Subject: RBAC and LDAP
Posted by dennisj on Wed, 01 Nov 2006 22:42:18 GMT
View Forum Message <> Reply to Message

Hi,

I have just come across RADICORE and am not a coder but an IT administrator. I have searched the RADICORE and Marston sites, and the Forums for 'LDAP', but have found very few references.

LDAP is often used for something similar to RBAC, and many web applications implement some form of LDAP support for access and control.

What is the relationship between, or potential relationship between, RADICORE's Menu and Security sytem and a directory that implements an LDAP interface (such as Active Directory)?

Thanks

Dennis

Subject: Re: RBAC and LDAP
Posted by AJM on Wed, 01 Nov 2006 23:08:51 GMT
View Forum Message <> Reply to Message

I have never used LDAP, but from my understanding it is used to provide a single logon to multiple desktop systems.

The problem with a web application is that it only knows what the web browser sends it, and the web browser has no way of obtaining the client's LDAP details and sending them to the web server. There is no way that an application running on a web server has access to whatever LDAP system is being used on the client, so I think any relationship between Radicore and LDAP would not achieve anything useful.

Subject: Re: RBAC and LDAP
Posted by dennisj on Thu, 02 Nov 2006 07:16:29 GMT
View Forum Message <> Reply to Message

Tony,

Thanks for the response.

I have minimal experience with LDAP and Web applications.

1/. Moodle http://moodle.org a php MySQL learning management system. If you turn on LDAP authentication, and point the Moodle application at your LDAP server, then, when a user clicks to logon, it takes the entered credentials and asks the LDAP server, over an LDAP connection, whether that user is allowed to proceed.

2/. An apache server can have the mod_auth_kerb module installed http://modauthkerb.sourceforge.net/ . "Mod_auth_kerb is an Apache module designed to provide Kerberos authentication to the Apache web server. Using the Basic Auth mechanism, it retrieves a username/password pair from the browser and checks them against a Kerberos server as set up by your particular organization." The Kerberos connection can talk to an LDAP server.

Because there is a bit of pressure to centralise identity and permissions management in an LDAP server, it would be great if there was some way for your security system to interact with LDAP.

As I said in my original post I'm not a coder. There is a general article here on this topic...
http://www.list.gmu.edu/confrnc/ifip/i01-kluwer01-jpark.pdf
ROLE-BASED ACCESS CONTROL ON THE WEB USING LDAP

The abstract reads...
This paper gives a framework for how to leverage Lightweight Directory Access Protocol (LDAP) to implement Role-based Access Control (RBAC) on the Web in the server-pull architecture. LDAP-based directory services have recently received much attention because they can support object-oriented hierarchies of entries in which we can easily search and modify attributes over TCP/IP. To implement RBAC on the Web, we use an LDAP directory server as a role server that contains users' role information. The role information in the role server is referred to by Web servers for access control purposes through LDAP in a secure manner (over SSL). We provide a comparison of this work to our previous work, RBAC on the Web in the user-pull architecture.

Dennis

Subject: Re: RBAC and LDAP
Posted by AJM on Thu, 02 Nov 2006 09:47:02 GMT
View Forum Message <> Reply to Message

The problem with this is that it requires software on the client which captures your logon credentials from the operating system so that it can be automatically passed to the web server when you enter the logon screen. That ability does not exist in any web browser, and I'm not sure if it can be done with javascript (which I do not use in Radicore), or whether it can only be done with an ActiveX control (which I also do not use n Radicore).

Even if I could use LDAP to provide a user's login identity I certainly would not use it as a replacement for my RBAC system. LDAP knows nothing of my user roles and tasks and knows

nothing about assigning tasks to roles.

You may have read somewhere that using LDAP is "cool", but unless you know and understand the technicalities you will not realise that it also has its down side.

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,c7f1e79
9-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

Subject: Re: RBAC and LDAP
Posted by AJM on Fri, 03 Nov 2006 10:19:20 GMT
View Forum Message <> Reply to Message

Radicore already has its own system for user authentication, user roles and access contol, and there would be no advantage in replacing this with one of many possible external LDAP alternatives. It would create more problems than its solves, therefore it is not something that I would want in my software.

LDAP may be "cool" but it is also impractical.

Subject: Re: RBAC and LDAP
Posted by dennisj on Sun, 05 Nov 2006 21:27:52 GMT
View Forum Message <> Reply to Message

Thanks again for your reply.

Leaving aside the question of using LDAP as the base user database, I wonder what your suggestion would be for a organisation that currently has all its users, passwords, and group permissions stored in an LDAP server? If the organisation was interested in RADICORE, what approach to user management would you suggest?

Is there some way of synchronising the user names and passwords between RADICORE and LDAP? Or would you just have to maintain two separate, duplicate user name and password databases? Or is there some other alternative?

Dennis.

Subject: Re: RBAC and LDAP
Posted by AJM on Sun, 05 Nov 2006 21:49:17 GMT
View Forum Message <> Reply to Message

Radicore requires that users, roles and permissions are stored in its own database tables, and the functionality that this provides cannot be duplicated with an external LDAP system. If implementing an LDAP interface means a loss of functionality then I'm afraid it is LDAP that would be shown the door.

If you absolutely need an LDAP interface then you could always get one of your own programmers to write one, but I wouldn't be prepared to guarantee the results.

When you consider all the other features that the Radicore framework has to offer, the lack of an LDAP interface is pretty insignificant.

Subject: Re: RBAC and LDAP
Posted by edortizq on Wed, 27 Aug 2008 15:42:09 GMT
View Forum Message <> Reply to Message

Congratulations for this great product!
I was concerned about how to use LDAP authentication with Radicore, it seems important for business to have only one authentication method for it's computer systems.
PHP provides interfaces for LDAP, I think it could be used for develop an asynchronic interfase between LDAP and Radicore, wich could permit to import LDAP users to Radicore's menu system, something like Openfire has implemented, it allows to user select the authentication method, propietary or LDAP.
Do you think it's possible for Radicore's future versions??

Subject: Re: RBAC and LDAP
Posted by AJM on Wed, 27 Aug 2008 16:28:39 GMT
View Forum Message <> Reply to Message

Radicore already has two authentication methods:
Single Factor, which is the default, which uses the user_id and password on the MNU_USER table.
Two Factor, which verifies the password against a RADIUS server, as documented in http://www.radicore.org/viewarticle.php?article_id=111
How would the introduction of an LDAP option be supposed to work?

As I have never used an LDAP service, nor have access to one, I would have nothing to test against.

Subject: Re: RBAC and LDAP
Posted by edortizq on Wed, 27 Aug 2008 21:31:51 GMT
View Forum Message <> Reply to Message

The solution for LDAP connection could be something like your RADIUS connection.
Or, you can import users from LDAP database and write them as read only in your menu system (for certain fields), then those users can be part of the RBAC system the same way you work it now.
You can find an attached script for connect and recover atributes and values from ldap database, it works for OpenLdap and W2K Active Directory.
If you can't get access to a Ldap connection, let me know, I could ask for some friend and maybe (just maybe) get access for test purposes.

File Attachments
1) ldapTest.php, downloaded 2150 times

Subject: Re: RBAC and LDAP
Posted by AJM on Wed, 27 Aug 2008 22:00:13 GMT
View Forum Message <> Reply to Message

Importing user information from an LDAP database is not a viable option as the Radicore framework requires more information on each user than is held in the LDAP system. It is not possible to relpace to the contents of the MENU database with an LDAP database.

Subject: Re: RBAC and LDAP
Posted by edortizq on Thu, 28 Aug 2008 18:19:14 GMT
View Forum Message <> Reply to Message

Good point, and what about an option like "Create user from LDAP", where you can connect to

LDAP server and select from there the user wich you are creating in Radicore??

Subject: Re: RBAC and LDAP
Posted by AJM on Thu, 28 Aug 2008 19:08:24 GMT
View Forum Message <> Reply to Message

That doesn't sound practical to me. Not all entries in the LDAP system would necessarily be users in the Radicore application, so it would be easier to create users manually (as at present) than to build a new screen which lists new entries on the LDAP system and then allows the user to select which ones should be copied across. Besides, there is still information in the Radicore database that would still have to be entered manually as it does not exist in the LDAP system and therefore cannot be copied across.

Using an LDAP database in place of Radicore's MENU database simply won't work, so it won't happen.

Subject: Re: RBAC and LDAP
Posted by AJM on Sun, 31 Aug 2008 13:31:41 GMT
View Forum Message <> Reply to Message

I have found an LDAP server which I can install on Windows XP and test against (see http://directory.apache.org/) so I will be able to implement LDAP authentication similar to what I have already done with RADIUS authentication.

In this way the user will still have an entry on the MNU_USER table, but the password will be authenticated against the LDAP server. The user_password field on the MNU_USER table will therefore be irrelevant.

This will be available (hopefuly) in release 1.40.0

Subject: Re: RBAC and LDAP
Posted by edortizq on Sun, 31 Aug 2008 20:54:03 GMT
View Forum Message <> Reply to Message

Thank you!! it will very useful.