

Re: AD & ADAM together in harmony

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2006-07/msg00050.html>

- *From:* "Anthony" <anthony.spam@xxxxxxxxxxxxxxxx>
 - *Date:* Tue, 11 Jul 2006 13:53:49 +0100
-

This is a really interesting problem, how to authenticate users on an extranet application. I don't have a fix for you, but a few thoughts. If you are authenticating internal users to the AD, then you are exposing the AD to that host. Once you have done that, you may as well give external users an account on your AD as well. I can't see the point of having a separate user database for external connections to an internal host. If you are worried about exposing the AD to the host, then you can use LDAPS to limit the risk. Using LOGIN authentication would achieve the same thing. You can also use authentication on the firewall or SSL VPN to authenticate external users safely before they get to the application. The most elaborate method is to have a separate domain for the DMZ, using Federation Services to keep the usernames and passwords in sync, but this is excessively complex.

Anthony

"GrITMan" <GrITMan@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:0654A1BF-CA02-4D21-B929-BEE67E005CCE@xxxxxxxxxxxxxxxx

We are planning on building an Intranet/Extranet for our payroll application. The idea is to use AD integrated IIS security for internal users to automatically identify and authenticate them on IE access, and use ADAM for clients.

The architecture will involve an internally hosted web server that will be available to internal users, plus we will publish these pages via ISA reverse proxy and SSL externally to the outside world.

The problem we have is figuring out how we go about switching from AD to ADAM during the authentication process? If, for example, the user does not authenticate automatically, how do we get it to check ADAM instead of popping up a username and password dialogue for AD? We have been told to use Forms authentication instead of IIS, but no

Re: AD & ADAM together in harmony

indication of actually how this would work or how to develop it.

The second option I have suggested to the dev team is to split the authentication physically into two separate pages, one for internal, one for external access. Thus we authenticate at the point of entry and then converge on single site content keeping that authentication in the session.

Again though, if we enable windows integrated security for the site, it applies to the whole site, so even if we authenticate external users up front with ADAM, further down the the line they will hit AD security somewhere and we're back to square one (even this is a guess, we're not sure how this will pan out)

What I want to know is a) are we going about this the right way? and b) if we are, how do we do this?

Any suggestions or advice will be welcome

Thanks

GrITMan