provisioning to AD resource is active for all attributes with mappings with `Active` lifecycle status, account activation status and credentials.

Automatic synchronization between HR and midPoint is not yet configured.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

This concludes the Module 7 labs.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

Module 8: Automating Integration

LAB 8-1: Generate Usernames in midPoint

Estimated Time: TODO

In this lab, we will turn on midPoint username generator and start using it instead of using user's employee number from HR or existing AD username.

We will switch off the existing configuration first.

In your browser with midPoint:

1. go to **Resources › All resources**
2. edit **HR** resource
3. click **Accounts** menu item
4. click **Configure**, then **Mappings** tile
   a. for the inbound mapping `empnum` → `name`:
      i. change **Lifecycle state** to: `Archived` to disable it
5. click **Save mappings**
6. click **Back** to get to the list of resources
7. edit **AD** resource
8. click **Accounts** menu item
9. click **Configure**, then **Mappings** tile
   a. for the inbound mapping `mapping-inbound-username-import-to-name` for `uid` → `name` attribute:
      i. change **Lifecycle state** to: `Archived` to disable it
10. click **Save mappings**

> We use `Archived` lifecycle state to indicate that the mapping is unlikely to be active again. For temporary mapping deactivation you may use `Suspended` lifecycle state. Both states (and also `Draft`) represent deactivated mappings, but we have those three states to express different reasons for mapping deactivation.

Now we will use object template to generate the username instead.

1. go to **Object templates › All object templates**

2. click **Person Object Template**
3. click **Mappings** menu item
   a. for the mapping `generate-name-jsmith-8-2`, set the following attributes:
      i. **Lifecycle state**: switch to `Active (production)`
4. click **Save**

The `Person Object Template` is used for all users with `Person` archetype. It is part of midPoint built-in objects. We have been actually using almost from the beginning of the course to generate users' full names.

> We are setting the mapping's lifecycle state directly to `Active`, without first going through the simulations. We can afford this in this particular case as there is no automatic synchronization with HR yet and this mapping won't affect any existing users in midPoint (`weak` strength).
>
> We will still use simulations before creating the users.

We will create new test users in HR application.

In your browser with HR application:

1. click **Register user** and fill in the following attributes:
   a. **First name**: `Louise`
   b. **Surname**: `Callahan`
   c. **Employee number**: `9000`
   d. **Locality**: `White Stone City`
   e. **Job**: `222#Export/Import Coordinator`
   f. **EmpType**: select/keep `FTE`
   g. **Status**: select/keep `In`
   h. click **Register user**
2. click **Register user** and fill in the following attributes:
   a. **First name**: `Andreas`
   b. **Surname**: `Baker`
   c. **Employee number**: `9001`
   d. **Locality**: `White Stone City`
   e. **Job**: `222#Export/Import Coordinator`
   f. **EmpType**: select/keep `FTE`

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

   g. **Status**: select/keep `In`
   h. click **Register user**
3. click **Register user** and fill in the following attributes:
   a. **First name**: `Clara`
   b. **Surname**: `Whiteherring`
   c. **Employee number**: `9002`
   d. **Locality**: `White Stone City`
   e. **Job**: `222#Export/Import Coordinator`
   f. **EmpType**: select/keep `FTE`
   g. **Status**: select/keep `In`
   h. click **Register user**
4. click **Register user** and fill in the following attributes (this user will have the same First name and Surname as the previous one):
   a. **First name**: `Clara`
   b. **Surname**: `Whiteherring`
   c. **Employee number**: `9003`
   d. **Locality**: `White Stone City`
   e. **Job**: `222#Export/Import Coordinator`
   f. **EmpType**: select/keep `FTE`
   g. **Status**: select/keep `In`
   h. click **Register user**
5. click **Register user** and fill in the following attributes:
   a. **First name**: `Jacques`
   b. **Surname**: `Smith`
   c. **Employee number**: `9004`
   d. **Locality**: `White Stone City`
   e. **Job**: `222#Export/Import Coordinator`
   f. **EmpType**: select/keep `FTE`
   g. **Status**: select/keep `In`
   h. click **Register user**
6. click **Export users to csv file**

In your browser with midPoint:

1. go to **Resources › All resources**
2. edit **HR** resource
3. click **Accounts** menu item
4. click **Reload** to reload the list of accounts from HR application CSV export file (midPoint is not aware of them as there is no automatic synchronization (yet))
5. search for accounts having `90` in **Name** field (or scroll to the last page of accounts)
6. find the new account `9000` and click **Import preview**
7. in **Select task execution mode** select: **Simulated production** and click **Select**

> **Simulated production** mode will evaluate all `Active` (and `Deprecated`) configuration items, but there will be no permanent effects on data; we are only simulating.

8. midPoint will display information about new user `lcallaha` (and not `9000`) which would be created
9. click **Back**
10. find the new account `9001` and click **Import preview**
11. in **Select task execution mode** select: **Simulated production** and click **Select**

> **Simulated production** mode will evaluate all `Active` (and `Deprecated`) configuration items, but there will be no permanent effects on data; we are only simulating.

12. midPoint will display information about new user `abaker2` (and not `9001`) which would be created (midPoint appends a number `2` because `abaker` user already exists in midPoint)
13. click **Back**

The username generator looks good! Let's create a scheduled reconciliation with HR.

1. click **Tasks**, then click **Create task** item in the context menu to open a simple task creation wizard for HR accounts
   a. click **Reconciliation Task** tile
   b. keep **Simulate task** value **OFF**
   c. click **Create task** and fill in the following details:
      i. **Name**: `HR Reconciliation`
   d. click **Next: Resource objects**
   e. click **Next: Schedule**
   f. in **Schedule** page, set the following:

   i. Set **Interval**: `60` (seconds)

g. click **Next: Distribution**

h. click **Save & Run**

2. go to **Users** › **Persons** and check the new users (no AD accounts have been created for them yet)

3. to display only those users, you may want to use midPoint's query language:

   a. in search panel above the user list, click ▾ and select **Advanced**

   b. paste the following query to the input box:

```
personalNumber startsWith "900"
```

   c. click **Advanced** to apply the query

4. the resulting users should match the information in the following table:

HR empnum / midPoint personalNumber	midPoint username	midPoint fullName	Notes
9000	lcallaha	Louise Callahan	No uniqueness issues
9001	abaker2	Andreas Baker	Iterated, because `abaker` (Alice Baker) already exists
9002	cwhitehe2	Clara Whiteherring	Iterated, because `cwhitehe` (Charles Whitehead) already exists
9003	cwhitehe3	Clara Whiteherring	Iterated, because `cwhitehe` (Charles Whitehead) and `cwhitehe2` (Clara Whiteherring) already exist
9004	jsmith3	Jacques Smith	Iterated, because `jsmith` (John Smith) and `jsmith2` (Joseph Smith) already exist

5. to switch to basic search and stop using the query, click ▾ and select **Basic** in the search panel

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

6. go to **Audit Log Viewer** and check what the reconciliation tasks did
   a. look for **Event type**: **Add object** operations for **Channel**: **Reconciliation**

> The username generator in `Person Object Template` generates values usable as Active Directory `sAMAccountName` values (strings shorter than 20 characters).

The reconciliation task is scheduled and will look for new/updated data in HR resource each minute.

LAB 8-2: Automate Active Directory Account Creation For All Persons

Estimated Time: TODO

In this lab, we will configure midPoint to create AD accounts automatically.

In most cases, midPoint roles and/or organizations are used for provisioning, but we have no roles yet. On the other hand, we have already assigned `Person` archetype automatically to each user created from HR resource. We will use `Person` archetype to create AD accounts as a *birthright* of each user created from HR data.

In your browser with midPoint:

1. go to **Archetypes › All archetypes**
2. edit **Person** archetype
3. go to **Inducements › Resource**
4. click **New**
   a. select **AD**
   b. click **Next: Resource object type**
   c. click **Next: Entitlements**
   d. click **Next Mappings**
   e. click **Save settings**
5. click **Back** as the archetype has been already saved automatically after the previous step
6. wait for the next regular reconciliation with HR resource, it will add the AD accounts for the new users (otherwise full recomputation is needed)
7. check the users created earlier and their Active Directory DNs either by checking users and their accounts or using **AD LDAP browser**

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

midPoint username	midPoint fullName	AD DN	Description
lcallaha	Louise Callahan	cn=Louise Callahan,ou=users,dc=example,dc=com	No AD DN uniqueness issues
abaker2	Andreas Baker	cn=Andreas Baker,ou=users,dc=example,dc=com	No AD DN uniqueness issues
cwhitehe2	Clara Whiteherring	cn=Clara Whiteherring,ou=users,dc=example,dc=com	No AD DN uniqueness issues
cwhitehe3	Clara Whiteherring	cn=Clara Whiteherring (cwhitehe3),ou=users,dc=example,dc=com	Iterated, because `cn=Clara Whiteherring,ou=users,dc=example,dc=com` already exists (for user `cwhitehe2` (Clara Whiteherring)).
jsmith3	Jacques Smith	cn=Jacques Smith,ou=users,dc=example,dc=com	No AD DN uniqueness issues

The distinguished name is made unique in AD's outbound mapping for `dn` attribute by using a simple Groovy script. The value is either `CN=Full Name`, if the Full Name is unique or `CN=Full Name (username)` if it is not.

Let's check if there are any persons without AD account:

1. go to **Users › Persons**
2. in search toolbar, locate **Users without account** search criteria
   a. click ⚙ button (tooltip: **Property settings**) to open a popup window:
      i. in **Name**: click the button and select **AD** resource
   b. check the ☐ for **Users without account** to apply the search criteria

There should be no users without AD resource accounts.

To stop using the search criteria, uncheck the checkbox for **Users without account** in search toolbar.

By the previous configuration, we instructed midPoint to create accounts in AD resource for all users with `Person` archetype. Users in midPoint are kept forever even for former employees. AD

accounts are configured to be disabled for users in `Long-term leave` or `Former employee` HR state and deleted later for `Former employee` state. This will be demonstrated later.

The new users created by midPoint have no passwords. They cannot log in to midPoint. Their AD passwords were randomly generated using a weak (one-time) activation outbound mapping in AD resource. For the sake of this training, we assume the users will visit helpdesk to reset their AD account passwords.

midPoint can be configured for authentication using Active Directory. It can also be used to change the passwords in Active Directory using its self-service interface. This configuration is out of scope of this training.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

LAB 8-3: Automate Active Directory Group Membership For All Persons

Estimated Time: TODO

In this lab, we will update midPoint provisioning configuration for AD resource to make all accounts of Person users members of a fixed pre-existing group.

The group membership management (called `association` in midPoint) is already prepared to be used in our AD resource from the resource template. We will review this configuration first.

In your browser with midPoint:

1. go to **Resources › All resources**
2. edit **AD** resource
3. click **Schema handling** menu item
4. notice the object type definition **AD Group** in `Proposed` lifecycle state

> Do not change the configuration of **AD Group** object type. It is required by the association configuration, but we will not use it in this training in any other way.

5. click **Accounts** menu item
6. click **Configure**, then click **Associations** item in the context menu
   a. the `adGroup` association for group's `member` attribute is configured in `Proposed` lifecycle state, ready for simulations.
7. click **Exit wizard**

As the configuration is in `Proposed` lifecycle state, even if we have already scheduled reconciliation for HR resource, nothing bad will happen. You **don't** need to stop the scheduled task!

We will configure `Person` archetype to put all accounts to AD's `cn=all-users` group.

1. go to **Archetypes › Person**
2. edit **Person** archetype
3. click **Inducements › Resource**
4. edit **AD** resource inducement
   a. click **Construction Associations** tab
      i. click + button

   ii. in **Grant entitlements / Group membership** popup click on group **cn=all-users,ou=groups,dc=example,dc=com** or click **Reload** first if no groups are displayed
   iii. click **Done**
   b. click **Done**
5. click **Save**

We will simulate what will happen for a single account, as usual.

1. go to **Resources › All resources**
2. edit **HR** resource
3. click **Accounts** menu item
4. click context menu for account `9000` and select **Import preview**
   a. 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. In our particular case, the only `Proposed` configuration is the association configuration in AD resource.

5. `cn=Louise Callahan,ou=users,dc=example,dc=com` AD resource account has a new indication *Projection entitlement changed*. Clicking the account simulation details will reveal a new association with group `cn=all-users` is going to be made
6. click **Back** to get to the list of processed objects
7. click **Back** to get to the list of HR accounts

We can run a simulated import or reconciliation task from HR resource to see what will happen for all users:

1. click **Tasks**, then click **Create task** item in the context menu to open a simple task creation wizard for HR accounts
   a. click **Import Task** tile
   b. toggle **Simulate task** to `ON`
   c. click **Create task** and fill in the following details:
      i. **Name**: `Import from HR - 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: Distribution**
  h. click **Save & Run**

> Running simulated import 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.

2. click **Defined Tasks** menu item
3. edit the task **Import from AD - development simulation** and wait for the task completion (task status: closed)
4. click **Show simulation result**
5. the Simulation results show:
    i. all 5 recently created AD accounts are going to be added to `cn=all-users,ou=groups,dc=example,dc=com` group (click **More info** in **Projection entitlement changed** tile to see more details)

Simulation looks OK for all 5 AD accounts. Let's activate the association configuration.

1. go to **Resources › All resources**
2. edit **AD** resource
3. click **Accounts** menu item
4. click **Configure**, then click **Associations** item in the context menu
    a. switch `adGroup` association lifecycle state to: `Active`
5. click **Save association settings**
6. wait for next regular reconciliation with HR resource, it will add the AD accounts for the new users to the `cn=all-users` group

To check the account membership after the reconciliation with HR finishes:

1. go to **Users › Persons**
2. edit any of the 5 recent users, e.g. `lcallaha`
3. click **Projections** menu item
4. click **AD** account
5. scroll down to **Associations** container
6. **AD Group Membership** should include the value: `cn=all-users,ou=groups,dc=example,dc=com`

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

All existing AD accounts before midPoint deployment were already members of the group. All newly created AD accounts for people from HR will be automatically members of the group from now on.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

LAB 8-4: Enforcing AD Account Data

Estimated Time: TODO

In this lab, we will test how midPoint enforces the values provided by its policies. We already know that midPoint can automatically detect orphaned account and delete them. But what about unauthorized AD account changes?

We will stop scheduled reconciliation with HR resource as it would fix *some* inconsistencies automatically, and we would like to explain what's going on.

In your browser with midPoint:

1. go to **Resources › All resources**
2. edit **HR** resource
3. click **Defined Tasks** menu item
4. edit task **HR Reconciliation**
5. click **Suspend** to suspend the task

We will delete one AD account directly in AD LDAP browser - such action is certainly possible, as AD administrator may, in error or not, delete account managed by midPoint.

In your browser with AD LDAP browser:

1. expand **dc=example,dc=com**
2. expand **ou=users**
3. edit **cn=Alexander Freeman**
4. click **Delete this entry**
5. confirm by clicking **Delete**

AD account was deleted.

Now we will try to update some AD account attributes outside midPoint.

In your browser with AD LDAP browser:

1. expand **dc=example,dc=com**
2. expand **ou=users** or click **Refresh** in the tree
3. edit **cn=Alice Baker**
   a. change the following attributes:
      i. **l**: `Silver City`

    ii. **givenName**: `Al`

  b. click **Update object**

  c. click **Update object**

4. expand **ou=groups**
5. edit **cn=all-users**
6. scroll down in the right panel and click **(modify group members)**
7. in the right part, in the list of **Group members**:

  a. select **cn=Alice Baker,ou=users,dc=example,dc=com**

  b. click **<<< Remove selected**

  c. click **Save changes**

  d. click **Update object**

After we have made some changes in AD outside midPoint, we will run reconciliation with AD - first in simulation mode.

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** task using click **Run now** and wait for the task completion (task status: closed)
5. click **Show simulation result**
6. the Simulation results show:

  a. 1 object `afreeman` to be updated in midPoint:

    i. link to newly created AD account is to be added

  b. 1 object `cn=Alexander Freeman,ou=users,dc=example,dc=com` to be activated (created) in AD:

    i. all attributes are populated by AD outbound mappings

    ii. account will be added to `cn=all-users,ou=groups,dc=example,dc=com` group (because of policy in `Person` archetype)

  c. 1 object: `cn=Alice Baker,ou=users,dc=example,dc=com` to be updated in AD with the following details:

    i. `Locality` attribute will be changed to `White Stone City` (because of data in HR)

    ii. `Given Name` attribute will be changed to `Alice` (because of data in HR)

    iii. account will be added to `cn=all-users,ou=groups,dc=example,dc=com` group (because of

policy in `Person` archetype)

If the reconciliation with AD would be scheduled, it would automatically do the changes presented in the simulation.

We will run the reconciliation manually:

1. get back to **Defined Tasks**
2. edit and run **Reconciliation with AD (real)** task again using **Run now** and wait for the task completion (task status: closed)
3. go to **Audit log viewer** and verify the executed changes there (1 account should be created and 1 account should be modified)
4. go to **Users › Persons**
5. edit **abaker** user
6. click **Projections** menu item
7. edit **AD** account
8. verify the `Locality` and `Given Name` attributes and `AD Group Membership` association have been updated to the same values as in simulation
9. click **Back**
10. edit **afreeman** user
11. click **Projections** menu item
12. edit **AD** account
13. verify the account has been created and its attributes populated

> List of projections also shows a message about *dead shadow(s)* for user `afreeman`. Dead shadows contain metadata about the (now deleted) accounts midPoint is aware of. They will be automatically removed by midPoint's `Shadow Refresh Task` (default retention policy for dead shadows is: 7 days).

(Optional) In your browser with AD LDAP browser:

1. expand **dc=example,dc=com**
2. expand **ou=users**
3. edit **cn=Alice Baker**
4. verify the attribute values in the account
5. verify that **cn=Alexander Freeman** account exists (has been re-created)

Now we will resume our scheduled HR reconciliation task.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

In your browser with midPoint:

1. go to **Resources › All resources**
2. edit **HR** resource
3. click **Defined Tasks** menu item
4. edit task **HR Reconciliation**
5. click **Resume** to resume the task. The task will be executed immediately.

As a matter of fact, the scheduled reconciliation with HR helps us to maintain the attribute consistency even without running scheduled AD reconciliation. HR reconciliation task evaluates all HR accounts and their owners in midPoint and their AD accounts. As we are using `strong` mappings everywhere, any inconsistency in attributes is automatically fixed by the HR reconciliation task. Please note that HR reconciliation task *cannot* detect any orphaned accounts (without midPoint owner) in AD!

In real deployments, the reconciliation with AD should be scheduled to be executed automatically to detect any inconsistencies.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

LAB 8-5: Handling HR Data Updates

Estimated Time: TODO

In this lab, we will verify that we can actually change data in HR application and that they will be picked up midPoint. We have already created new users, now let's check updates.

In your browser with HR application:

1. click **Show users**
2. edit **Geena Green (employee number: 1001)** entry using **Modify**
3. update the following fields:
   a. **Locality**: `Hot Lava City`
4. click **Modify user**
5. click **Export users to csv file**

In your browser with midPoint:

1. wait for the next scheduled reconciliation with HR
2. edit user **geena**
3. check that user's **Locality** has been updated to: `Hot Lava City`
4. click **Projections** menu item
5. edit **AD** account
6. check that `locality` attribute has been updated to `Hot Lava City`

You can also check user-related audit log entries.

1. while editing **geena** user
2. click **History** menu item
3. click the first entry's **Time** value
4. midPoint audit log shows that both midPoint user and her AD account `cn=Geena Green,ou=users,dc=example,dc=com` were updated:

Item	Old value	New value
Locality	Small Red Rock City	Hot Lava City

We have seen that midPoint is correctly picking up updates of existing HR data just like the new entries.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

LAB 8-6: Handling Long-term Leave

Estimated Time: TODO

In this lab, we will test midPoint behaviour for HR long-term leaves.

In this training, long-term leave stands also for parental leave etc. Such users and their accounts should be disabled.

In your browser with HR application:

1. edit user **Martin Knight (employee number: 1006)** by clicking **Modify**
2. change the following attribute:
   a. **Status**: select `Long-term leave`
3. click **Modify user**
4. click **Export users to csv file**

Wait for the next scheduled reconciliation with HR.

In your browser with midPoint:

1. go to **Users › Persons**
2. search for and edit user **knight**
3. check the following:
   a. User's **Lifecycle state** is `Suspended`
   b. User's effective status (displayed in the summary panel) is `Disabled`
4. click **Projections**
5. edit **AD** account
6. scroll down to verify that **Administrative status** is `Disabled`

Inactive users from HR are inactive in midPoint and AD resource.

We will return the employee back to the active state now.

In your browser with HR application:

1. edit user **Martin Knight (employee number: 1006)** by clicking **Modify**
2. change the following attribute:
   a. **Status**: select `In`
3. click **Modify user**

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

4. click **Export users to csv file**

Wait for the next scheduled reconciliation with HR.

In your browser with midPoint:

1. go to **Users › Persons**
2. search for and edit user **knight**
3. check the following:
   a. User's **Lifecycle state** is `Active`
   b. User's effective status (displayed in the summary panel) is `Enabled`
4. click **Projections**
5. edit **AD** account
6. scroll down to verify that **Administrative status** is `Enabled`

When returning from long-term leave, user and his/her accounts in target systems are enabled.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

LAB 8-7: Handling Leavers

Estimated Time: TODO

In this lab, we will test midPoint behaviour for former employees. Such users and their accounts should be disabled and their accounts should be deleted in the future automatically. We will use "disabled instead of delete" and "delayed delete" activation concepts of midPoint to first disable such users and their AD account and plan a delayed delete for their AD accounts.

> The delayed delete interval is set for 5 minutes for this training.

In your browser with HR application:

1. edit user **Martin Knight (employee number: 1006)** by clicking **Modify**
2. change the following attribute:
   a. **Status**: select `Former employee`
3. click **Modify user**
4. click **Export users to csv file**

Wait for the next scheduled reconciliation with HR.

In your browser with midPoint:

1. go to **Users › Persons**
2. search for and edit user **knight**
3. check the following:
   a. User's **Lifecycle state** is `Archived`
   b. User's effective status (displayed in the summary panel) is `Disabled`
4. click to **Projections**
5. click **AD** account
   a. User's AD account is disabled
   b. Trigger is set for user's AD account to be applied in 5 minutes from now (time of account disable when user entered `Archived` lifecycle state).
   c. The trigger time is displayed when you hover the mouse pointer over the AD account icon
   d. This trigger will be used to delete the AD account.

> The trigger is stored in midPoint Shadow object corresponding to the resource account. It is not stored in the user object nor in the real account in AD.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

You can check accounts with triggers in **AD account notices** dashboard:

1. go to **Dashboards › AD account notices**
2. dashboard indicates how many accounts are using the account marks
3. click **More info** in **Users with accounts with triggers** tile to display the list of users with triggers for any of their account
4. click **More info** in **Accounts with triggers** tile to display just list of accounts with triggers
   a. all accounts with triggers on any resource are displayed (in our particular case, we can have triggers only for accounts in AD resource)

Wait 5 minutes.

After 5 minutes have elapsed, wait for the next scheduled execution of `Trigger Scanner` task.

In our particular case, the HR reconciliation task may process the triggers earlier as it runs each minute. If our HR reconciliation task was running in longer intervals, you could either wait for the `Trigger Scanner` task or run it manually:

1. go **Server tasks › System tasks**
2. click **Trigger Scanner** task.
3. this task is automatically scheduled each 5 minutes. Information about last task run is either in task's summary panel or visible in **Operational attributes**
4. to force running the task immediately, click **Run now** and wait for the task completion (task status: closed). Please note that `Trigger Scanner` will act only on objects that have their triggers in the past.

In our particular case, HR reconciliation will process the trigger earlier than `Trigger Scanner` task.

After 5 minutes have elapsed and either `Trigger scanner` or `HR Reconciliation` task has run, check the user again:

1. go to **Users › Persons**
2. click **knight** user
3. click **Projections**
4. user's AD account should be deleted

You can also check the **Users without account** search criteria:

1. go to **Users › Persons**
2. in search toolbar, locate **Users without account** search criteria

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

   a. click ⚙ button (tooltip: **Property settings**) to open a popup window:
      i. in **Name**: click the button and select **AD** resource
   b. check the ☐ for **Users without account** to apply the search criteria
3. user `knight` should be in the list as midPoint has deleted his AD account

To stop using the search criteria, uncheck the checkbox for **Users without account** in search toolbar.

Of course, you can also check users without AD accounts in **AD account notices** dashboard:

1. go to **Dashboards › AD account notices**
2. dashboard indicates how many users are without AD accounts
3. click **More info** in **Users without AD accounts** tile
   a. all users without AD accounts displayed

midPoint has automatically deleted AD account for former employee with a delay. This would allow administrators to transfer some important data (e.g. mailbox) before the account is deleted. It will also prevent an immediate account deletion in case the data in HR is incorrect.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

LAB 8-8: Adding A New Outbound Mapping TODO BONUS?

Estimated Time: TODO

In this lab, we will demonstrate how an AD outbound mapping can be added to already existing configuration. We will still need and use simulations.

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. click **Outbound mappings (to Resource)**
   b. use **Add outbound** button to create a new mapping:

Name	Source	Expression	To resource attribute	Lifecycle State
mapping-initials	givenName familyName (You need two source attributes here)	Script	initials	Proposed

   c. click **Show script** for the `initials` attribute mapping
      i. paste the following code:

```
basic.uc(                                          ❶
    basic.stringify(givenName)?.take(1) +          ❷
    basic.stringify(familyName)?.take(1)           ❸
)
```

❶ uppercase the concatenation of…

❷ first letter of user's `givenName` property converted to String

❸ first letter of user's `familyName` property converted to String

      ii. click **Done**

5. click **Save mappings**

Now we are ready to run the simulated reconciliation.

1. click **Defined Tasks** menu item
2. edit **Reconciliation with AD - development simulation** task
3. click **Run now** and wait for the task completion (task status: closed)

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

4. click **Show simulation result**
5. the Simulation results show:
   a. there will be resource objects affected (click **More info** in **Resource objects affected** tile to see details) - AD attribute `initials` is being populated

We will switch the new simulated mapping to `Active` lifecycle state.

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. click **Outbound mappings (to Resource)**
   b. edit the mapping `mapping-initials` and set:
      i. **Lifecycle state**: `Active (production)`
5. click **Save mappings**

Wait for the next scheduled run of reconciliation with HR. Then you can verify the mapping has been applied.

1. go to menu Users[Persons]
2. edit user **geena**
3. click **Projections** menu item
4. click user's **AD** account
5. the `initials` attribute should contain the following value: `GG` (**G**eena **G**reen)

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

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

In your browser with AD LDAP browser:

1. expand **dc=example,dc=com**
2. expand **ou=users**
3. click any account and verify the `initials` attribute is populated

We have successfully created a new outbound mapping for AD resource. Simulations were again helpful - even if the solution is actually deployed.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

LAB 8-9: Adding New Attribute Provisioning From HR to AD TODO BONUS?

Estimated Time: TODO

In this lab, we will import another attribute from HR for users and let it provision to AD resource. We will need two mappings: one inbound mapping to get HR data to midPoint and one outbound mapping to populate AD resource account.

In your browser with **HR application**:

1. click **Show users**
2. notice how `Job` attribute is displayed. The value contains job code and job title concatenated with `#`. We will start with importing the value as it is and improve it later.

We will add the inbound mapping first.

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. use **Add inbound** button to create an additional mapping:

Name	From resource attribute	Expression	Target	Lifecycle State
job-to-title	job	As is	title	Proposed

5. click **Save mappings**

We would add a new outbound mapping for AD now, but we will realize a suitable mapping from midPoint `title` property to AD's `title` attribute is already present in AD resource in `Draft` lifecycle state (because it was copied from the resource template).

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. click **Outbound mappings (to Resource)**

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

   b. edit `mapping-title` mapping and set:
      i. **Lifecycle state**: `Proposed (simulation)`
5. click **Save mappings**

Both mappings are in `Proposed` lifecycle state, so they will not influence the scheduled reconciliation task.

Now we are ready to run the simulated import from HR resource.

1. go to **Resources › All resources**
2. edit **HR** resource
3. click **Defined Tasks** menu item
4. edit **Import from HR - development simulation** task
5. click **Run now** and wait for the task completion (task status: closed)

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

6. click **Show simulation result**
7. the Simulation results show:
   a. there will be resource objects affected (click **More info** in **Resource objects affected** tile to see details) - AD attribute `title` is being populated
   b. the list of modified objects also includes Users objects in midPoint (**Title** property is being populated). Click **View processed objects** to see also the users.
   c. some AD accounts already contain values for `title` and will be overwritten:
      i. `cn=Brad Carpenter,ou=users,dc=example,dc=com`
      ii. `cn=Jimmy Taylor,ou=users,dc=example,dc=com`
      iii. `cn=Peter Hunter,ou=users,dc=example,dc=com`
      iv. `cn=Diane Davis,ou=users,dc=example,dc=com`
      v. `cn=Patrick Anderson,ou=users,dc=example,dc=com`
   d. for other AD accounts we are simply adding a new `title`

We will switch the new simulated mappings to `Active` lifecycle states.

In your browser with midPoint:

1. go to **Resources › All resources**
2. edit **HR** resource

3. click **Configure**, then click **Mappings** item in the context menu
4. edit the mapping `job-to-title` and set:
   i. **Lifecycle state**: `Active (production)`
5. click **Save mappings**

Then navigate to AD resource.

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. click **Outbound mappings (to Resource)**
   b. edit the mapping `mapping-title` and set:
      i. **Lifecycle state**: `Active (production)`
5. click **Save mappings**

Wait for the next scheduled run of reconciliation with HR. Then you can verify the mapping has been applied.

1. go to **Users › Persons**
2. edit user **geena**
   a. notice the property **Title** and its value
3. click **Projections** menu item
4. click user's **AD** account
   a. notice the `title` attribute should contain the same value as in HR application and midPoint user

In your browser with AD LDAP browser:

1. expand **dc=example,dc=com**
2. expand **ou=users**
3. click any account and verify the `title` attribute is populated

We have populated yet another value from HR to AD through midPoint. The values do not look very nice as they contain some internal HR codes, but we will improve that in the following lab - we will show how to safely exchange mappings in production.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

LAB 8-10: Exchanging Inbound Mapping TODO BONUS?

Estimated Time: TODO

In this lab, we will demonstrate how mapping can be safely exchanged for another one. As our system is already in production, we need to be extra safe. We need to use simulations, just like before.

In the previous lab, we have seen that the `job` attribute in HR application actually contains a code, which is something we want to avoid. We want to show `CEO` instead of `124#CEO`. For the sake of the previous lab, it was OK, but now we need to do better.

We will parse the `job` attribute during import and store only the value after `#` separator using a simple Groovy script.

For the first time, we will use lifecycle state to deprecate the existing mapping to allow it still to be evaluated during scheduled HR reconciliation, while we will prepare a new proposed mapping for simulations. Then we will switch these two mappings.

In your browser with midPoint:

1. go to **Resources › All resources**
2. edit **HR** resource
3. click **Configure**, then click **Mappings** item in the context menu
4. edit the mapping `job-to-title` and set:
   i. **Lifecycle state**: `Deprecated`
5. use **Add inbound** button to create a new mapping for `job` attribute:

Name	From resource attribute	Expression	Target	Lifecycle State
job-to-title-nice	job	Script	title	Proposed

   a. click **Show script** for the `job-to-title-nice` attribute mapping
      i. paste the following code:

```
def separator = '#'

if (input == null || input.indexOf(separator) == -1) {
    return input
} else {
    return input.tokenize(separator)[1]
}
```

ii. click **Done**

6. click **Save mappings**

> The script parses the value using '#' character and returns the second item. For `123#CEO` it returns `CEO`. To be on the safe side, we will take care of anomalies too:
>
> - `CEO`: returns `CEO`
> - empty string: returns empty string
> - null: returns null

The new mapping is in `Proposed` lifecycle state, so it will not be used by the scheduled HR reconciliation. We can simulate the configuration change safely.

> We won't make any change to AD's outbound mapping for `title` attribute. That one will use the midPoint property value once we correct it in midPoint.

We will run the simulated import from HR resource.

1. go to **Resources › All resources**
2. edit **HR** resource
3. click **Defined Tasks** menu item
4. edit **Import from HR - development simulation** task
5. click **Run now** and wait for the task completion (task status: closed)

> **Simulated development** mode will evaluate all `Active` and `Proposed` configuration items, but there will be no permanent effects on data; we are only simulating. At the same time, the real scheduled reconciliation task executed all `Active` and `Deprecated` configuration items, so the old configuration is still in production.

6. click **Show simulation result**

7. the Simulation results show:
   a. there will be resource objects affected (click **More info** in **Resource objects affected** tile to see details) - AD attribute `title` is being updated
   b. the list of modified objects also includes Users objects in midPoint (**Title** property is being updated). Click **View processed objects** to see also the users.

> You can improve your script expression and run simulated import without worries and any impact on real users and their AD accounts while the mapping is in `Proposed` lifecycle state.

We have seen what will happen. We will now switch the mappings.

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
5. edit the mapping `job-to-title` and set:
   a. **Lifecycle state**: `Archived`
6. edit the mapping `job-to-title-nice` and set:
   a. **Lifecycle state**: `Active (production)`
7. click **Save mappings**

Wait for the next scheduled run of reconciliation with HR. Then you can verify the mapping has been applied.

1. go to menu Users[Persons]
2. edit user **geena**
   a. notice the property **Title** and its value: it should be updated to the new format
3. click **Projections** menu item
4. click user's **AD** account
   a. notice the `title` attribute should contain the same value as in HR application and midPoint user

In your browser with AD LDAP browser:

1. expand **dc=example,dc=com**
2. expand **ou=users**

3. click any account and verify the `title` attribute is updated correctly

We have succeeded in exchanging mappings using lifecycle state and simulations during real operation (scheduled reconciliation with HR was not suspended in the process). This way you could improve your configuration and still see what would happen thanks to the simulations.

The mapping in `Archived` lifecycle state can be eventually removed.

This concludes the Module 8 labs.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

Module 9: Overriding Incorrect Data

LAB 9-1: Overriding Malicious User Status

Estimated Time: TODO

In this lab, we will show how midPoint can be used to disable user/account even if data in HR system is incorrect.

Imagine the following situation: some malicious user must be deactivated immediately. We cannot wait until the user is properly deactivated using HR `status` attribute, we must act *now*

Let's create the user first.

In your browser with HR application:

1. click **Register user** and fill in the following attributes:
   a. **First name**: `John`
   b. **Surname**: `Newman`
   c. **Employee number**: `9005`
   d. **Locality**: `Fast River City`
   e. **Job**: `107#Junior Consultant`
   f. **EmpType**: select/keep `FTE`
   g. **Status**: select/keep `In`
   h. click **Register user**
2. click **Export users to csv file**

In your browser with midPoint:

1. wait for the next regular reconciliation with HR resource
2. go to **Users › Persons**
3. check that user `jnewman` has been created in midPoint and has Active Directory resource account

Now we will override user's status in midPoint because we have realized the user must be immediately deactivated.

In your browser with midPoint:

1. go **Users › Persons**

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

2. edit user **jnewman**
3. in user's summary panel, badge **Enabled** signalizes user's effective status, also `Lifecycle state` is: `Active`
4. click **Activation** menu item
5. click **Show empty fields** if **Administrative status** is not displayed
6. set the following properties:
   a. **Administrative status**: `Disabled`
7. click **Save**
8. edit user **jnewman** again
9. in user's summary panel, badge **Disabled** signalizes user's effective status (even if user's `Lifecycle state` is still `Active`)
10. click **Projections** menu item
11. click **AD** resource account
12. scroll down to **Activation** container
13. you should see the following:
    a. **Administrative status**: `Disabled`

Malicious user and his accounts are disabled and will be kept disabled regardless of state information coming from HR resource. Reconciliation execution will not change it. midPoint has overridden the HR data for user's status.

If the user is cleared from suspicion, administrator may reset the Administrative status to **Undefined** value again, allowing HR data to be used.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

LAB 9-2: Overriding Incorrect HR Data

Estimated Time: TODO

In this lab, we will show how midPoint can be used to enable user/account or override incorrect attribute values provided by HR data.

Imagine the following situation: user has been created in HR with some errors, e.g. incorrect locality and even status. We cannot wait until the user is fixed in HR, because this is some VIP user who needs to work, but his account is kept inactive because of those errors.

Let's create the user first.

In your browser with HR application:

1. click **Register user** and fill in the following attributes:
   a. **First name**: `John`
   b. **Surname**: `Doe`
   c. **Employee number**: `9006`
   d. **Locality**: `Fat Rover City`
   e. **Job**: `999#CXO`
   f. **EmpType**: select/keep `FTE`
   g. **Status**: select `Long-term leave`
   h. click **Register user**
2. click **Export users to csv file**

In your browser with midPoint:

1. wait for the next regular reconciliation with HR resource
2. go to **Users › Persons**
3. edit user **jdoe**
   a. check user's **Lifecycle state**: it's `Suspended`
   b. check user's **Locality**: it contains incorrect locality `Fat Rover City` instead of `Fast River City`
   c. check the user has **AD** account disabled

Change of Administrative status won't work in this case; the current implementation allows Administrative status to override Lifecycle status only to deactivate the user. Any attempt to blindly fix `Locality` or `Lifecycle state` would not work: the user is synchronized from HR by scheduled reconciliation; we must create an exception.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

1. go to **Resources › All resources**
2. edit **HR** resource
3. click **Accounts** menu item
4. search for account `9006`
5. click the context menu for the account and click **Add marks**
6. check **Invalid data** mark
7. click **Add**

`Invalid data` mark causes the HR account data to be ignored for account's owner during synchronization. We can override user data now.

1. while displaying content of **Accounts** menu item
2. click the **jdoe** in **Owner** column to edit the user
   a. edit the following properties:
      i. **Locality**: set `Fast River City`
      ii. **Lifecycle state**: select `Active`
   b. click **Save**

User and his AD account are now enabled.

Wait for the next scheduled reconciliation with HR to see that midPoint overrides have not been reverted. You can even test that any updates of HR data for `9006` are ignored.

In your browser with HR application:

1. click **Show users**
2. edit **John Doe** entry using **Modify**
3. update the following fields:
   a. **Locality**: `Fast River Chaty`
4. click **Modify user**
5. click **Export users to csv file**

In your browser with midPoint:

1. wait for the next scheduled reconciliation with HR
2. edit user **jdoe** again
3. check that users **Locality** is still set to: `Fast River City`

Before we correct HR data, let's see how midPoint dashboard can help us to see which account

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

marks are in use.

In your browser with midPoint:

1. go to **Dashboards › Account marks**
2. dashboard indicates how many accounts are using the account marks
3. click **More info** in **Invalid data accounts** tile
   a. all accounts marked as `Invalid data` on any resource are displayed, in our particular case: account `9006` on HR resource
4. go to **Dashboards › Account marks**
5. click **More info** in **Protected accounts** tile
   a. all accounts marked as `Protected` on any resource are displayed
6. go to **Dashboards › Account marks**
7. click **More info** in **All marked accounts** tile
   a. all accounts marked with any mark on any resource are displayed

If you prefer a report, that can be used too.

In your browser with midPoint:

1. go to **Reports › Dashboard reports**
2. click ▶ icon to run **Account Marks Dashboard Report**
3. click **show task** link displayed at the top of the page
4. wait until the task completes
5. click **Download report** to save the report as HTML file
6. open the downloaded HTML file in browser to display the report

To access the report outputs later:

1. go to **Reports › Created reports**
2. download desired report

Let's correct HR data now and set a different locality.

In your browser with HR application:

1. click **Show users**
2. edit **John Doe** entry using **Modify**
3. update the following fields:

   a. **Locality**: `White Stone City`
   b. **Status**: `In`
4. click **Modify user**
5. click **Export users to csv file**

The HR data will be ignored until we remove account's `Invalid data` mark.

In your browser with midPoint:

1. go to **Resources › All resources**
2. edit **HR** resource
3. click **Accounts** menu item
4. search for account `9006`
5. click the context menu for the account and click **Remove marks**
6. check **Invalid data** mark
7. click **Remove Marks**

Wait for the next scheduled reconciliation with HR.

1. while displaying content of **Accounts** menu item
2. click the **jdoe** in **Owner** column to edit the user
   a. check the following properties:
      i. **Locality**: `White Stone City`
      ii. **Lifecycle state**: `Active`

Synchronization works again for this user.

We have seen that not just user's status but also other user properties may be overridden by administrator if needed. In addition, we have tried how account marks can be reported using midPoint's dashboard and reports.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

LAB 9-3: Overriding Username

Estimated Time: TODO

In this lab, we will try to override username in case the generated one is not *appropriate*.

There are situations when the generated username is or resembles an insulting or offensive word. Fortunately, even in these situations, midPoint can help.

Let's create the user first.

In your browser with HR application:

1. click **Register user** and fill in the following attributes:
   a. **First name**: `Brenda`
   b. **Surname**: `Itchy`
   c. **Employee number**: `9007`
   d. **Locality**: `Fast River City`
   e. **Job**: `191#Accountant`
   f. **EmpType**: select/keep `FTE`
   g. **Status**: select/keep `In`
   h. click **Register user**
2. click **Export users to csv file**

In your browser with midPoint:

1. wait for the next regular reconciliation with HR resource
2. go to **Users › Persons**

Based on our naming convention, the username generator generated the following username: `bitchy`. For obvious reasons, user could complain about such username.

Fortunately, there is an easy way how to override midPoint username.

In your browser with midPoint:

1. go to **Users › Persons**
2. edit user **bitchy**
3. replace the following properties:
   a. **Name**: `britchy`

4. click **Preview changes** to display what will be saved to midPoint and target system account(s)
   a. midPoint is previewing the username change in midPoint and all target system accounts (in our case, only AD)
   b. change of **Login name** in Active Directory is indicated

> Preview changes is a simple functionality of doing simulation without talking about execution mode and configuration to use. It will simply preview what would be done and allow to save or cancel the operation.

5. click **Save**

As midPoint uses the username generator only *once* because of weak mapping in `Person Object Template`, overriding the username won't conflict with the mapping. Just be careful to not select any username that already exists; in such situation midPoint would show an error message during Preview changes and/or saving the user.

For example if you would try to change the username of `Brenda Itchy` to `cwhitehe`, an error similar to the following would be displayed:

```
Too many iterations (100) for focus(user:ac6cab9f-519c-4ea2-8354-fa84664a70f8(cwhitehe)): cannot determine values that satisfy constraints: Found conflicting existing object with property name = PP({.../common/common-3}name):[PPV(PolyString:cwhitehe)]: user:3fd75c16-8697-4049-aa9c-bbfcd4ea8c2e(cwhitehe)
```

Username is never automatically changed if user's Given name or Family name change.

This concludes the Module 9 labs.

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

Appendix A: Environment Cheat Sheet

The following table summarizes the list of connections used during the training.

Application	URL	Username	Password
Portal	http://AWS_workstation_IP	(no login)	(no password)
midPoint GUI	http://AWS_workstation_IP/midpoint	`administrator`	`1st3ps`
HR application	http://AWS_workstation_IP/hr	(no login)	Proxy password: `e=mc2`
AD LDAP browser	http://AWS_workstation_IP/phpldapadmin	(no login)	Proxy password: `e=mc2`

© 2023 Evolveum, s.r.o., Unauthorized use prohibited

Appendix B: Environment Reset

This appendix is applicable only for training courses where command shell is provided.

To **completely reset** the training environment and start from scratch, please execute the following commands:

```
cd DIRECTORY_WITH_TRAINING
docker compose down -v
docker compose up -d
```

All containers will be created from scratch (images won't be re-downloaded nor rebuilt).

© 2023 Evolveum, s.r.o., Unauthorized use prohibited