Evolveum MidPoint 4.8 Release

Nitish Deshpande

November 30, 2023

EXECUTIVE VIEW

This KuppingerCole Executive View looks at the new features in release 4.8 of Evolveum's midPoint IGA platform. Evolveum continues to innovate midPoint by introducing new features around advanced analytics, role mining and self-service support. A technical overview of the overall midPoint's features is also included in this report.

Content

Figures

Introduction

Identity Governance and Administration (IGA) merges the traditional User Access Provisioning (UAP) and Identity and Access Governance (IAG) markets. While many current vendors today offer comprehensive capabilities to qualify as IGA vendors, there are a few, especially the new entrants, that focus on providing either Identity Lifecycle Management (ILM) or Access Governance capabilities to meet unique requirements of the organizations.

ILM remains a core IAM requirement, but Access Governance is becoming a more sought-after capability for organizations requiring better visibility of identity administration and access entitlements across its IT infrastructure. Governance offerings range from simple reporting and dashboarding to other advanced capabilities that include AI and/or machine learning techniques enabling pattern recognition to deliver valuable intelligence for process optimization, role design, automated reviews, and anomaly detection. IGA comprises the capabilities in IAM market that broadly deal with end-to-end identity life-cycle management, access entitlements, workflow and policy management, role management, access certification, SoD risk analysis, reporting, and access intelligence and Access Intelligence for business-related insights to support effective decision making and potentially enhance governance. Several essential components and practices of IGA include:

- Identity lifecycle management
- Provisioning and deprovisioning of access
- Access intelligence
- Access request and approval
- Access certification
- Role management
- Segregation of Duties (SoD)
- Audit and compliance

The latest trend is to integrate IGA tools with AI and Machine learning (ML) capabilities. In doing so, IGA tools benefit by consuming the user's access activity such as authentication and authorization information across IT applications and systems to establish and continuously update user access patterns based on their role and peers' groups. Similarly, Data Access Governance (DAG) tools can benefit from IGA integrations by consuming user identity and access entitlement information and in turn offer contextual information on device endpoint and data residing on the device and other sources to the IGA tools for better policy management.There is a lot of scope for adoption of forecasting and prediction capabilities in IGA solutions. In the below poll result, half of the participants have not deployed AI and ML related features for supporting IGA functions. Variety of opportunities can be brought to the forefront by predicting and forecasting the outcome of activities. This function can be termed as ‘Simulations’. The opportunity to look into the future, offering a preview of what will be executed. It will help bring better insights and make better decisions. This ability to anticipate can enable organizations to prepare and strategize for potential outcomes, ensuring the avoidance of any unforeseen or undesirable consequences.

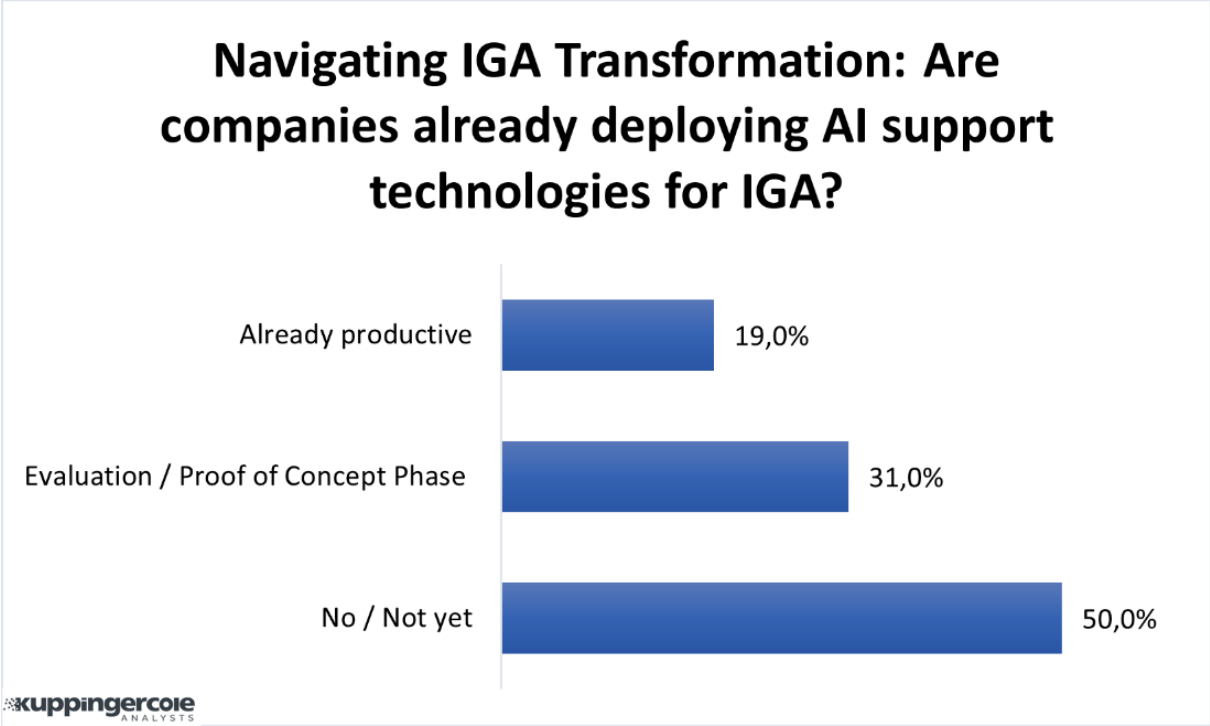

Figure 1: Scope of AI in current IGA landscape (Source: KuppingerCole Analysts)

Regarding IGA solutions, additional capabilities should be considered to improve process efficiencies, alleviate repetitive tasks, and reduce human error. Providing analytics capabilities to IGA can provide insights into access patterns, compliance status, and potential risks. The addition AI and ML can be used to automate complex tasks. Automation within IGA can help with access provisioning when new users join the organization and the deprovisioning process when users leave or change roles. Automating these processes can help minimize the risk of orphaned accounts and unauthorized or overprovisioned access. Another consideration for organizations is moving IT security services to the cloud and adopting cloud-native approaches to attain cost efficiency, scalability, agility, and innovation capabilities. Vendors have identified this opportunity of AI and ML and have started working on it to provide new capabilities. Evolveum has made investments in its IGA platform by introducing various features leveraging AI and ML.

Product Description

Founded in 2011, Evolveum is an Open-Source IGA vendor based in Slovakia. Their midPoint product is provided as an open source and is delivered as a single platform that focuses on IGA data protection and organizational management use cases.

Evolveum continues to invest in identity analytics of its midPoint IGA platform. midPoint as an IGA solution, has strong features around access reviews and provides support for target systems through various industry standard connectors.

Evolveum's midPoint is offered as an open-source Identity Governance and Administration (IGA) solution with a range of key features. midPoint offers support for various identity repositories including standard LDAPv3, and Active Directory (AD) access. While midPoint provides SCIM for identity provisioning, it favors a policy-driven approval process over a traditional workflow engine. Evolveum supports deployment of midPoint through various options such as on-premises, Docker, hybrid, and cloud, with customization possible through Apache Maven. midPoint can expose all of its functionality through REST and SCIM APIs, complemented by command-line interfaces. The UI of midPoint displays functional dashboards, a shopping cart paradigm for role requests, and robust approval workflows. The solutions also supports reporting capabilities for auditing purposes, however, there's a noted absence of advanced identity and access intelligence features.

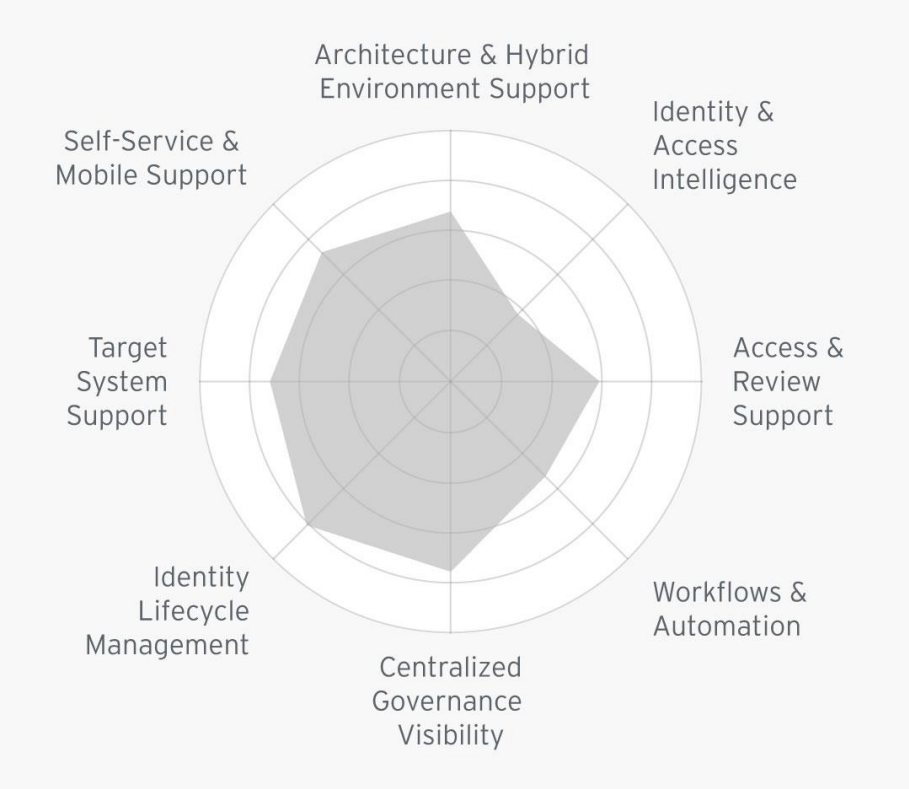

Figure 2: Evolveum midPoint's IGA capabilities rating (Source: KuppingerCole Analysts KC Open Select tool)

midPoint supports a comprehensive list of connectors, particularly for on-premises systems, facilitating seamless integration and data exchange. Its policy management capabilities can enable organizations to enforce and automate access control effectively. Furthermore, midPoint has good support for access reviews for enhancing security and compliance. The solutions also supports DevOps, offering flexibility and automation in deployment and management.

Due to its open-source nature, midPoint is offered as a product with no license fees excluding the maintenance costs. midPoint's features for access governance include a

centralized role management that consists of role discovery support. Role mining has been added in the new release that can help with simplifying Role Based Access Control (RBAC) by detecting candidates for business roles based on the existing data. In addition to other governance features, midPoint supports role lifecycle management and data protection. They provide policies for RBAC and organizational structure that can be used for SoD use cases. In this new release, they are leveraging a strong skillset around computational engineering to present the advanced features for role mining, simulations, and self-service support.

The 4.8 release consists of features which have been expanded in various areas of the midPoint platform. The changes are focused on providing tools in three main areas:

1. Simulations: This feature allows to see and predict what will happen during different operations, such as reconciliation, by performing advanced analytics
2. Object and Event Marks: This capability defines which events are monitored during processing simulations in the system and what is allowed to be performed on objects that are marked because of incorrect data
3. Role Mining: AI and machine learning powered functionality for mining roles based on existing data in midPoint

Evolveum uses the strong foundation of its IGA platform and combines it with constant innovation for providing advanced features.

Simulations

Evolveum uses the term simulation as an umbrella for including various modules of the “what-if” analysis. This feature allows admins to see the consequences of certain actions without the risk of comprising the current system.

Simulations bring a multitude of advantages to the forefront. They provide a unique opportunity to look into the future, offering a preview of what will be executed for example during reconciliation processes. This foresight enables organizations to prepare and plan for potential outcomes, ensuring that any unexpected or undesirable consequences are avoided. Simulations serve as a safeguard against incorrect configurations, allowing for timely adjustments before any damage is incurred, thereby mitigating the risk of operational disruptions or security breaches. Simulations also aid in evaluating the quality of data by offering an interactive reporting and discrepancy marking mechanism. This not only assists in data cleansing but also provides a deeper understanding of the underlying processes, rules, and policies within the organization. It highlights where exceptions may exist, allowing for fine-tuning and optimization.

Evolveum suggests simulations provide benefits such as the assurance for final testing in a production environment without the fear of causing unintended disruptions. It is a comprehensive process to analyze data integrity and simultaneously clean up irregularities to provide consistent data. This process also involves analysis of correlation rules used to map correlated users to existing users. The mappings can be customized based on the attributes of users and can provide quick awareness of orphaned accounts, for instance. Once the simulations are run, the results show a wide variety of metrics, such as how many objects will be activated/deactivated through this event. Metrics are computed based on the event marks. These event marks are available out of the box but can be configured based on

requirements. During these simulations, no actual changes are executed, however, they are solely stored for later analysis. Organizations can then experiment, fine-tune, and validate their processes without the potential risks associated with real-time implementation. This feature can avoid unnecessary damage by identifying incorrect configuration on an attribute level by enabling mappings.

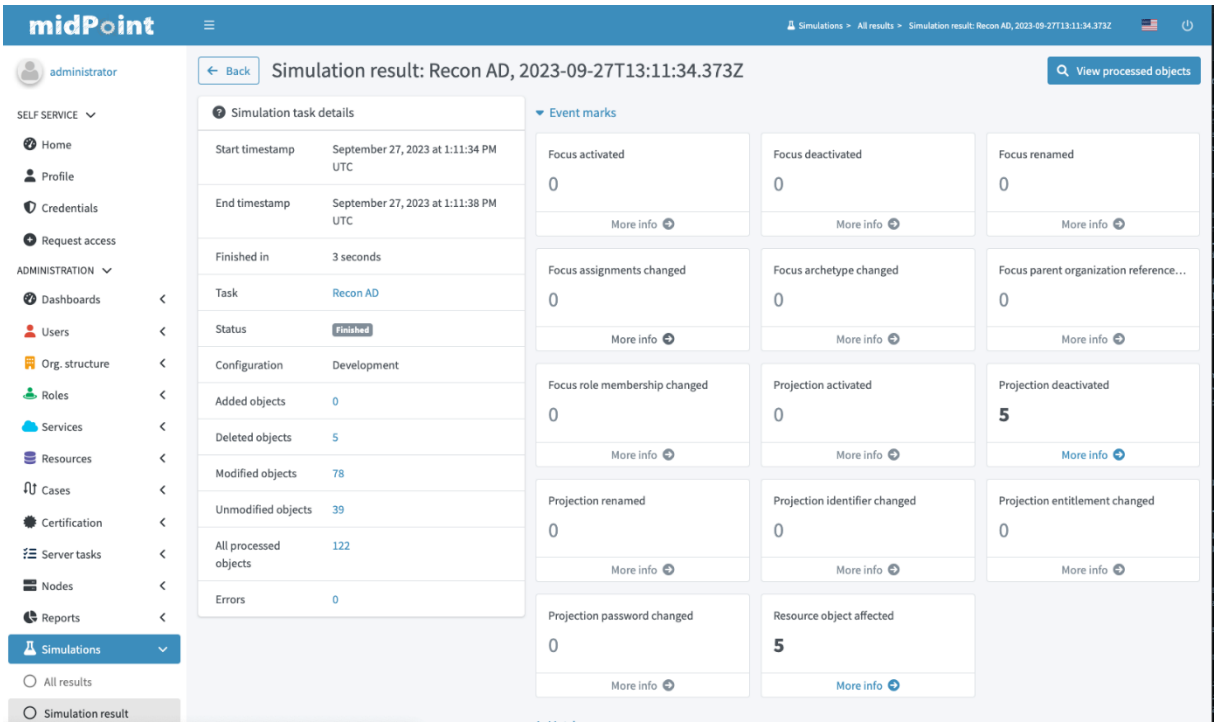

Figure 3: Simulation results dashboard (Source: Evolveum)

Simulations help to understand the processes, policies and rules in organizations and understand where exceptions exist. In essence, simulations in midPoint serve as a powerful tool for informed decision-making, risk mitigation, and process enhancement, ultimately contributing to the overall efficiency and security of an organization's identity management and governance systems.

Object and Event Mark

Monitoring system events with event markers helps track the execution of events within the system, providing visibility into processes. Simulations can determine the number of users to be activated/ deactivated and how many accounts or attributes will be modified, offering a comprehensive overview of the expected changes. Summarizing these changes simplifies the analysis process, making it more straightforward and easier to comprehend. Object marks allow for defining permissible actions on objects, while also highlighting objects with incorrect data and protecting sensitive objects from unauthorized modifications. Dashboards and reports are essential tools to assess the current state of the system's data. By setting rules and thresholds, simulations used for reconciliations can help identify reasons behind threshold breaches, ensuring a well-monitored and controlled system.

In midPoint, the dashboard of object marks can be configured for different marks to see the real state of the system. The combination of simulations and marked object/ event marks

plays a pivotal role in enhancing trust among stakeholders in various domains. When everyone involved knows what to expect, it not only increases transparency but also generates a sense of predictability and preparedness. For customers, this can be especially beneficial, as they can better anticipate and plan their interactions with a system or service, leading to more confidence in their decisions and interactions. midPoint leverages these capabilities to confidence in IGA by ensuring access management and security measures are clearly understood and predictable, which is essential for safeguarding sensitive data and maintaining compliance. Furthermore, this process can also contribute to data cleanliness, as the insights gained from simulations and marked conclusions can help identify and rectify data discrepancies, further strengthening the overall trust and reliability of the system. Moreover, simulations together with object marking can significantly speed up the automation of “Joiner, Mover, Leaver” (JML) processes.

Role Mining

The incorporation of AI and machine learning-powered functionalities within midPoint has facilitated the role mining process. midPoint uses this technology by enabling the detection of roles through data clustering, pattern recognition, and similarity methods, facilitating the identification of patterns and relationships within existing data. This, in turn, allows midPoint to suggest potential candidates for new business roles, streamlining the process of role creation and optimization. As a result, access management becomes considerably simpler, reducing administrative overhead and enhancing transparency in access assignments.

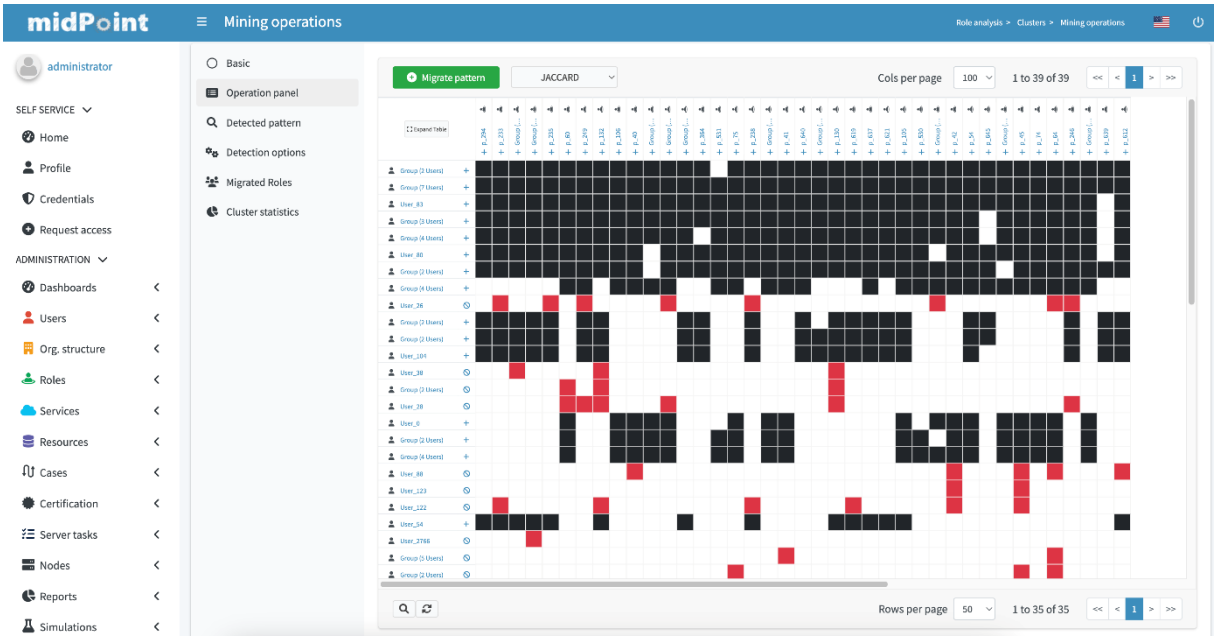

Figure 4: User-permissions matrix for role mining

midPoint’s role mining matrix provides a visual representation of existing assignments of roles to users. This matrix helps to identify which business roles can be created and how many assignments will be reduced. Moreover, the utilization of AI and ML in role mining ensures the establishment of efficient audit trails, providing a comprehensive and easily traceable record of access activities. This not only enhances security and compliance but also contributes to a more agile business environment by expediting decision-making

processes. Additionally, the data-driven insights acquired through AI/ML-driven role mining can serve as a foundation for policy mining, paving the way for the development of advanced policies and access control measures that are more closely aligned with the organization's evolving needs and objectives. In sum, AI/ML-powered role mining in midPoint represents a significant advancement that not only optimizes access management but also lays the groundwork for improved governance, security, and adaptability within the organization.

Strengths and Challenges

midPoint offers a unique simulation feature, which has various benefits. It not only aids in predictive analysis but also plays a crucial role in data cleanup and integrity maintenance. Evolveum suggests it can lead to significant enhancements in the quality of HR data and facilitate thorough cleaning of application inventories. The usefulness of these simulations is notable, as they are available for a wide array of objects, including users, applications, and roles. To further enhance data protection and analysis, object marking is employed to prevent inadvertent damage and generate valuable insights for creating informative dashboards. Additionally, the inclusion of a role mining feature adds to the system's comprehensive capabilities, making it a robust solution for Identity Governance and Administration.

midPoint still has some challenges such as support for major compliance frameworks is missing. Noticeably, MidPoint is missing more advanced identity and access intelligence capabilities however Evolveum has plans to introduce features around advanced identity analytics in the near future.

Evolveum currently has a five-year innovation plan for its midPoint platform. Upcoming features for the 2024 are focused on role engineering, certification improvements, lightweight reconciliation, and an advanced lifecycle management. Evolveum also plan to introduce features around risk management, advanced analytics, personas improvements, mobile application, and a connector marketplace in the next few years.

Evolveum customers are primarily focused in the EMEA region with North America coming in as the second most important region. Evolveum's customer deployments include medium to enterprise companies and universities. midPoint provides good on-premises DevOps options and hopes to move towards a hybrid or a full cloud environment in the future. Overall Evolveum MidPoint continues to improve and may be of interest to organizations with general IGA for mainly on-premises deployments, but their solution is also cloud ready through their cloud partners.

Strengths

- Simulation feature provides forecast as well as data integrity
- Good use of AI/ML for role mining
- Open-source solution provided at no (license) cost
- Object marking helps to prevent damage, make analysis through configurable dashboard
- midPoint now supports flexible authentication from this new release
- Possibility to modify connectors via coding

- Open access is provided with unlimited testing before adoption of the solution

Challenges

- Limited but growing partner ecosystem outside EMEA
- Support for major compliance frameworks for reporting is missing
- Some advanced identity analytics features are missing but are in roadmap
- Integration to third party ITSM solution is not available out of the box but can be created through request
- SDK support is limited to Java and Python

Related Research

Leadership Compass: Identity Governance and Administration 2022
Leadership Compass: Access Governance 2023
Leadership Compass: Access Management 2023
Leadership Compass: Access Control Tools for Multi-Vendor LoB Environments

About KuppingerCole

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators, and software manufacturers in meeting both tactical and strategic challenges and making better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

For further information, please contact clients@kuppingercole.com.