Subject: Re: RBAC and LDAP
Posted by dennisj on Fri, 03 Nov 2006 09:56:55 GMT
View Forum Message <> Reply to Message

Tony, thanks for your response again.

I don't think I was suggesting a replacement of your RBAC system with LDAP, more suggesting something along the lines of using an LDAP server instead of an SQL server for the data that relates to users and roles. I think you mentioned that you have DAO's to facilitate Database independence for the RADICORE system. A custom DAO that talks LDAP not SQL -for user and role information- might theoretically be possible.

However, I can see that the question of assigning tasks to roles in LDAP would not necessarily be entirely straight forward.

Both Firefox and IE can access a user's desktop operating system logon credentials and use these to log on to remote (eg LDAP connected) servers. Some Mozilla documentation is here http://www.mozilla.org/projects/netlib/integrated-auth.html , and more tips here, http://www.cauldwell.net/patrick/blog/PermaLink,guid,c7f1e799-c4ae-4758-9de7-5c3e7a16f3da.aspx . I tested this today in Firefox, I set the network.automatic-ntlm-auth.trusted-uris setting to our Institute's Sharepoint server, and was able to log on with out being prompted for any further credentials, apart from the original OS logon.

But I think the main point here is not the single-sign-on sharing of operating system credentials, but the concentration of identity and role management in one place, an LDAP enabled server, so a large part of this identity data does not have to be duplicated in two different places.

Dennis