An Oracle White Paper
July 2010

Wave Methodology: A Practical Approach to Defining Roles for Access Control

ORACLE

Executive Overview

Defining user roles as a way to manage access to computer-based systems is an efficient, effective alternative to managing access on a user-by-user basis—which can be virtually impossible when dealing with large numbers of dynamic users. To assist organizations in creating a role-based model for access control, Oracle has developed a wave methodology that separates users into manageable groups, or “waves,” for the purpose of defining roles.

Introduction

The need for access to organizational resources has grown dramatically in scope and complexity as the need to communicate and collaborate within and beyond the enterprise has grown. More and more users—employees, partners, even customers—require access. Making matters more complicated, the type of access they require often changes as their relationship to the organization changes. In this growing and dynamic environment, access control becomes a significant challenge. It’s no longer possible to manage access on a user-by-user basis when there are so many users with so many changing needs. Increasingly, the answer is role management.

Role management is the process of defining and assigning roles to individuals who require access to organizational resources, and then managing their access according to those roles. Creating roles based on usage and enterprise policies enables greater visibility and makes access more manageable, because access control is exercised against a limited number of roles rather than a large number of individuals. Role management is an efficient and effective way to address the challenges of access control for a large and constantly changing universe of users.

Overview: The Wave Methodology for Role Definition

Using roles as the basis for access control can make the process more efficient, but organizations must begin by defining roles for this purpose. In organizations that have large numbers of users with access spread across multiple applications, role definition can be a monumental task. This white paper will

- Introduce the wave methodology for role definition
- Describe in detail the steps for role definition prescribed by the methodology
- Suggest useful initiatives that can be put in place once a model for role definition has been identified

Oracle's wave methodology separates large numbers of users into more manageable groups, or "waves," for the purpose of defining roles. This is accomplished by first dividing users into business units based on their managers, departments, divisions, or other commonalities. These business units are then grouped into waves (usually four to six business units per wave), which are then prioritized based on the needs of the business. Each wave requires a seven-step process for role definition. Figure 1 summarizes the process; the remainder of this paper is primarily devoted to explaining the steps in greater detail.

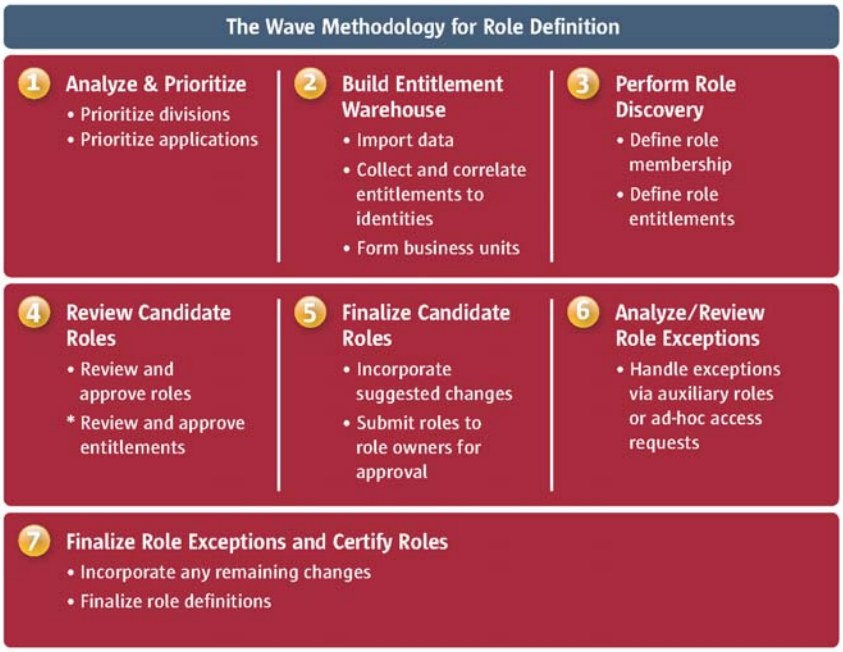

Figure 1. Oracle's wave methodology for role definition follows seven key steps.

Step 1: Analyze and Prioritize the Environment

This step requires a series of meetings with the role definition project team, and stakeholders representing IT and the various business divisions. The stakeholders are usually managers, department heads, and others who can add value to the role definition process with their knowledge of the

environment. During these meetings, the group defines the purpose of the project, develops an overview of the methodology, and identifies the best approach to prioritizing the environment. The overall prioritization exercise is primarily focused on business divisions and the applications that are utilized by those divisions.

Prioritization of Divisions

Business divisions are prioritized based on the following criteria:

- **Current cost of user administration.** The greater the need to reduce the cost of administering users in a division, the higher that division is prioritized. This greater need is demonstrated by the following criteria:
  - **Number of users.** A larger number of users within a division generates greater pain in user administration activities.
  - **Number of human resources (HR) events.** A larger number of new hires, rehires, transfers, and terminations generates more user administration activity.
  - **Access criticality.** Some divisions are absolutely necessary for the operations of the company. Access must be granted to individuals from this division first to support the core operations of the business.
- **Ease of implementation.** Role definition is typically easier for divisions that have very clear demarcations of job functions. The easiest divisions are dealt with first in order to provide a quick return on investment. This also provides useful experience when dealing with more-complex divisions. The following criteria are used to determine the ease of implementation:
  - **Number of different job functions.** The ratio of the number of users to the number of job functions provides a good metric to determine which division will entail the easiest role-definition task. The higher the ratio, the easier it is to define roles for that division.
  - **Stakeholder availability and influence.** The stakeholders must allocate time to the process. It is imperative to determine the best months for stakeholders to work with role engineers. The stakeholder must also have sufficient influence to summon the resources necessary to complete the task. This includes reviewing and approving the roles, as well as gathering and coordinating the data (user and entitlements) necessary to perform role mining.
  - **Number of applications in use.** It is important to determine the number of applications used by a division. The fewer applications, the easier it is to define roles for the division.

Prioritization of Applications

The prioritization of role definitions for specific applications is driven by the prioritization of divisions and based on the following criteria:

- **Current cost of user administration.** The greater the need to reduce the cost of administering users for an application, the higher the priority that application has for role definition. This greater need is demonstrated by the following criteria:
  - **Number of new accounts created/modified/deleted per month.** Automating the user administration activities for applications that have a higher user administration cost generates a higher ROI.
  - **Number of individuals who use the application.** The larger the number of application users, the greater the ROI will be when access is automated.
  - **Average timeframe for provisioning.** If the provisioning activity on an application is very time-intensive, the role-based model will reduce the time frame and provide a greater ROI.
  - **Frequency of use.** If an application is used more frequently than others, it should be given a higher priority for role definition.
- **Application security profile.** The higher the security and risk profile (and therefore, the greater the need for stringent user access controls), the higher priority the application is for role definition. A high security and risk profile is demonstrated by the following criteria:
  - **Sensitivity of application (potential risk of untimely removal of idle/expired accounts).** If the application is classified as sensitive, it requires more-stringent security controls and must be higher in priority.
  - **Criticality to Sarbanes-Oxley (SOX) compliance.** If an application is SOX-critical or classified as a payment card industry application, it should be given a higher priority.
  - **Length of existing certification process.** If performing user access reviews is especially time-consuming, a role-based system can reduce the time and provide a higher ROI.
- **Ease of implementation.** Role definition is typically easier for applications that have a process for extracting user access data, a designated subject matter expert, and a designated owner. It is also easier to define roles for applications that have built-in roles and a smaller number of access levels.

Based on the information gathered about the business drivers, overall security strategy, organizational context, and the internal IT landscape, you can develop a plan for defining roles that targets the areas that will maximize the positive impact to the business and shorten the time necessary to achieve ROI.

Step 2: Build the Entitlement Warehouse

Once the environment has been prioritized and the initial divisions and applications have been identified, the next step is to build an entitlement warehouse to serve as a repository for the HR profile data (such as name, job function, department codes, and location) for each user associated with the relevant divisions and applications. This data should be obtained from an authoritative source, for example, an enterprise directory or HR application. Once the profile data has been collected, the next step is to collect the entitlements and correlate them to the identities within each application. Initially,

this may be done for a handful of applications or for one large application such as an enterprise resource planning (ERP) system.

Figure 2. Step 2 is to build the entitlement warehouse, a repository for HR profile data for users.

Once the data is imported and correlated, the users are divided by their respective business units. A business unit is a logical grouping of users such as a department, a subgroup within a department, or a group of departments. Organizational hierarchy can also be used to determine business units. The goal is to form a group of users that is a manageable size.

Optional Step: Perform Access Certifications

Once the entitlement warehouse has been populated, you may want to initiate an access certification process in which you review each user and their associated accounts. This step is not only a critical access control; it also cleanses the user and entitlement data prior to defining roles.

Step 3: Perform Role Discovery

During this step, a set of roles is discovered for the business units you are working with. When considering how to discover roles, there are three general approaches.

- **Top-down.** This option approaches the process from the perspective of what a user needs access to, based on the user's HR attributes, context in an organization, and what is determined appropriate by the user's managers. This methodology is used traditionally when no tools are available to analyze a user's actual access.
- **Bottom-up.** This approach evaluates the access assigned to users in each application and then clusters users based on their similarities. Although generally more successful than the top-down approach, this method is very cumbersome when performed manually.
- **Hybrid.** The hybrid approach to role definition has been the most successful approach. It takes into account user context information—such as manager, location, job title, and job function(s)—in conjunction with the actual access held by the users, providing a holistic view of the users that have similar access as well as insight as to why (such as similar job function, location, or manager).

No matter which approach is used for role discovery, there is consensus that the traditional method of using spreadsheets for defining roles is ineffective, time-consuming, and very expensive. The good news is that there are a number of tools available today that have made the process more efficient and effective. For instance, Oracle Identity Analytics provides automation for all three approaches.

The wave methodology for role definition utilizes the hybrid approach and assumes that you have a role management tool to aid you in this process. The top-down portion of this approach is encompassed in step 1, as well as in the HR data incorporated in the entitlement warehouse created in step 2. This information is used to determine which users should be included in a particular iteration of the role definition process. The bottom-up portion of this approach is captured in a process called role mining. In role mining, clustering and categorization algorithms are applied to a set of user data to define a set of possible roles. The role management tool should also provide analytics to aid in deciding the level of access associated with each role, based on the percentage of users who hold that level of access. The role-mining process typically occurs in two phases that are distinguished by the applications incorporated within each step.

Role Mining Phase 1: Define Role Membership

During the initial phase, a subset of the user population is segmented based on the HR attributes (such as job code or job title) captured in step 2, and only those applications that are the most critical to that particular group of users are included. This places the focus on identifying which users should be included as members within the candidate roles. By limiting the number of applications (and therefore, the entitlements incorporated in the mining process), noise is reduced in the mining results. The candidate user population is typically segmented based on HR attributes (such as job code or job title) captured in step 2. Tool analytics can show the percentage of users who have access to a particular application, making it easier to determine which applications to exclude. For instance, a policy may be set that applications should only be included if at least 80 percent of the users have access to the application.

Role Mining Phase 2: Define Role Entitlements

The goal of this phase is to finalize the set of entitlements that should be included within a role definition. As in the first phase, analytics will help determine which entitlements from each application should be included in the role definition—based on the percentage of users to whom the entitlement is currently assigned. The combined analytics allow you to decide (down to the individual entitlement level) whether an entitlement should be included in the definition of the role. Again, policies can be set that dictate whether to include an entitlement, based on the percentage of users who currently have that level of access.

The following sample reports and screenshots contain the type of information that should be generated as a result of the role-mining exercises performed in this step. This information is critical in supporting the decisions that will be made in the next step.

Oracle Identity Analytics lists all the applications contained within a defined role, along with the percentage of users who have access to those applications. It also provides the data necessary to determine which applications should be included in a defined role.

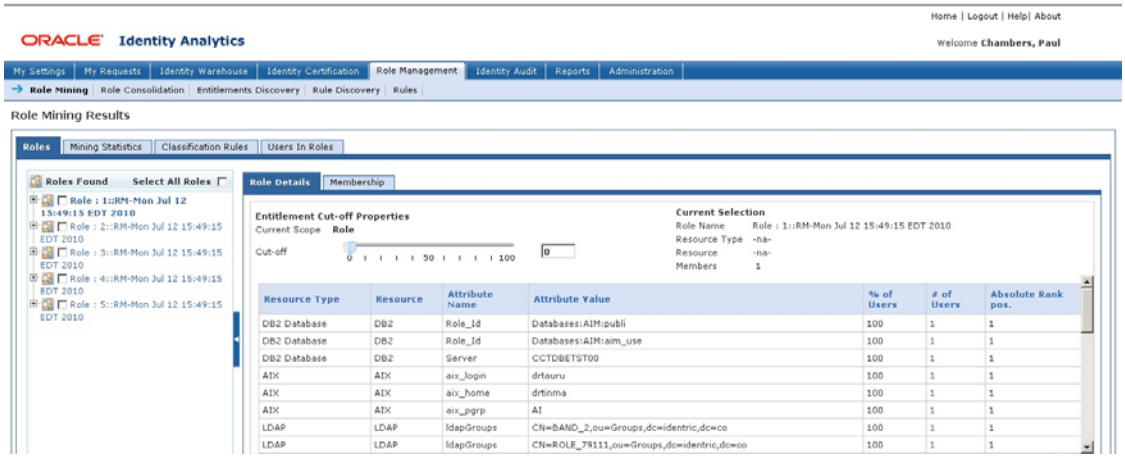

Figure 3. Oracle Identity Analytics's Role Discovery feature lists all the applications within a defined role and the percentage of users with access to those applications.

Oracle Identity Analytics generates reports, such as the one shown in Figure 3, that list all the entitlements encompassed within each role.

Step 4: Review Roles

During this step, the stakeholders identified in step 1 are asked for their feedback about the role definitions created so far. These review meetings are sometimes referred to as workshops and are an important component of the wave methodology. In fact, the key to a successful role definition strategy is to ensure that all stakeholders are involved in the review process. But because roles can contain access or entitlements from a number of applications across disparate business units, it can be extremely difficult to obtain feedback from each stakeholder individually.

In a workshop, the stakeholders begin by reviewing and approving role membership. Approval is not automatic of course; changes can and should be made during the meeting with the aid of the role-to-user report and the role analytics tool.

Once the role members are finalized, the next step is to define the metadata for each role: name, description, and owners. Of particular importance here are role owners, who will be responsible for the final approval of the roles, as well as for ongoing approvals and certifications during the maintenance phase of overall role management.

The stakeholders next review and approve the entitlements included within the definition of each role. Stakeholders can use the role entitlement report to gain a better understanding of the entitlements included within each role. They can then make suggestions for fine-tuning the access, based on their knowledge of what is required for the users in that role.

Optional Step: Define Role Assignment Rules

At this point you might choose to define role assignment rules. Role assignment rules encapsulate the business logic that determines whether a role should be automatically assigned to a user. These rules

most often include logic that detects one or more HR-related attribute. For instance, a role assignment rule may assign the role "Financial Analyst 1" if the user were assigned the value of "FA Level 1" for their job code attribute. Any combination of attribute values can constitute a rule and any combination of rules can be applied to a particular set of users. These rules are generally evaluated during the automated provisioning process.

Optional Step: Define Separation of Duties Policies

You may also choose to discuss potential separation of duties (SoD) conflicts among the roles and entitlements during this step. SoD conflicts can occur at the role level or at the individual entitlement level. Once potential conflicts are identified, audit policies can be created that will check whether two conflicting roles are assigned to the same user. The role management tool should provide the means to both define the policies as well as apply them to the enterprise environment on an ongoing basis. Although this process can be done outside of the role definition process, it is useful to do it at this point because the stakeholders who identify and define these policies should be participants in the role definition process.

At the conclusion of step 4, suggested changes not executed during the workshop are collected and documented as action items for the next step in the methodology.

Step 5: Finalize Roles

During this step, any of the remaining changes to the role definitions suggested during the workshop are incorporated. Once these changes are implemented, and once the role metadata is associated with the roles, the roles are submitted for approval to their assigned role owners. The role management tool is responsible for automating this entire process and auditing the approval decisions.

Step 6: Analyze and Review Role Exceptions

Once each role has been approved, the next step in the methodology is to review any access assigned to users that falls outside of the definition of their assigned roles. During this review, you can either remove the access from the user or allow the access as an exception to the role model. The role management tool should provide a report or other mechanism to view access that falls outside of the assigned roles.

It is important to keep in mind that although a role-based approach to access control is an effective method for controlling and managing the access users have within an organization, it is impossible to define a role that covers every assignment need of an entire organization. The enterprise environment is simply too dynamic to be constrained by a static definition of access. Because of this, exception cases are created for users whose access may not fit neatly into one of the roles. This methodology provides two options for handling these exception cases.

Option 1: Auxiliary Roles

The exceptions can be handled within a role by including an auxiliary role. Roles defined within the model can be associated with a base role (or parent role), and also with an auxiliary role that contains those "one-off" entitlements that do not fit neatly within the defined model. For instance, a user with a special job function can be assigned a base role along with an auxiliary role, which provides the user with the special access required, based on the circumstances. As a best practice, auxiliary roles are defined if the extra access is needed by more than two or three users who are a part of the base role.

Given the ongoing cost of managing roles within an organization, one of the overall goals of the role-definition process is to minimize the number of roles defined for an organization. With this goal in mind, the auxiliary role approach may not be the best method for handling exceptions. In fact, if administrators are not careful, this approach can lead to role explosion.

Option 2: Ad Hoc Access Request

Another option is to include the exceptional access in the ad hoc access request process. In this option, the exceptional access is made available by request in the tool used to automate the access request process. In most cases, this option is (or should be) a part of the user-provisioning application. But it could also be included in a solution that has been built in-house or incorporated within the service desk application. Regardless of where the functionality lives, the exceptional access would be made available in the user interface of the request tool that assigns access to users. This access could be granted through the applications that are used by a population of users, or it could be made available for assignment to all users. For instance, entitlements that grant specific access within the financial reporting application may be restricted to those users who are members of the finance business unit.

Step 6 is one of the most important steps in the wave methodology, since it allows the business to remove unwanted access that has been accumulated over time by users. It is also important from a compliance perspective and it is central to enforcing the concept of least privilege.

Step 7: Finalize Role Exceptions and Certify Roles

In this final step, any remaining changes from the previous steps are made and the role definitions (membership and entitlements) are finalized. Also, role exceptions are either removed or approved, based on the decisions made in the previous step.

The final action in this step is to launch the role-certification process, which periodically reviews and approves the entire role model. During these reviews, each role is reviewed by the role owner for accuracy and approved or disapproved based on a point-in-time snapshot of the role. These decisions are captured and audited within the role management tool to ensure that the role model is working as expected. For the first certification, you secure the final approval necessary for the changes incorporated during this step, and establish a baseline for subsequent role certifications. By providing a baseline for comparison, it is possible to highlight only those roles that have changed since the last review, which can streamline the entire process.

Looking Ahead

After the process of role definition is complete, organizations must follow up with subsequent processes to ensure that the reliable data entered in the role-definition process is protected and reviewed as the organization continues to evolve.

Role-Based Provisioning

Once a role-based model has been defined, a logical next move is to leverage that model in the user-provisioning process. At the very least, this involves exporting the role definitions for the access-request process. If role assignment rules have also been defined, these rules should be accessible to the process responsible for automatically assigning access. Once this is accomplished, the roles become more than just an aid to reporting and access control compliance—they become a means for simplifying and streamlining the process of assigning and managing access within the enterprise.

Role Governance

Once a role model has been defined, it is important to institute a governance model for managing and maintaining the roles on an ongoing basis. Roles, like identities, are not static and must be managed through a disciplined change-control process. Based on our experience in helping companies adopt a role-based model for access control, we have also pioneered a procedure for defining, implementing, and administering a role-governance body. Although the topic of role governance is beyond the scope of this paper, it should be noted that a role governance board is a cross-functional oversight body whose primary objective is to ensure that the appropriate policies and procedures are followed for the creation, modification, and deletion of roles.

Conclusion

As the number and type of users who require access to organizations' computer-based resources continues to climb, the traditional method of managing user access on a case-by-case basis has quickly become antiquated. Further, users within and outside the company must not only access resources, they must contribute to the development of those resources, unhindered by slow access controls. The process of managing the complex web of user access is a critical matter of security and a never-ending maintenance task as well.

Based on years of experience in helping companies adopt a role-based model for access control, Oracle's wave methodology for role definition has proven to be an effective method for engineering roles. This seven-step process walks administrators through 1) analyzing and prioritizing the divisions and applications most urgently requiring access controls, 2) building a warehouse to store data critical to effective role definitions, 3) performing role discovery, 4) defining rules and policies for roles, 5) finalizing roles, 6) analyzing and reviewing exceptions to the rules, and 7) finalizing role exceptions and certifying the defined roles.

While some of the steps outlined in this methodology can be accomplished without the aid of technology, it is virtually impossible to accomplish all these steps without the aid of a tool such as Oracle Identity Analytics.

Wave Methodology: A Practical Approach to Defining Roles for Access Control
July 2010

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com