IDENTITY MANAGEMENT
AS NOWADAYS' NECESSITY

Evolveum®

January 2017
White Paper

Contents

Introduction: The rising need for Identity Management

This century is a century of information and information technologies, therefore if companies want to keep up with the progress and their competitors, they need to simplify the internal processes to make them as effective as possible. Especially when a company grows and divides into departments among which the cooperation can get stuck easily, time is of the essence.

When dealing with fluctuation of employees, a company cannot afford to underestimate the importance of security. Also in connection with customers or business partners, a company can easily notice the need for safety and protection of information.

To be effective means to shorten the time of specific actions and automate them as much as possible. Manual processes of identity management from granting access to managing users' accounts can become very challenging or nearly impossible with big number of users. Automated solutions therefore save a lot of time. That's where a self-service solution becomes very useful. Making decisions about authentication to allow specific users to access particular systems via password or deciding about authorisation to which sources users can access can go from being a chaotic, time-consuming activity to a very clear and effective one.

By minimizing the threat of information theft and maximizing the smoothness of Identity Management (IDM) processes, a company can keep or even raise its competitiveness and flexibility by not losing time and resources for processes that can be handle perfectly by technology.

Identity Governance and Administration in all stages of the user's lifecycle

By enabling a company to define, enforce, review and audit Identity and Access Management (IAM) policy, as well as to map IAM functions to comply with requirements, a significant amount of control over security is gained. Any organization, regardless of its size, will need a practical solution that can provide that through the full user lifecycle, from onboarding new users to their offboard and the elimination of their accounts.

When new employees are hired, they need to get their roles and accesses assigned as soon as possible so there is no time wasted and they can proceed to work immediately. Also when their positions are changed or some employees are added to a working group, a reorganization of accesses or passwords needs to be fast. From the IGA point of view, it is also inevitable that regular access reviews and audits will be done. If employees are leaving a company it is necessary to disallow their accounts and access privileges as soon as possible to avoid any potential security exposures.

A company may also need to grant access to customers, business partners or suppliers and provide secure access to externally hosted applications such as cloud-based applications. Offboarding partners is also a common thing in business which can become complicated. In connection with that, there is a need for the coordination of authentication and authorization with the company’s back-end or third-party systems.

For all these actions, an Identity Governance and Administration tool as a part of IAM solution can satisfy all company's needs. It can help with reducing the risk of fraud, theft of intellectual property or data loss. It will also help to save time as well as costs and increase effectiveness.

Dealing with multiple problems at once

When deciding for an IDM solution the best option for any company is the option that solves as many problems as possible at once. There are various products available on the market, but not all of them may satisfy company's specific needs. A good quality solution should meet the company's needs in these features:

- usability
- applicability
- security range
- availability
- adjustability

Usability

The IDM solution should simplify Identity Management processes, therefore it has to be easy to work with. Deploying the solution as well as maintaining it is supposed to be smooth and comprehensible. There is an enormous difference in time and costs between flicking couple of switches and writing thousands of lines of code. Both usability and internal logic need to comply with the idea of self-service.

Applicability

An IDM solution that helps to manage users, but not groups, organizational units, projects, services, devices or any other concept related to Identity Management is far from being efficient. The solution is supposed to be applicable in any enterprise that needs to manage employee identities, organizational structure, employee roles, temporary workforce, agents, partners and similar types of identity records. That includes universities, government agencies, third-sector organisations as well as companies regardless of their size.

Security range

A risk elimination can be reached by providing a possibility to manage policies, access rights and privileges that each individual user has. All privileges are supposed to be aligned with the policies. A good IDM solution should support access certification: regular access reviews and audits as well as the possibility to periodically review various settings such as the assignment of roles to users.

Availability

To ensure high availability so the end users are able to log in regardless of the load on the system must be matter of course. A solution is supposed to be able to handle not only small but also big user volume. There is a high probability that a problem with the user management backend will lead to bad customer experience, which can undermine the customer's trust or even make the customer leave to seek services from a competitor.

Adjustability

A good IDM solution should be able to answer the organization’s specific needs regardless to its size, complexity, organizational structure or focus. It should also be able to provide a feedback about important actions, ideally in a computer processable form. Tracking such changes should therefore help to reconstruct older state of the system in the case it’s needed to get back in time.

Why open source?

Open source solutions offer various benefits that make them different from closed source tools. The burden of licenses or the inability to adjust the code without support agreement is just the tip of the iceberg. The security of open source software was doubted in the past. But nowadays open source is the default base for developing software which is used in various facets in different companies. A key advantage of an open source solution is its community that is created over time.

Open source security solutions have been on the market for more than two decades and has evolved rapidly thanks to the community that consistently comes up with excellent features for both general and security purposes. In this community, corporations, smaller companies or even individuals share their ideas about a solution, helping to make it better. By this being created so openly, there is no mystery behind what the code is actually doing. The community is also involved in the development process through the creation of additional features, bug reports, and code reviews of the projects. This community involvement greatly increases the population of testers and code reviewers. Interested parties support the development of new features. This leads to a synergistic effect: everyone who uses the solution benefits from it and also saves money thanks to sharing costs with numerous companies, even frenemies.

Use case: a migration from a commercial solution to an open source one

A large insurance company operating in several European markets works on the implementation of a project for unburdening itself from material bureaucratic paperwork. Parallel to that a migration from an existing commercial IDM deployment to an open source one takes place.

Such a complex project can run into plenty of operative problems that start to appear while using particular processes. New attributes are added as well as policies. The new IDM solution brings the company a possibility to engage significantly more systems than before.

Every company is unique and so are its needs. Therefore only a solution integrated with an access management system as well as custom insurance applications can be the most efficient solution precisely adjusted to the company's specific needs. Customer self-service is just one of many fields where IDM solutions play a crucial role. That's where midPoint excelled. It helps to connect new systems by means of the connectors and to synchronise data. At the end of the project, there is one midPoint solution containing a paperless project which is mentioned above and systems that the company worked with before the project as well as systems added after its beginning.

„We appreciate the flexibility of communication according to our requirements and the quality of the services. The expertise of Evolveum employees is on a level high enough to meet the requirements of the clients in the field of identity management in a very quality and professional way”. These words of satisfaction from company's operations manager sum up the outcome of our IDM solution implementation.

What about the future?

Technologies evolve fast. The Identity Management field is no different. As the needs of companies may become more complex, they look for more advanced solutions. But a good IDM solution has to do more than just answer current company's needs. It should also predict the future ones and therefore be flexible in time. In both cases, the IDM solution should be well-supported with fixes, updates as well as new releases the whole time. That way, it will be able to assimilate to a company, providing sufficient solutions for its problems at any moment.

Evolveum's IDM solution midPoint

One of the most comprehensive IDM solutions currently available on the market is midPoint. It synchronizes several identity repositories and databases, manages them and makes them available in a unified form. MidPoint brings various possibilities of usage thanks to its ability to work for an enterprise as well as for cloud services, Internet portals, telcos, service providers and so on. As an IGA tool, midPoint helps enterprises to solve problems in these three areas: identity provisioning, identity governance & compliance and also access management.

MidPoint as an open source solution can easily meet any company's needs to save costs thanks to its license-free character. The support cost is reduced by a network of excellent technology partners. The most significant saving is in the deployment cost. MidPoint is a second-generation product built on more than a decade of first-hand IDM experience. It has been built by people who deployed IDM solutions for the people that deploy IDM solutions. It can be expected that 80% of the use cases your IDM solution needs can be implemented in midPoint by simply flipping a configuration switch. MidPoint can have a huge effect with very little implementation effort.
To ensure its efficiency and uniqueness, it offers the following features:

- **User provisioning and deprovisioning:** midPoint can automatically create and manage user accounts, groups or even organizational units to allow and disallow users' rights. It helps a company to make sure that users have the correct access rights and permissions. In addition, it simplifies and automates the processes related to the management of access rights.

- **Identity synchronization and reconciliation:** midPoint can seamlessly synchronize several databases. It can make sure that the data is always up to date. The synchronization happens every time a change is detected. Because of generic synchronization, it is able to synchronize almost any object, not just users and accounts.

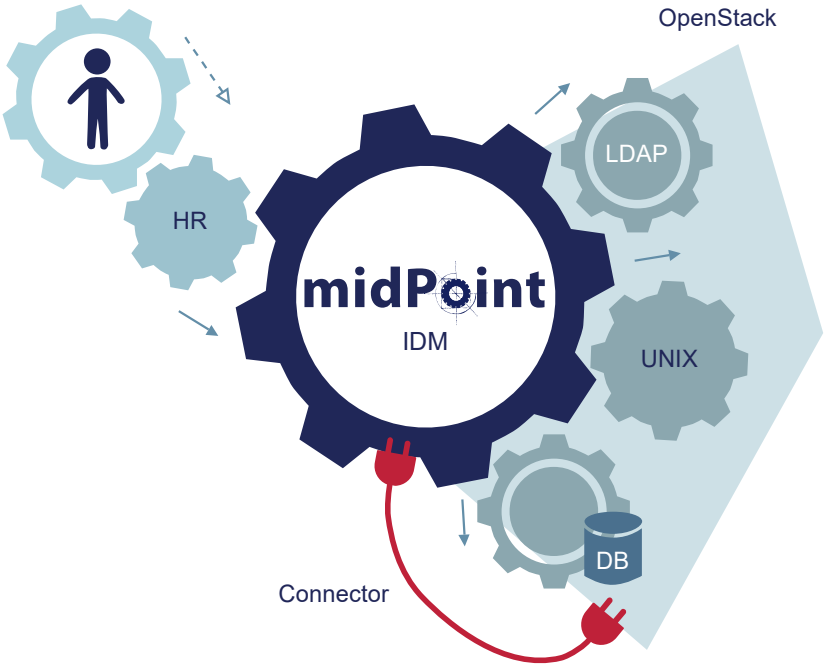
- **Identity management process automation:** midPoint has a built-in workflow engine that can drive approval of access requests.

- **Role-based access control (RBAC):** midPoint can automatically compute user's privileges based on his his assigned roles. It has the ability to specify expressions in the role definitions that determine how and when the role is used. MidPoint allows its end users to customize roles or even role assignments according to their needs. It supports hierarchical, conditional or parametric roles.

- **Management of identity-related parts of the enterprise security policy:** Thanks to its IGA possibilities, midPoint can check password quality or maintain segregation of duties. It manages policies, access rights and privileges that each individual user has. MidPoint has a very powerful and flexible authorization mechanism. Thanks to that, a company can control which parts of GUI a user can access, what operations are allowed, on which objects they are allowed and for which attributes.

- **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 connectors:** midPoint connectors are simple pieces of code providing a connection to another system and the management of identity data. The connectors are non-intrusive: the connected system does not need to be changed.



For more information

To learn more about midPoint and ways it can be useful to you, please visit our site evolveum.com or write us an email.

About Evolveum

Evolveum is focused on professional open source development of leading Identity and Access Management solutions. Established by several independent IT professionals, it's core team is a unique combination of experienced software engineers, identity and access management experts and progressive business-oriented minds. The company's vision is to dramatically improve the field of Identity and Access Management (IAM) by creating and maintaining state-of-the-art professional open source products.

Most of the Evolveum core team is situated in central Europe. However, the products or our work and our expertise is distributed all around the world by the network of our partners, contributors and users. In this way Evolveum is currently present in a significant part of the world.