Introduction

- How Does It Work?
- What Makes MidPoint Unique?
- Technology
- Quick Start
- See Also
- External links

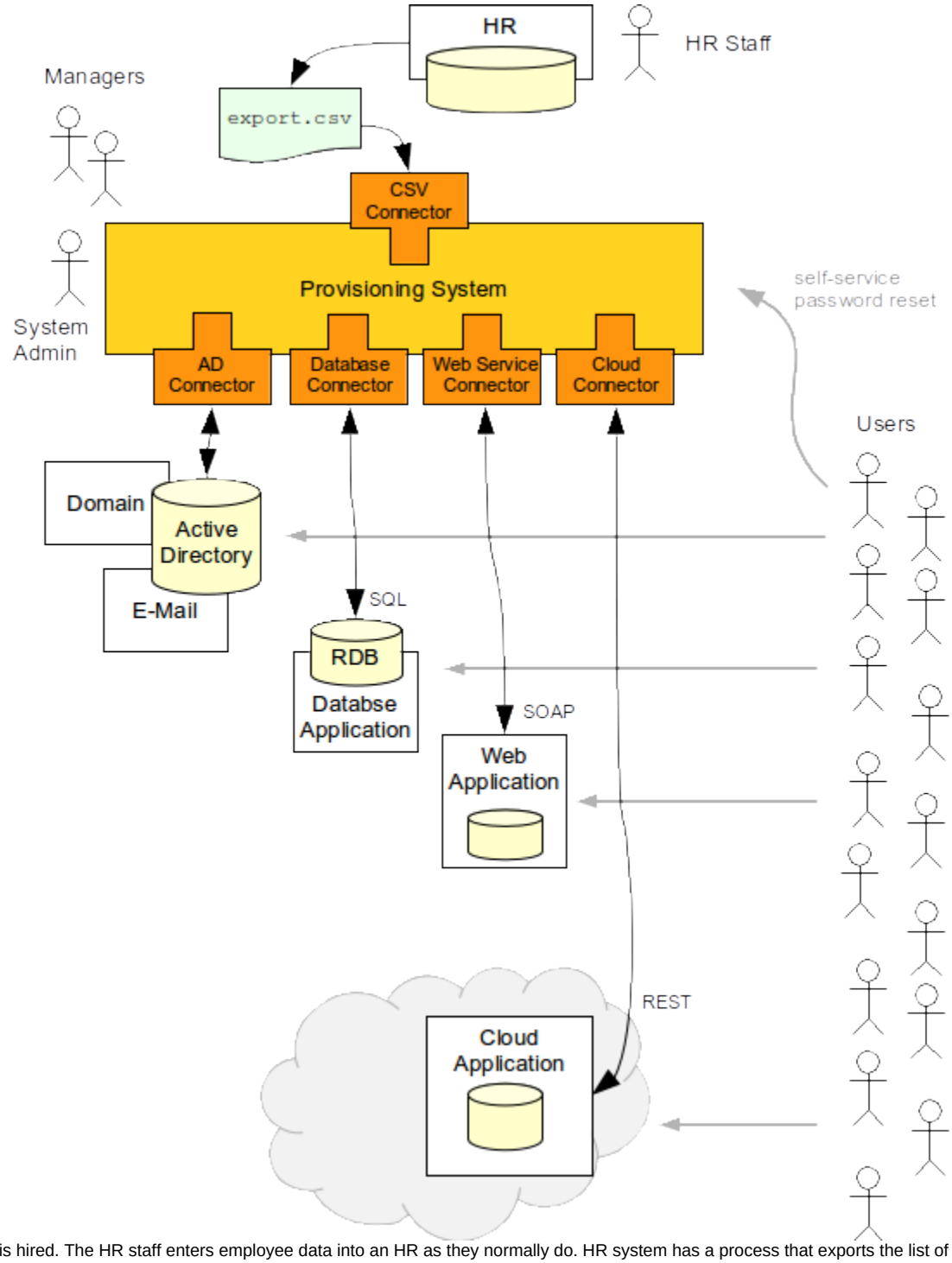
midPoint is an identity management and governance system. It is a comprehensive system that synchronizes several identity repositories and databases, manages them, makes them available in a unified form, manage roles, authorizations, entitlements and implements almost every aspect of identity management and governance. It belongs to the "management" part of Identity and Access Management (IAM) field.

The most important features of midPoint are:

- User **provisioning and deprovisioning**: midPoint can automatically create and manage user accounts, groups, organizational units and so on.
- Identity **synchronization and reconciliation**: midPoint can seamlessly synchronize several databases. It can make sure that the identity data are always up to date.
- Identity management **process automation**: midPoint has a built-in engine that can drive approval of access requests.
- **Role-based access control (RBAC)**: midPoint can automatically compute user privileges based on his membership in roles. MidPoint RBAC model is one of the most powerful models in the entire IDM field.
- Management of identity-related parts of the **enterprise security policy**: midPoint can check password quality, maintain segregation of duties, and so on
- Support for security **auditing and reporting**: midPoint keeps an audit trail of all changes to user privileges. It has a built-in reporting engine to generate reports for identities collected from all the connected systems.
- Non-intrusive integration using **identity connectors**: midPoint connectors are simple pieces of code that allows it to remotely connect to other system and manage identity data. The connectors are non-intrusive: the connected system does not need to be changed.
- Management of **organizational structure** and its synchronization to other systems.
- **Identity governance**: Management of complex policies that govern business aspect of identity management.

How Does It Work?

MidPoint is something like a sophisticated robot for identity data synchronization and maintenance. MidPoint continually watches the information sources such as HR system. If something changes in the information source the provisioning system pulls the new information, recomputes it, applies policies and then pushes that information to other systems. Let's explain that using an example:



New employee is hired. The HR staff enters employee data into an HR as they normally do. HR system has a process that exports the list of all the employees to a text file every day. MidPoint is using a connector to continually monitor the file for changes. Therefore it finds a new line describing the new employee and reads the data from the file. MidPoint can be configured with a set of rules and scripts that is used to process the data. E.g. the rules may take the field "organization unit" from the HR record and used that to determine which organizational unit the user belongs to and which business roles should this user have. This logic is different in each organization and midPoint is built to be easily customizable.

Once midPoint determines what the new user is and what roles he should have then the really interesting bit starts. MidPoint will compute what accounts the user should have. This is usually computed from the roles that the user has. Account attributes and entitlements are computed as well, e.g. the list of groups that user should belong to. Once midPoint knows how the accounts should look like it can use connectors to automatically create them. Connectors are simple pieces of code that communicate to the target systems. The connector knows how to read, create, modify and delete an account. Therefore midPoint can automatically create all the accounts that a user needs. Automatically. In a couple of seconds.

The connectors usually communicate using a protocol that is native to the target system. Therefore connectors talk to Active Directory using LDAP interface, they modify the database using SQL or provision to the cloud service by using RESTful services. This means that midPoint is *non-intrusive*: the target applications do **not** need to be modified. They stay exactly as they are. This is crucial feature that makes midPoint such efficient and practical tools. It is much easier to adapt a couple of simple connectors than to modify dozens of information systems (especially if too many of them still remember 20th century).

What Makes MidPoint Unique?

There is a long list of features that make midPoint really a unique system. But there are basically three aspects that are the most interesting:

- **MidPoint saves money**. Identity provisioning systems had a reputation of being extremely expensive to deploy and maintain. But midPoint has changed that completely. MidPoint is design to be cost-efficient. The open-source character means that the licensing cost is zero. The support cost is reduced by a network of excellent technology partners. But the most significant **saving is in the deployment cost**. MidPoint is built on more than a decade on IDM experience. It is built by people who *deployed* IDM solutions. We know very well what an IDM engineers needs "in the field". Therefore we have implemented that directly in midPoint code. It can be expected that 80% of the things that your IDM solution needs can be implemented in midPoint by simply flipping a configuration switch. MidPoint can make a huge effect with a very little implementation effort.
- MidPoint **goes beyond user management**. MidPoint is real **identity management**. Of course it can manage users and accounts. But it can also manage groups, organizational units, services, devices or any other concept that can be technically reached by the connector. MidPoint can bind all these concepts to the identities therefore it can easily manage user membership in organizational units or groups. It can also manage organizational subscription to services or device ownership. And all of that is done by simply reusing the principles of identity management and applying them to much broader category of objects.
- MidPoint is an **identity governance** system. MidPoint does not just deal with provisioning and synchronization of identity data. MidPoint applies policies to those data. MidPoint can enforce segregation of duties policy. It can support object lifecycle policies. MidPoint can govern organizational structure. Those are business aspects of identity management. And midPoint is one of the very rare breed of system that implements both identity management and identity governance in a **single integrated product**.
- MidPoint is **open source**. Yes, this means that the licensing cost is zero. But there is much more in this. It also means that midPoint **code can be modified**. Other vendors will void your support agreement if you modify product code. But we in fact encourage partners to modify midPoint code. This is the best way to make really extreme customizations. But it is also a way how to bring new ideas into midPoint. How to allow partners to participate on product development. How to maintain a very creative community. This allows midPoint to be great and to remain great.

Technology

midPoint is essentially a **Java** application. Its internal structure is "wired" together using a **Spring** framework. It is quite strictly divided into internal components separated by interfaces, which provides fair assurance of reusability and maintainability. The structure itself is lightweight. Heavyweight components such as Java Enterprise Java Beans (EJB) or Enterprise Service Bus (ESB) are **not** used (although integration with them is possible).

The system can adapt to **several data store mechanisms**. The only supported mechanism is relational database (supporting all major databases), however there was an experimental implementation of repository using a noSQL database as a proof of concept. Therefore we are confident that other storage schemes could be implemented in the future as long as the underlying data store is powerful enough to support midPoint data model.

The system is using an ConnId framework as a mechanism to interact with other systems (resources). ConnId is also used by other identity management systems and we are working closely with other vendors to maintain and develop ConnId framework.

The unique feature of midPoint is the method of dealing with data changes and consistency. Most identity management systems work with absolute state, e.g. the complete copy of new user or account data. Such approach is very problematic in case of concurrent changes that are much more common in the IDM field as one would expect. The midPoint solution is to use model based on relative changes instead of on absolute changes. Several concurrent changes can be executed in parallel without the need to lock the entire data record. This approach significantly improves usability of the system and also supports better data consistency.

See Also: Architecture and Design, Unique Features

Quick Start

If you are new to midPoint, there are two "tracks" to start exploring it:

- **MidPoint Book** is an excellent starting point for any midPoint-related activity.
- Features section will provide a detailed explanation of midPoint functionality.
- Architecture and Design will provide theoretical overview of what midPoint is and how it works.
- First Steps provides a guidance how to quickly install midPoint and configure it.
- Documentation section provides a lot of in-depth information about system configuration, customization and maintenance.

See Also

- Enterprise Identity Management
- Features
- Architecture and Design
- midPoint History
- Documentation

External links

- What is midPoint Open Source Identity & Access Management
- Evolveum - Team of IAM professionals who developed midPoint