KuppingerCole Report

EXECUTIVE VIEW

By Martin Kuppinger
August 18, 2020

One Identity Active Roles

One Identity Active Roles is a powerful tool for integrated management of both on-premises Microsoft Active Directory and Microsoft Azure Active Directory. It comes with strong support for managing Exchange Servers and Office 365, but also Identity Lifecycle Management that supports a range of non-Windows and SaaS applications.

By **Martin Kuppinger**
mk@kuppingercole.com

Content

1 Introduction

Digital identity is a critical business-enabling technology for all types of organizations, including Small to Mid-Size Businesses (SMBs). However, as is borne out by cybercrime reports year-after-year, digital identity is also a primary vector through which SMBs are attacked. Many SMBs lack a fully staffed IT department to handle the complexities of deploying, maintaining, and securing complex IAM solutions. This is a factor fueling the need for targeted solutions that support these businesses in managing their environments.

The risks of not having well-maintained and secure IAM solutions - can be great, ranging from lower productivity associated with password resets and incorrect entitlements; loss of data such as employee and customer PII; loss of trade secrets and other valuable business information; diminished revenue from reputation damage and fraud; to unwittingly becoming a vector of attack to other members in a supply chain. Many managers and owners naively assume that they are too small to be attacked by malicious actors, but **cybercrime studies** show that organizations of all sizes are increasingly targeted because of the perception that they are less secure than larger organizations.

Organizations can have a variety of use cases and technical requirements they need to meet with IAM. Regarding use cases, everyone needs B2E IAM, many need B2B, and some need B2C. Consider B2E, where most will have Microsoft Active Directory in place. Many organizations also utilize various cloud-based SaaS applications but do not have the IAM functions centralized or even under control. Furthermore, with a very significant ratio of organizations utilizing Microsoft 365 including Office 365 and thus having Microsoft Azure Active Directory (Azure AD) in place, a unified approach for managing these services is required.

For all organizations, getting a grip on the environments such as Microsoft Active Directory and Azure AD requires capabilities beyond what enterprise-grade IGA (Identity Governance and Administration) tools commonly deliver. The in-depth management of Active directory, Azure AD, and related environments demands specific capabilities, such as the in-depth management e.g. of SAP environment also does. Thus, there is a place for such solutions in combination with full-blown IGA tools.

A sometimes-overlooked capability is that IAM systems can aid in regulatory compliance. Under the General Data Protection Regulation (GDPR) in the EU, collecting clear and unambiguous consent from consumers for the use of their data is necessary for compliance. Well-designed IAM solutions can enforce and help demonstrate compliance with regulations that require segregation of duties, i.e. SOX in the US.

There are three major categories of functions within IAM to look at:

Identity Administration: The ability to administer identity lifecycle events including provisioning/de-provisioning of user accounts, maintaining identity repositories, managing access entitlements, and synchronization of user attributes. A self-service user interface allows for requesting access, profile management, password reset, and synchronization. Configurable cloud-native connectors offer automated user provisioning to both on-premises as well as SaaS applications. Other common identity administration capabilities include administrative web interface, batch import interface, delegated administration, SPML, and SCIM support.

Access Management: This category includes authentication, authorization, single sign-on and identity federation for both on-premises and SaaS applications delivered as a cloud service. The underlying support for industry standards such as SAML, OAuth, and OpenID Connect can vary.

Access Governance: This group of capabilities that are frequently absent from the portfolio of entry-level IAM tools centered around AD, given that many organizations only look for an easy-to-use, administrator-centric approach on maintaining Access Governance and enforcing least privilege principles.

One Identity with its Active Roles offers a comprehensive and proven tool for managing identities and access in the environments that are centered around Microsoft Active Directory and with strong support for Azure AD, but also delivering a strong addition to enterprise-grade IGA tools for in-depth management of Microsoft Active Directory and Azure AD.

2 Product Description

One Identity Active Roles is a proven, mature solution. Over the past years, the solution has been extended to support the "hybrid Active Directory", as One Identity calls it, i.e. delivering support for Azure AD in addition to the on-premises Active Directory, where the roots of Active Roles are. It provides an integrated tool for administering both of these environments, but also the ability for managing further systems. It can extend the AD account lifecycle management and reporting beyond these platforms to non-Windows systems and SaaS applications. While not being a comprehensive IGA (Identity Governance and Administration, delivering Identity Lifecycle Management and Access Governance) solution, it comes with strong support for a range of use cases.

The focus of One Identity Active Roles is on providing a high degree of automation in the management of user accounts and groups in Active Directory and connected systems. It is targeted at delivering improved usability and efficiency for administrators and operators, when compared with the native tools provided with Active Directory and Azure AD. Aside from improved administration and user experience, the focus is on automation, on regulation of administrative access, and the integration of a range of other systems and applications that can be connected to Active Roles.

The ability to manage both the traditional on-premises Active Directory (AD) and Azure AD from a combined tool already provides a significant advantage, given that while there is some technical integration in synchronizing information between these directories, there are no out-of-the-box tools provided with these which would allow for a consistent, integrated administration. This - is a major advantage.

Beyond that, managing secure access for administrators and operators is additionally of significance. When just using built-in tools, there is little control over administrative activities, if these are allowed by the account used – and if they are administrative accounts, there are little to no restrictions. Active Roles provides control for such changes by utilizing administrative policies that define the permissions certain users or groups of users have for managing AD and Azure AD environments. Approval workflows (which can be constructed via a drag-and-drop graphical UI) for changes are supported and privileges of users can be controlled through a least-privilege model. The risks of unwanted changes, either by fault or fraudulent action, can be successfully mitigated.

Active Roles furthermore adds support for strong authentication by integrating with Identity Providers and their authentication capabilities via the OAuth and Radius protocols. This adds security, robustness and flexibility for the authentication of administrators and operators.

These capabilities allow for both efficient day-to-day management of AD and Azure AD, and for automation of user lifecycles across these and other connected systems. Active Roles capabilities for administration include, amongst others:

- AD Group Management, which is one of the common challenges specifically in AD management with its concept of nested groups

- Management of computers including shares, printers, or local users, which is specific to on-premises AD
- Management of mailboxes and related tasks around Microsoft Exchange and Exchange Online

However, Active Roles is more than just a management tool for AD and Azure AD, as it also supports Identity Lifecycle Management capabilities beyond these environments. An important foundation for this is on one hand the support for the SCIM (System for Cross-Domain Identity Management) standard, which is the major standard around Identity Lifecycle Management, and on the other hand the integration to One Identity Starling Connect, which allows for using SCIM-based connectors inbound and outbound from a range of target systems.

Based on that, administrative actions on accounts in AD and Azure AD can automatically trigger actions on other systems such as LDAP directories, Office 365, databases such as Oracle Database and Microsoft SQL Server, and a series of other systems with direct integration. Additionally, all systems supporting the SCIM standard, such as Salesforce, ServiceNow and Ping Identity also can be integrated with Active Roles including through One Identity's own Starling Connect solution. Beyond the common Identity Lifecycle Management tasks such as user management (create, modify, delete) and entitlement management via group management, Active Roles also supports tasks such as the assignment of resources in Windows or the creation of mailboxes in Exchange and Exchange Online. Furthermore, all AD-joined systems including Linux, Unix, and Mac OS X are supported through Active Directory bridge technologies such as One Identity Authentication Services.

Last but not least, Active Roles supports a range of reporting and analytics capabilities. While this is not a full Access Governance solution supporting access reviews or SoD (Segregation of Duties) policies, it provides good insight and support for fulfilling audit and security requirements in the daily work of AD and Azure AD administrators and operators.

Active Roles runs on Windows Server both onPrem and in the cloud while the administrative tools are available as both MMC (Microsoft Management Console) applications and as web applications. Active Roles also can automate functions based on Microsoft PowerShell.

3 Strengths and Challenges

One Identity Active Roles is a powerful solution for organizations running infrastructures with on-premises Active Directory and/or Microsoft Azure AD. It provides a consistent, efficient management interface to these platforms, as well as support for managing Exchange/EOL mailboxes. In addition it adds security features, controlling and limiting the capabilities of administrators and adding request and approval workflows for administrative actions.

The solution is not limited to just managing these environments, but comes with robust capabilities for Identity Lifecycle Management and provisioning to a range of additional solutions, either by utilizing the SCIM interface and One Identity Starling Connect or an AD Bridge solution. Thus, it is well able to serve baseline IAM requirements, specifically for organizations heavily reliant on the AD/AAD environments or for the AD/AAD portion of a more complex heterogeneous enterprise, while adhering to corporate policies and adding powerful capabilities for administrators.

While the current UIs are adequate to the common users of such solutions, MMC still is a rather traditional user interface. One Identity would be well advised in transferring all capabilities to modern, web-based UIs, with Azure AD increasingly becoming the central platform for organizations, and on-premises AD gradually retiring into a legacy state. What might be considered as a gap is the lack of strong analytical capabilities for the current state of entitlements in AD and Azure AD.

In summary, Active Roles can complement IGA solutions in large enterprises by adding strong features for increasing efficiency and automation in AD and Azure AD management, while being a comprehensive offerings for organizations that don’t want to go for a full IGA solution or prefer to focus on AD/AAD for the time being.

ONE IDENTITY™

Strengths

- Purpose-built for optimizing administration of Microsoft Active Directory and Azure AD
- Provides Lifecycle Management for a range of non-Windows and SaaS applications, including support for the SCIM standard
- Workflow-based request and approval of administrative tasks
- Good out-of-the-box integration to Azure AD and Office 365, with full support for hybrid management of on-premises AD and Azure AD
- Well-thought-out and easy-to-use user interface, but also support of traditional MMC for Windows administrators
- Good reporting and analytical capabilities, while not offering full Access Governance
- Can well co-exist with full IGA solutions, delivering in-depth control of AD and Azure AD

Challenges

- No full-featured IGA capabilities, but targeted at Microsoft Active Directory/Azure AD environments
- Good auditing and analysis capabilities, but limited interactive analytics of complex entitlement structures
- Not all capabilities available through web-based UI yet

4 Related Research

Architecture Blueprint: Access Governance and Privilege Management - 79045
Executive View: One Identity Manager – 80310
Executive View: One Identity Safeguard Suite- 80074

Copyright

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

KuppingerCole, founded back 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 make 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.

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