Erin Putrah
System Architect

Universal Content Management

A Security System for Unstructured Data

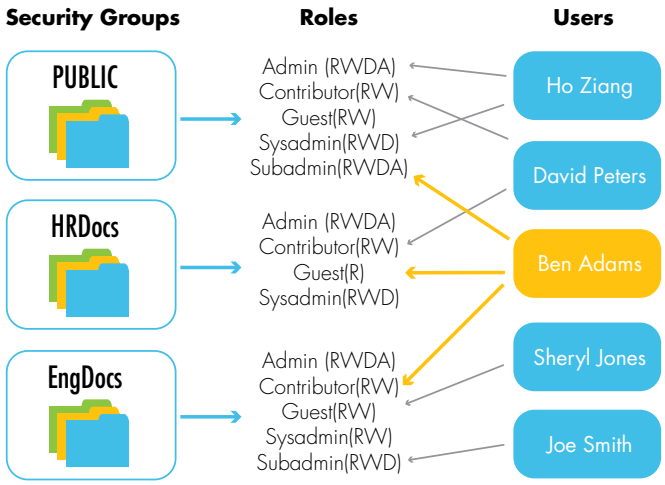
For years organizations have struggled with managing their ever-growing collection of unstructured data. Today, Oracle has content management solutions that enable organizations to maximize the value and reduce the risk of maintaining unstructured data primarily because of security.

In contrast to a file system, where anyone can drag and drop documents and security is limited, Oracle's Universal Content Management allows users to add metadata to documents that can be used not only to better locate the document, but also to secure the document.

Security within UCM operates at the document or content level. The first step in securing content occurs upon entering the document into the system. When an item is checked into the system, certain metadata information is required, one of which associates the document to one specific security group. While UCM comes with two out-of-the-box groups, additional groups are easy to add. The next step is permissions and roles. Permissions consist of capabilities, including read, write, delete and admin. Roles are groupings of permissions. Some roles might have read and write capabilities and other roles might have admin rights. Once roles and permissions are associated, the fourth step to document security is to assign users to roles.

Let's look at an example to demonstrate the first four steps of securing a document. Ben Adams, in Figure 1, has a Subadmin role in the public group, which means he has read, write, delete and admin capabilities. As well, Ben has the role of Guest for the HRDocs security group, which means he simply has read capabilities. Ben's third role is as a Contributor to the EngDocs group, which gives him read and write capabilities. If Ben does not have at least read access to a document, he'll never know it's in the system because it won't return with any of his search results. So, that document is not only secure, but it is also not cluttering up Ben's search results.

The fifth and final step of document security is UCM system authentication. UCM dynamically allows



association to external lightweight directory access protocol (LDAP) stores, such as Oracle Internet Directory (OID) or Active Directory (AD). Upon login, UCM queries the external store directly to verify access rights. The ability of UCM to integrate with an external store enables organizations to maintain a single point of administration for all enterprise application credentials.

Having covered the five steps to implementing UCM's document-level security, I'll leave you with this parting wisdom. When configuring UCM's internal security, it is vital to plan out all security groups, permissions and roles prior to system implementation in order to ensure that every situation is handled. Groups, permissions and roles can be added after the initial implementation, but will affect the system's efficiency. Also, be aware that the number of security groups, roles and accounts can impact system performance, so it's best to use a minimalist approach. System performance is impacted by security, because every time a search is run, a user's permissions must be deciphered before results can be returned and the user will notice any slowdown. Use the following equation to understand how adding security groups can slow down the system: (# of security groups) X (# of roles) / 1000 = time of operation in seconds. Ultimately, UCM's internal security is a very powerful tool, and with careful planning, enables UCM to serve as a security system for an organization's unstructured data.