

Re: ADAM and Windows Address Book

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-09/msg01105

- *From:* "Rich Raffenetti" <raffenetti@xxxxxxxxxxx>
 - *Date:* Wed, 20 Sep 2006 19:51:59 -0500
-

Thanks. Could you tell me an example of the ADAMSync command that will create the user-->bindproxy conversions for me. I missed that. Thanks.

"Dmitri Gavrilov [MSFT]" <dmitrig@xxxxxxxxxxxxxxxxxxxx> wrote in message news:%23stEH2I3GHA.696@xxxxxxxxxxxxxxxxxxxx

WRT R2 ADAM -- sorry to disappoint you, but you have no reason to move to R2. ADAM SP1 and ADAM R2 are the same exact set of binaries. So, adamsync that you have will do user->bindproxy conversions for you.

--
Dmitri Gavrilov
SDE, Active Directory team

This posting is provided "AS IS" with no warranties, and confers no rights.
Use of included script samples are subject to the terms specified at <http://www.microsoft.com/info/copyright.htm>

"Rich Raffenetti" <raffenetti@xxxxxxxxxxx> wrote in message news:OG5HV442GHA.4796@xxxxxxxxxxxxxxxxxxxx

I understand from another posting that it is the R2 ADAMSync that will create bindproxies for me. I have been using the ADAM/SP1. I hope the documentation is updated!

Since we want to provide an ADAM as a secure alternative to punching holes in the firewall for AD, we are really playing to all platforms that have their own address book-like application. I would expect to serve many WAB users too, of course.

Our AD is the repository for all employee accounts, whether they be for Windows, Macintosh, or linux/unix. Most platforms have email systems that utilize an LDAP lookup. If I couldn't make it work for WAB, how could I serve the others.

My experience with one or two other address book applications is that they do well for anonymous lookups and not so well for authenticated

Re: ADAM and Windows Address Book

lookups. WAB is like that too. ;-)

However, with the proxied authentication that you refer to here, I would expect that the authentication will work better like WAB and we will use SSL/636 to protect the password and data stream.

Should I understand it that the new R2 ADAMSync will do the proxy setup for each account – avoiding the incredibly difficult process described in the ADAM/SP1 system? That would be great! (I don't appreciate what DirSync is.) :-)

I knew I had a good reason to move to the R2 ADAM. We just recently installed the R2 schema extensions in production! This is great news! :-)

"Lee Flight" <lef@xxxxxxxxxxxxxxxx> wrote in message news:uELwthv2GHA.4164@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

I have little to add to that other than:

ADAMSync will do AD user to ADAM bindproxy transforms for you (it just does DirSync under the hood).

Do you really need WAB as opposed to writing your own address book application. Spending some time with a copy of JoeK's book and rolling your own app might be a better investment than increasing your reliance on WAB at this time.

Lee Flight

"Joe Kaplan" <joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:eMN2NgO2GHA.1288@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Lee is a better guy to ask on sync options. I haven't done this yet. The bottom line is that you could write a program to do this for you and ADSI can support this, although not really well with script or VB6. You are looking at C++ or .NET 2.0, as you really need the DirSync control to do this well, and script doesn't (and won't) have access to this.

Re: ADAM and Windows Address Book

Most people would suggest you get a product that does this, but I'm not sure about the status of things like ADAMSync with respect to bindProxies. Last I remember, that wasn't supported but was maybe coming soon.

Basically, the bind proxy allows your users to hard code their AD credentials in the WAB settings in order to authenticate. The advantage here is not having to give out the password to a fixed account, but there are disadvantages too. If users change passwords in AD and forget to update WAB, WAB will stop working and will lock out their account if they try repeatedly (and you enforce pwd lockout). That creates a potentially costly support nightmare.

Another potential option to avoid the whole problem is changing ADAM to allow anonymous searches and ACLing the stuff in ADAM appropriately such that the anonymous user can see only the things you want them to in the address book. This is obviously less secure, but has a big upside in terms of both of the other two scenarios in terms of desktop management nightmares. Your particular requirements will have to guide you here. :)

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>

--

"Rich Raffenetti"
<raffenetti@xxxxxxxxxxxx> wrote in
message

Re: ADAM and Windows Address Book

news:uSrnfPO2GHA.5048@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

I read about the bindProxy objects and setting one up for each user and keeping them synchronized scares me a bit. Has anyone written an ADSI program (or equivalent) to create the bind objects? Of course, this wouldn't be necessary if WAB was fixed.

"Joe Kaplan"

<joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote in message

news:eIzZu5M2GHA.480@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Yes, the issue appears to be with the implementation of WAB and not a problem with ADAM or SSPI per say. SSPI is certainly capable of using the current thread's credentials OR using specific credentials, but WAB is not taking advantage of the latter for some reason, even though the UI would seem to indicate that

Re: ADAM and Windows Address Book

it would.

If specific credentials need to be used, it seems to me that the only solution for Rich is to create a service account in ADAM and use that (or create bindProxy objects for each user if it is important that each user use their own passwords). This would accommodate the simple bind case, which WAB seems to work with. Since SSL is in use, this would be secure.

Joe K.

--

Joe
Kaplan-MS
MVP
Directory
Services
Programming
Co-author
of "The

Re: ADAM and Windows Address Book

.NET
Developer's
Guide to
Directory
Services
Programming"
<http://www.directoryprogramming.net>

--
"Lee Flight"
<lef@xxxxxxxxxxxxxxxx>
wrote in
message
<news:uuGW43J2GHA.4484@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Hi

inline
below...

"Rich
Raffenetti"
<raffenetti@xxxxxxxx>
wrote
in
message
<news:OtYwK%23G2GHA.4108@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

I
really
appreciate
your
testing
and
results.

So
let
me
see
if
I
understand
it.

Since
I
need
a
Windows
login,
the

Re: ADAM and Windows Address Book

simple
bind
is
of
little
interest.

If
I
want
a
Windows
login
to
ADAM
from
Address
Book,
I
must
be
logged
into
a
domain
account.

That
is
because
the
SSPI
logon
uses
the
credentials
of
the
logged
on
account.

If
the
logged
on
account
is
not
a
domain
account,

Re: ADAM and Windows Address Book

then
no
authentication
can
take
place
because
ADAM
does
not
authenticate
accounts
that
are
not
either
ADAM
accounts
or
Windows
accounts
for
the
domain
that
ADAM
is
in.

The
bind
method
distinguishes
for
ADAM
between
windows
accounts
(domain
or
local
to
the
ADAM
instance)
and
native
ADAM
accounts.
An

Re: ADAM and Windows Address Book

SSPI
connection
must
be
a
windows
account
from
ADAM
perspective
and
the
only
authorities
ADAM
can
appeal
to
for
auth
of
the
account
are
domain
(joined
to
or
trusted)
and
the
OS
ADAM
server
is
running
on.
If
the
only
credentials
WAB
can
offer
over
SSPI
are
those
of
the
logged

Re: ADAM and Windows Address Book

on
account
that
runs
WAB
and
if
that
account
is
not
auth'd
by
an
authority
ADAM
has
access
to
then
there's
no
access.

A
conclusion
is:
The
username/password
supplied
to
the
Address
Book
properties
pages
is
not
used
for
authentication
to
the
ADAM
instance
–
ever!
If
I

Re: ADAM and Windows Address Book

report
this
to
MS,
will
it
be
considered
a
bug?
Are
any
hotfixes
known
for
this?

The
username/password
in
WAB
can
be
used
for
a
simple
bind
(with
or
without
SSL)
using
credentials
of
an
account
that
is
native
to
ADAM.
SPA
must
be
unchecked
for
this
to
work.

Re: ADAM and Windows Address Book

WAB
is
clunky,
the
real
problem
is
as
JoeK
pointed
out
that
the
use
of
credentials
and
the
selection
of
"SPA"
in
the
interface
should
be
mutually
exclusive
(and
also
no
one
knows
what
"SPA"
means).
IMO
WAB
and
the
Outlook
LDAP
Address
Book
could
both
do
with
a
refresh;
googling

Re: ADAM and Windows Address Book

around
it
seems
like
WAB
may
be
replaced
in
vista.

I
believe
Address
Book
fails
the
same
way
when
pointed
directly
at
an
Active
Directory
domain
rather
than
an
ADAM
LDAP
instance!

Pointing
WAB
at
a
DC
the
only
authority
is
the
domain
(or
trusted
domain)
no

Re: ADAM and Windows Address Book

local
windows
SAM
auth,
clearly
any
non
domain
account
will
fail
to
auth.
However
unchecking
SPA
and
entering
domain
credentials
(in
appropriate
form)
will
work
against
AD
(SSL
may
be
required
depending
on
policy)
as
the
simple
bind
with
windows
credentials
will
be
authenticated
by
AD.

Lee
Flight

Re: ADAM and Windows Address Book