

Re: Openldap to AD

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-01/msg02103

- *From:* Michael Ströder <michael@xxxxxxxxxxxxx>
 - *Date:* Fri, 26 Jan 2007 19:41:45 +0100
-

Al Mulnick wrote:

How are the passwords stored in your OL implementation?

If passwords are hashed there is no way to bring them into AD.

I'm thinking that it may be easier to at least one-way sync from OL to AD. You could roll your own or purchase a 3rd party package. Products range in price from free to inexpensive to blow your socks off expensive. Typically, the really expensive ones will offer something that does password sync bidirectionally.

Generally it's not a big deal to implement a robust syncing with your favorite scripting language and the accompanying LDAP module.

Which version of OpenLDAP is this? If it's 2.3.x and you need fast syncing it would be worth to look into the syncrepl protocol and implement that (see RFC 4533).

- 1) are you sure you want to sync passwords?
- 2) Really? Do you want to sync passwords or would it be better to do away with one of the directories altogether and just standardize on the other?

Also you can integrate AD's Kerberos with OpenLDAP. Or chain the LDAP simple bind request to OpenLDAP to AD. But this is some configuration work and requires user sets to be the same and recent version of OpenLDAP. Since this is off-topic here you might want to check out the openldap-software mailing list.

Ciao, Michael.

.