

CA Advisor

SECURITY MANAGEMENT NEWSLETTER

August 2008

Improving Entitlement Management With Role-Based Access Control

By Srinivasan Vanamali



Role-based access control (RBAC) is becoming the norm for managing entitlements within commercial systems and applications. RBAC can also play a significant role in establishing a model for enforcing

security within organizations. It simplifies entitlement management by using roles (as opposed to users) as authorization subjects. Having a holistic approach to role definition can help alleviate certification-related regulatory compliance challenges, and should be considered an integral part of any Identity and Access Management (IAM) initiative.

While RBAC should not be considered a panacea for all ills related to access control, it has proven to be cost effective for organizations in reducing entitlement management costs and complexity. It also reduces the risks of users having inappropriate access privileges and aggregating entitlements as they change job functions.

Role Engineering

As organizations start deploying IAM solutions, it is becoming increasingly important to devise a common set of roles that can be reused, over and over again, as opposed to defining roles every time an IAM component is deployed.

Role engineering is the process of defining roles and related information — such as permissions, constraints and role hierarchies — as they pertain to the user's functional use of systems, applications and business processes. Organizations often implement IAM systems based on a role-based paradigm without much consideration for roles. To minimize deployment effort or to avoid project scope creep, role definition is often not considered part of the initial project. Frequently, organizations also do not invest enough time to define roles in sufficient detail; rather, they tend to define high-level roles that do not reflect actual organizational job functions. The result is that additional efforts are required to manage job- and function-specific permissions manually, outside the IAM system. This often results in IAM systems not delivering the expected business value. The process of defining roles should be based on a complete analysis of how an organization functions and should include input from a wide spectrum of users, including business line managers and human resources.

Role Engineering Approaches

There are two fundamental approaches to role engineering: top-down and bottom-up. The top-down approach is primarily business-driven, and roles are defined based on the responsibilities of a given job function. Roles are defined by reviewing organizational business and job functions and mapping the permissions for each job function. This approach provides business oversight and alignment of roles with business functions and reusability.

Some key considerations for the top-down approach are as follows:

- Carefully define the scope and boundaries for the project.
- Identify enterprise access policies to determine entitlements for a given job function.
- Group users in a given business unit based on privileges corresponding to their job function.
- Make sure you do not have mutually exclusive roles assigned to the same person. For example, a person who creates a purchase order should not be the one who approves it.
- Lastly, consider role hierarchies which help simplify role definitions by aggregating roles.

The bottom-up approach is based on performing role-mining/discovery by exploring existing user permissions in current applications and systems. Once user permissions are explored, the next step is to perform role normalization and rationalization. One of the outcomes of this approach is that users often accumulate entitlements based on their previous job functions performed over a period of time; it can become too daunting to extract the entitlements without the business involvement. This is a key aspect of role rationalization to be considered as part of a bottom-up approach.

Finally, a hybrid approach can combine top-down and bottom-up approaches to leverage normalized roles derived from role mining and align them to job functions, with the involvement of business.

Summary

As organizations embark on various RBAC-oriented IAM initiatives, it is imperative for a successful role definition to have management support, sufficient funding for the role engineering effort, business unit participation and resources committed to the project. The importance of roles should not become an afterthought, but should be considered an integral part of any IAM initiative. Organizations also need to address requirements for roles from a compliance standpoint. Entitlement certification is becoming a critical aspect of various regulatory compliance initiatives. A holistic approach to role definition helps alleviate certification-related regulatory compliance challenges.

Role engineering is a key cornerstone in the process of defining roles that meet the organizational requirements. Once the roles are defined and an inventory has been published, it has to be maintained by both the business and IT, as this helps to keep the information current and available for any future IAM initiatives.

Srinivasan Vanamali, CISA, CISSP is a Senior Security Architect at CA — with more than 18 years experience in a variety of IT management and technical roles. His expertise includes key aspects of security including identity and access management, industry standards, deployment methodologies, compliance and technology vision.

For the latest issue of the 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](#).