

## Re: Integration issues...

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2006-08/msg02888](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-08/msg02888)

---

- *From:* "Mark" <[mlockett@xxxxxxxxxxxx](mailto:mlockett@xxxxxxxxxxxx)>
  - *Date:* 25 Aug 2006 13:48:05 -0700
- 

Thanks very much Joe. This does sound like a lot. I have read a lot of documentation and it doesn't sound clear as to whether or not these applications will do what I am looking for. I may just have to create a lab and set these up and investigate more.

Thanks,  
Mark

Joe Kaplan wrote:

This is exactly the type of problem that federation and ADFS wants to solve, but it probably won't work for you unless the HR app is a web application and it supports federated logon with the WS-Federation protocol. If those were both true, you could set up ADFS on both forests and it would work.

In the meantime, I think the quickest solution might be to provision accounts for their HR reps in your AD. If you don't want them in your AD, then you could potentially provision accounts in an ADAM database for them. Then, you would need to either create bind proxy objects for your users in ADAM so they could authenticate with their domain credentials using an LDAP simple bind. If the app can support both LDAP secure and simple binds, then you could avoid the bind proxy objects, but that doesn't sound likely based on your description.

In order for the other domain users to have the same passwords in ADAM, you would need some sort of a sync mechanism. I believe MIIS could provide that, but I'm not an MIIS expert.

I hope that helps give you some ideas. There is a fair amount here to come up to speed with, so good luck!

Joe K.

--

Joe Kaplan-MS MVP Directory Services Programming  
Co-author of "The .NET Developer's Guide to Directory Services Programming"  
<http://www.directoryprogramming.net>

--

Re: Integration issues...

"Mark" <mlockett@xxxxxxxxxxxx> wrote in message  
[news:1156508930.553264.259690@xx](mailto:news:1156508930.553264.259690@xx)

Thanks guys. To expand a little more, we have an HR database application that uses LDAP for authentication. We have it pointed to our root domain currently where all of our child domain users can authenticate to. My company has now purchased a new company that has their own IT staff and standard procedures that are not a match to ours. Therefore, we do not trust their domain at this point. It may happen in the future, but not for now. We do however pay them and they need to be able to log into this HR application to view all their information. The application does not allow you to point to multiple LDAP sources. Is this something ADAM with MIIS could help solve or is there a better solution out that I have not found? Thanks again for the replies and help.

Mark

Joe Kaplan wrote:

ADAM won't really help much with two untrusted domains unless something like MIIS is used to sync the passwords from both domains into ADAM. ADAM has the ability to authenticate users in AD via passthrough and bind proxy auth, but you could only do one domain at a time this way.

If the OP has the ability to control the code that is doing the LDAP auth, the poor man's solution would be to try LDAP auth against the first domain and then try the second one. I've seen a few apps that handle things this way. ADFS actually uses a mechanism like this to support both AD and ADAM user stores.

Joe K.

—  
Joe Kaplan—MS MVP Directory Services Programming  
Co—author of "The .NET Developer's Guide to Directory Services Programming"

Re: Integration issues...

<http://www.directoryprogramming.net>

---  
"Paul Williams [MVP]" <ptw2001@xxxxxxxxxxxx> wrote in message

[news:%23\\$%vLiZ8xGHA.2396@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](news:%23$%vLiZ8xGHA.2396@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Can you expand on your requirements? Do you want to have these applications interoperate with both AD domains? I can't see what you want to do, or how ADAM will help, unless you wish to synchronise two directories into one unified view to present to the application.

---  
Paul Williams  
Microsoft MVP – Windows Server –  
Directory Services  
<http://www.msresource.net> |  
<http://forums.msresource.net>