

CA Advisor

SECURITY MANAGEMENT NEWSLETTER

September 2008

Maximize Identity Management Benefits With an Accurate Role Foundation

By Michael Liou

User identity and business roles would seem to be almost inseparably intertwined. Yet there has been a gap in the IT infrastructure that has maintained some degree of separation between the two in the identity management ecosystem. Until now, that is.

As identity management has become mainstream, organizations have recognized the inherent value of tying identity management solutions with a role



model. Role engineering is becoming a frequently adopted step in this process of grouping user access rights so they can be automatically applied and managed. It will yield an accurate role model (or validate the accuracy of the organization's existing role model) to provide a foundation that improves identity management and identity compliance initiatives.

Interestingly, the discipline of role management has been somewhat overshadowed by a market that quickly embraced identity management often without stopping to formalize the role discovery process. Now, organizations have begun to understand that, in order to maximize the benefits of identity management, they must have a role foundation that is accurate and up to date.

Role engineering is certainly not a revolutionary concept. For years corporate sleuths have manually poured over org charts and access control lists to search out commonalities, define roles and then map employees to common sets of privileges. This process may sound

elementary, but it quickly becomes very challenging (and time-consuming) as organizations grow larger, their user populations become more diverse and they expand across geographic boundaries.

What's new is that automated role engineering is just now becoming practical, thanks to increasingly sophisticated applications that apply computational analytics to help build role models. CA recently partnered with Eurekify to offer its role management solution which is based on advanced pattern-recognition technology. Eurekify, in tandem with CA Identity Manager, creates an end-to-end solution that enables organizations to easily and efficiently manage user identities throughout their lifecycles.

All the Right Steps

The first step in successful role management is creating an accurate role model. Precise role models improve overall identity management because they allow organizations to appropriately automate identity processes while minimizing management overhead.

The first step in defining a role model is importing the baseline data that you will use to define roles. Be careful to identify the best data source (or sources) for this step, since the quality of your results will depend on it. Typically, an identity management solution like CA Identity Manager already serves as a centralized source of identity information so it provides a logical source

Organizations have begun to understand that, in order to maximize the benefits of identity management, they must have a role foundation that is accurate and up to date.

for baseline data. If your organization hasn't yet deployed an identity management solution, other likely data sources include the corporate directory, a centralized business system or a mainframe security solution such as CA ACF2™ or CA Top Secret®.

The second step is cleaning the data to ensure your role model is built on accurate user information. Flawed data is sure to produce false results such as unnecessary roles or inaccurate entitlement assignments. Eurekify Enterprise Role Manager employs sophisticated analytics that identify anomalies — existing roles and privileges that are out of pattern — to help you scrub data.

After cleanup, you're ready to build the role model. You can tackle this task from two approaches. The first, a top-down role modeling strategy, analyzes organizational characteristics to identify commonalities in roles. For instance, all employees in the European sales organization would typically be granted the same set of fundamental access privileges; that would be labeled the "European Sales" role.

It's vital to ensure that the role model is accurate before integrating that information into the identity management system.

The alternate approach is bottom-up modeling which examines existing privilege assignments to suggest potential roles. If, for instance, upon examining existing data, you find virtually all users

have accounts in the email, human resources and corporate expense systems, there's a good chance this can be used as a baseline for the "General Employee" role.

Regardless of the path you take, or if you employ a combined approach, it's vital to ensure that the role model is accurate before moving on to the final step, which is integrating that information into the identity management system. These roles can then be used in automating processes such as provisioning or allowing users to make self-service requests. As rights and roles will continuously change, it's a good practice to review the role model on a regular basis and update it as necessary. Having used a role management solution, you will be able to follow the same methods as used in the initial analysis so that role and privilege definition processes remain consistent.

Identity management solutions deliver important business and security benefits by automating processes such as provisioning, user self-service or identity administration. Surprisingly, deployments are often based on an inaccurate role foundation as the difficult and time-consuming nature of role engineering de-prioritized this process. Only after the identity management investment was made did the organization recognize the benefits that a better role foundation would yield. The good news is that role management technologies now exist that exponentially decrease the effort involved in role engineering, presenting an opportunity for you to efficiently maximize the return on your identity management investment.

Michael Liou is a Principal Product Marketing Manager at CA, where he is responsible for defining the strategy and positioning for CA's Identity Lifecycle Management solutions. He has spent the past eight years in the software industry, gaining experience in solution consulting and most recently, leading product management at an enterprise mobile application software company. Michael has a Bachelor of Science in Operations Research and Industrial Engineering from Cornell University and is a Certified Information Systems Security Professional (CISSP).

For the latest issue of CA Advisor: Security Management Newsletter, visit ca.com/newsletters/secure. To subscribe to receive future issues, or to manage your preferences, visit the [CA Preference Center](#).