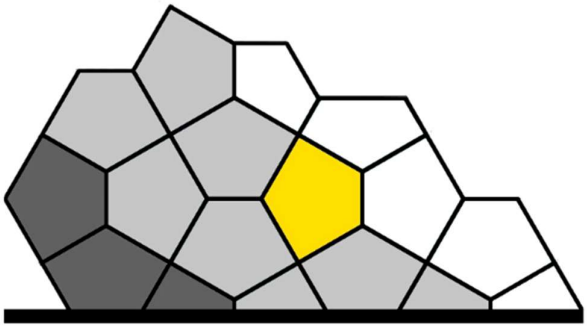
Mining For A Role



A Madigan Solutions White Paper

ABSTRACT

Role Based Access Control is not a new concept within Identity and Access Management and one that will not be disappearing anytime soon.

Ensuring that roles are appropriately scoped and maintained is just as important as certifying who has them.

The paradigm of Role-Based Access Control should not be an unfamiliar one to those involved in the Identity and Access Management space. It has become the established model when it comes to access control in organisations and enterprises because it combines flexibility, ease of administration, and dovetails nicely into the automation of business processes, helping reduce costs, both from a time and administrative perspective.

That said, it does come with its own set of problems. It can also be one of the more costly and certainly time-consuming parts of an Identity and Access Management programme with a large volume of data to sift through to identify roles.

Over time this can lead to users having a proliferation of roles and application access. Without proper checks and balances, this can lead to users having too much access and introduces a major pain point when trying to understand what access has been granted and whether it is still applicable to the job function or individual.

WHAT IS ROLE MINING?

Simply put, role mining is analysing existing access to IT resources within an organisation to generate a set of roles that collates these access rights into a set of related functions, the result of which will be a simplified entitlement assignment model. There are two approaches, top-down (examining job functions to determine relevant permissions) and bottom-up (making use of the existing permission assignment data).

BOTTOMS UP!

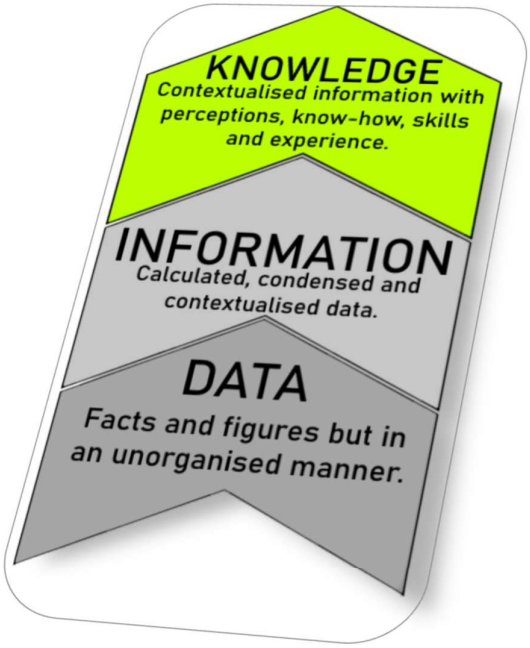
Traditionally, role mining approaches have focused on top-down analysis. This involves examining job functions and trying to determine the set of permissions that are relevant to the set of tasks that are associated with them. This approach can of course generate meaningful roles which are representative of the jobs within an organisation, but the overall process is very labour intensive.

However, the more likely scenario is that organisations have been happily working away with their existing Direct Access Controls or Role-Based Access Control model and with the progression of time, job demands, and functions have evolved. This could be due to a merger or acquisition, perhaps the application functionality has been expanded, or perhaps the employee has moved to a different role. However, without ongoing role maintenance, the existing set of roles have become less useful and more chaotic.

This is where the “bottom-up” approach comes in. This technique takes the existing user and permission assignment data and mines that data to formulate roles. Of course, solely looking at user permission assignment data will only achieve so much when performing this analysis. Therefore, having extra data points, such as HR data and organisation structure information can help extract more benefit from the mining process when it comes to accurately identifying potential candidates.

THERE'S ROLES IN THEM HILLS!

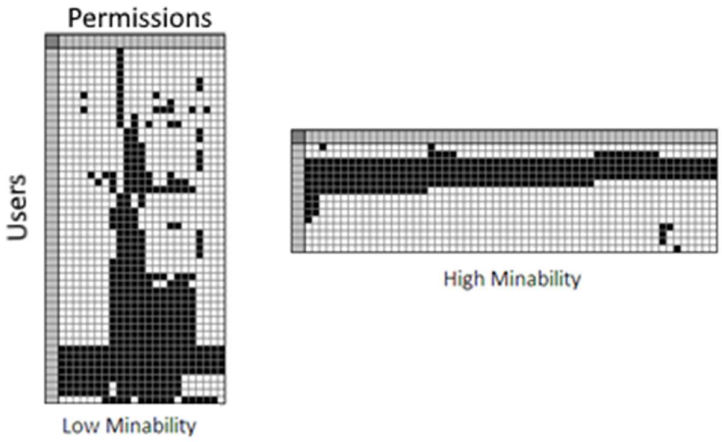
Digging and sorting through all that data is going to be time consuming but just like with real mining operations, there are tools and techniques which will help with the exploration exercise.



Once all the data has been collected, you can start to chip away at areas where you feel the most immediate value will come from, rather than trying to break all the rocks at once and hoping you find some gold.

This could be based on a geographic region, perhaps only a particular application needs addressing, or maybe a potential set of useful roles could be yielded by separating by manager. Of course, there is nothing stopping a combination of these criteria being used to help produce a larger cross section of data to further examine.

Once this initial exploration step has been completed, the results will help determine which partitions will yield the most positive results for further examination - referred to as "mineability".



Once a suitable area has been identified, further surveying work should be performed by setting some additional parameters, such as:

- The minimum number of users for the candidate role.
- The minimum number of entitlements that should be considered when creating the candidate role.
- The *clustering* preference. For example, should the role cover the highest number of users, entitlements, or a balance between the two?

THE ROLE LIFECYCLE

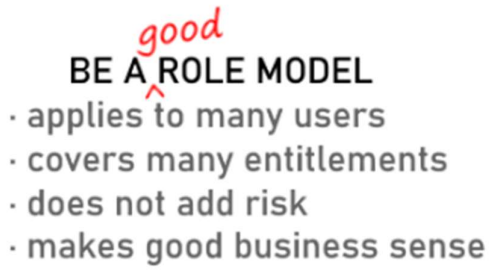
After the candidate roles have been identified, the next steps are:

- **Validate** each role.
- **Publish** each role to the Identity Management / Identity Governance platform.
- **Assign** existing users to the new role (and decommission redundant roles as necessary)

The vetting process could involve the roles being released for review and approval by an appropriate member of staff unrelated to the person responsible for identifying the candidate roles.

Once the role has been approved, it can be published into the identity governance administration tool.

However, having to go through and realign all users to these new roles is also a time-consuming task, so would it not be more efficient if the tooling could do it for you? That is certainly possible with the right tooling in place.



WAYS TO ADD VALUE

- **Integrating risk analysis.**
- **Easily consolidating existing access to newly mined roles.**
- **Versioning and rollback capabilities.**

ROLE OPTIMISATION AND LIFE-CYCLE

As organisations evolve over time, permissions and roles can get diluted. It is easier to create and grant a new role which gives a limited set of permissions to perform a function rather than review and improve the quality of all existing roles.

This can lead to users having a proliferation of roles & accesses, making it difficult to understand who has what and, crucially, complicating the re-certification process.

By performing regular re-evaluation of the existing Role-Based Access Control set, roles can be tuned to user behaviours and business requirements.

Coupling this with an ability to version roles, the role life-cycling model starts to look a little more complete. Inherently, this version control also presents the opportunity to rollback should the need arise.

Finally, the ability to automatically consolidate access to the roles eliminates a huge amount of administrative overhead meaning the process of role optimisation starts to become more rewarding for the effort.

WHAT ABOUT RISK?

Of course, when assigning users access rights, there is going to be an element of risk, be it an operational risk or an access risk. With so many different actors (employees, contractors, robotic process automation etc) involved, keeping a handle on these risks can be difficult!

One way to address this is by taking the same data snapshot and modelling it for the risks which have been defined elsewhere within the tool. This does not have to be done in conjunction with the mining process but can be used as another check and balance to ensure that the role optimisation and life-cycling processes are having a positive effect on the overall risk profile.

Over time, using several of these snapshots, a picture can be built up on progress towards reducing the risk profile within the roles of the organisation.

Those risk criteria can be configured to suit the needs of the organisation. Some examples:

- Not Recertified.
- Power Users (Users with a lot of critical permissions).
- Separation of Duties Risk (Users with SoD conflicts).

A pro-active approach here will do wonders to keep risk managers on-side!

SUMMARY

Sadly, there is no silver bullet to Role-Based Access Control - yet. What you may find is a combination of these two role mining approaches may work best for your organisation and which combination (top-down/bottom-up or bottom-up/top-down) is ultimately down to your specific needs and resources.

However, there are tools and expertise out there to help ease the burden. Tools can help sieve through the vast amounts of data and help present the information in a way that simplifies the decision-making process.

Tools such as **IBM Security Verify Governance** can help:

- **Sift** through the vast amounts of data and help present the information in a way that makes the decision-making process straight-forward.
- **Model** the risk profile of users and their entitlements over time.
- **Streamline** the introduction of optimised roles by reducing the administrative effort of migrating users to these new roles.

LEARN MORE

To learn more about how to analyse your Role-Based Access Control needs within your organisation and how an IBM Security Verify Governance solution can be used to realise this, visit **www.madigansolutions.com**

ABOUT MADIGAN SOLUTIONS

Madigan Solutions UK Limited is a leading provider of IBM Security Verify solutions. Whether your needs are access management, identity management & governance or privileged access control & monitoring, Madigan Solutions can help you satisfy those needs.