

Re: Recommended strategy for providing access to web apps via Inte

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-05/msg00711

- *From:* David Dixon <DavidDixon@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 11 May 2007 12:07:00 -0700
-

Thanks Joe, that is just the type of info I was looking for!

"Joe Kaplan" wrote:

LDAP is an ugly solution on the public internet, as it may require drilling holes in your firewall to allow an external organization to perform LDAP operations against your directory. It also exposes a much larger surface area of your directory than you really want or need to, as once you have opened the firewall up for LDAP, the external entity can execute ANY LDAP query, not just LDAP binds for authentication. Also, it is often difficult to get different technology stacks to talk to different LDAP directories as they all work a little differently and you can end up in a sticky integration mess.

These federated authentication protocols are designed to address these issues by using "web" standards like XML, PKI and HTTP to perform the protocol level integration and broker the trust between entities. They are designed just to perform the operations appropriate to the use case (authenticating users across organizational boundaries and providing limited sets of information about those users to business partners), so they don't expose a large, scary surface area.

People use LDAP all the time for doing authentication, but it is an ugly solution outside the firewall and across organizational boundaries.

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>

--

"David Dixon" <DavidDixon@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:D32F43A5-64CD-45BC-B09E-AF841046D9C7@xxxxxxxxxxxxxxxxxxxx

Re: Recommended strategy for providing access to web apps via Inte

Thanks for the information Joe, your response was really helpful to me!
Any thoughts on why Microsoft does not recommend using LDAP for AD authentication?

Thanks again!

"Joe Kaplan" wrote:

I would probably suggest using ADFS as your authentication technology to provide this kind of access. It gives you a ton of flexibility with allowing access to web apps on the public internet to both your own employees and outside users.

If you need a secondary authentication store for external users, ADAM works well for this. ADAM also integrates with ADFS nicely, so you can work that into your solution.

If you need to access an externally hosted application and want to authenticate using your own identities, ADFS can work quite well for this too. Your external vendor would also need an ADFS infrastructure and would need to modify the app to work with ADFS (which may or may not be a big deal), but this can work. This is actually the primary mechanism our company uses for integrating identity with external vendor apps.

There is a fair amount to study to get up to speed with ADFS, but MS has written some decent docs. The Deployment Guide is lengthy, but pretty thorough.

Joe K.

--

Joe Kaplan—MS MVP Directory Services Programming

Re: Recommended strategy for providing access to web apps via Inte

Co-author of "The .NET Developer's Guide to Directory
Services
Programming"

<http://www.directoryprogramming.net>

--

"David Dixon"

<DavidDixon@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in
message

<news:6289AF49-64C0-4356-9D61-4B3BEB415DB6@xxxxxxxxxxxxxxxxxxxx>

My organization is beginning to look at providing a segment of the user population (not employees) access to certain web apps and data. These users are not physically in our offices, hence we would need to build a secure method to allow them to access these resources via the Internet. We also have at least one outsourced solution (which provides online discussion capabilities) that we want to control access to as well (preferably using AD authentication). What I mean by control access is that we need to ensure that only approved and valid users defined by us (i.e. are in AD) are allowed to access it.

That being said, here are my questions:

- 1) Is it generally a good idea to build an authentication solution that uses our internal AD for authentication? Would ADAM be a viable option?
- 2) For the outsourced scenario, would it be feasible to expect that we could provide a link to the outsourced site from a portal and force users to

Re: Recommended strategy for providing access to web apps via Inte

authenticate through the portal (using our internal AD for authentication) prior to accessing the outsourced site?

3) I am hearing that the vendor of the outsourced solution is pushing LDAP as a means to allow us to use our AD accounts for authentication purposes.

I have heard that generally Microsoft does not recommend using LDAP for authentication against AD. Is this true and if so, what are the primary reasons?

I am definitely knowledgeable of the Microsoft Platform and AD, but I am far from a guru in this arena. Any feedback on my questions or pointers to additional info would be greatly appreciated. Thanks!