

Re: Query AD from DMZ via LDAP?

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-04/msg00420

- *From:* "Joe Kaplan" <joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 9 Apr 2007 17:04:31 -0500
-

You don't really need ADAM for this unless you need LDAP simple bind, as you can bind to the DC that trusts the internal DC to do the authentication. Getting group membership is likely going to be hard no matter what.

If you can do secure LDAP through the firewall, that simplifies things greatly. Having a separate forest for this when you don't need it for anything else doesn't make a lot of sense. Of course, if you are going to use that forest as your hub for policy and patch management in the DMZ, then maybe you need it anyway.

Remember that ADAM isn't an LDAP proxy, in that it doesn't forward general queries to AD. It can do pass through authentication and bind proxy authentication and it can also build a logon token for the pass through authentication user that you can query to get group SIDs (read tokenGroups constructed attribute from the "rootDSE" object), but it might not give you exactly what you want.

Keeping it simple sounds good to me too.

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>

--

"emde" <emdeusenet@xxxxxxxxxx> wrote in message
<news:1176148924.407651.29750@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Joe:

I plan on having ADAM installed in a domain controller where there is a forest trust to the internal domain. Would this work with the passthrough authentication? If so, it looks like this is my best option. Although the secure ldap thru the firewall is looking very attractive at the moment :)

Re: Query AD from DMZ via LDAP?

On Apr 9, 11:35 am, "Joe Kaplan"

<joseph.e.kap...@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote:

You could use ADAM with passthrough authentication or bind proxy objects, but the ADAM server would need to be a member of the domain, so that may or may not be viable from a firewall perspective. Whether or not you use bind proxy objects depends on the type of authentication your app can perform. If it is limited to LDAP simple bind, then bind proxies would be needed (and a sync mechanism to populate them and keep them synced with the AD). If your app can do a Windows secure (GSS-SPNEGO SASL) bind, then pass through authentication will work.

ADAM might allow you get the group memberships as well, but it may be difficult to resolve the SIDs that ADAM would give you into friendly names unless you can actually query the source AD directory, so that might not help very much.

Another thing you might consider would be to poke a hole in the firewall to allow LDAP traffic through, perhaps limiting the traffic to port 636 (with SSL enabled on the AD server). That is probably the easiest way to go if it is an option.

ADFS could also be used to solve this problem, as it can provide authentication to apps on the public internet (among many other things), but it might be more than you want to chew off if you don't need federation services or don't need to integrate multiple directories (or you app can't use federation services easily due to how it is designed).

This is a pretty broad area here with multiple possible solutions, so my response is pretty broad too. However, I can hit more details on some of this stuff if you have more specific questions.

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>
—"emde" <emdeuse...@xxxxxxxx> wrote in message

