

Re: ADSI Problem

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-01/msg01229

- *From:* "Joe Kaplan" <joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 16 Jan 2007 22:30:56 -0600
-

So, are you building ASP.NET applications for ASP 3.0 apps? You can't use the .NET ActiveDirectoryMembershipProvider with an ASP 3.0 app as they don't share authentication information. If you want to build .NET apps, then the built in mechanisms to support forms-based authentication are the way to go. In a .NET web app, you generally discover the identity of the authenticated user via the HttpContext.User property, which returns an IPrincipal with an Identity property that has a Name property. This works with both Windows and Forms auth, so it makes it easy to use from the code as it doesn't necessarily have to care how the app is doing authentication.

If you want to do ASP 3.0 apps, then you need to roll your own forms auth system. That is typically done by persisting state using either cookies or query string variables. Both of these need to be cryptographically protected to prevent tampering by the end user.

As for a code-based mechanism for actually doing auth against AD that you can easily call from script, OpenDSObject with the LDAP provider is probably your best bet. You said your server wasn't a domain member, so your options are really limited with how you can use Windows security and Basic or IWA auth are not possible. That's too bad.

If you need to retrieve data from AD programmatically, I'd suggest using IADsNameTranslate, ADO to perform queries or IADs to bind to specific objects and return their properties.

Unfortunately, script and ASP 3.0 are not my things, so I'm not the expert in this stuff, but there are other people out there who can help more.

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>

—
"robinwilson16" <robinwilson16@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:39B35EA5-D059-43E2-B4DD-93AB2D17DDEE@xxxxxxxxxxxxxxxxxxxx

Re: ADSI Problem

Right I've got the script working now with my ASP applications by passing the username over as a form post variable. I was hoping to use sessions, but it appears that it is quite difficult to share sessions.

I still need to work out whether a user is a member of a particular user group.

I did manage to get the user's email address using:
user = Membership.Provider.GetUser (username.Text, true);
status.InnerHtml += user.Email;

But there appears to be no method for checking if user X is in group Z in order to return True or False.

Is there some other way to query if a user is in a particular group?

Thanks

Robin

"Joe Kaplan" wrote:

Why not just let IIS authenticate the users? If the web server is a domain member, you can just turn on Basic, Digest or IWA auth and it will just work.

If you are doing forms authentication using ADSI (which it sounds like you are trying to do) and want to authenticate against AD, you really should be using the LDAP provider, not WinNT. I generally don't recommend using ADSI for authentication (and neither does Microsoft) as it does not scale well. However, that doesn't sound like the problem you are having (although it might be if the app is very heavily used).

You'd have more and better options if you switched to .NET for your web apps (ActiveDirectoryMembershipProvider for one), but it sounds like you got a big existing base in older technologies like ASP.

Another option is to look at ADFS to implement web SSO, but that might be too big of a bite to chew off. It does support older app platforms, but in Windows token mode, which might not be a way you are used to doing identity integration in your apps.

Re: ADSI Problem

In general, I tend to recommend staying away from the WinNT provider except for doing stuff with the local machine or NT4 domains.

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>

--

"robinwilson16" <robinwilson16@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
<news:B683DC84-4966-4D49-9901-8D37510AAE03@xxxxxxxxxxxxxxxxxxxx>

Well the main goal is that all domain users will be able to log on to the various web applications as at the moment everyone has different usernames and password for all the resources and it is very confusing.

I thought I had found the answer and re—wrote the applications to use ADSI to authenticate users instead of using local databases. It worked eventually for the less heavily used ones although IIS needed restarting every few days to keep it working but putting it on a vb web application that is heavily used and the ADSI script stops working after about 5 minutes.

I still think this is the best option. I have had a look at ADAM but it seems I would need to constantly update the local ADAM schema when new users are added or they change their passwords. It also says that it does not sync passwords in the documentation??? I tried the method in the documentation to

Re: ADSI Problem

sync an active directory object (i.e. the users) at home on a test domain and it wouldn't work.

Do you have any ideas how I can get this to work without increasing security risks by joining the web server to the domain?

Thanks for the help
Robin

"Al Mulnick" wrote:

To know if ADAM was something you could use, we'd need to know more about your design goals and such. What is it you want to accomplish and what do you have to work with?

I suspect that at this point changing authentication mechanisms is not the answer to your problem. That's just a guess though as your situation may dictate that you do so.

Al

"robinwilson16"

<robinwilson16@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote in

message

news:0E5CB532-910C-467E-8C79-EE9A3ED61FE6@xxxxxxxxxxxxxxxxxxxx

Hello

That string is
WinNT://school.local/userid

It always works on the member server and sometimes on the webserver.

It's

Re: ADSI Problem

just too temperamental to use
as a solution at the moment.

Could I use ADAM to get it
to authenticate with
localhost instead?

Not
sure
how I would go about
setting it up though.

I can always ping
school.local whether it
works or not.
I don't really want to add the
webserver to the domain
either for
security
reasons.

Either authentication works
straight away or it hangs for
about 5
seconds
and fails.

It would be less frustrating
if it didn't work at all!

"QuaffAPint" wrote:

What is
strAdsPath
that is
getting
passed –
what does it
look like?
Are you
passing the
user like
'domain\userid'
?

–Matt

On Jan 15,
9:19 am,
robinwilson16
<robinwilso...@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Re: ADSI Problem

wrote:

Thanks
for
the
reply

I
have
tried
with
LDAP://
instead
of
WinNT://
and
it
is
still
the
same
and
also
with
the
IP
address
instead
of
the
domain
name
Do
you
know
how
I
can
also
the
script
to
make
it
work
all
the
time.
I
only
need

Re: ADSI Problem

a
simple
login
script
which
authenticates
users
via
AD
and
sets
up
a
session.

The
script
seems
to
allow
so
many
users
to
log
in
and
then
it
breaks.
Restarting
IIS
usually
gets
it
working
again.
This
seems
like
very
strange
behaviour???

I
will
try
posting
at
vbscripting
too,

Re: ADSI Problem

thanks
Robin

"Al
Mulnick"
wrote:

Honestly?

It
surprises
me
that
it
works
at
all.

I
wouldn't
have
thought
mixing
WINNT
provider
with
adspath
would
work
as
you
have
it.
IADS
sometimes
surprises
me
though
:)

You
may
want
to
post
this
on
the
VBScripting
news
groups

Re: ADSI Problem

and
possibly
for
IIS.
You
may
also
want
to
check
the
IIS
logs
to
see
what
errors
you're
throwing.
You
have
no
authentication
mechanism
that
I
see
in
there,
so
you're
relying
on
anonymous
connections
(and
using
WINNT
provider)
meaning
that
you
should
be
logging
some
attempts
(if
not
try
enabling

Re: ADSI Problem

Re: ADSI Problem

auditing
to
see
them
better)
to
the
domain.

"robinwilson16"
<robinwilso...@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
wrote
in
message
<news:AA50061B-2F91-41D8-92DC-DC38D21B54>

Hello

I
have
written
a
script
to
authenticate
Active
Directory
users
via
ADSI
within
a
vb
script
in
IIS.
It
works
fine
on
one
pc
which
is
a
member
server.

Re: ADSI Problem

But
on
the
webservice
which
is
not
part
of
the
domain,
the
script
works
ok
for
a
while
then
stops
working
with
the
following
errors
when
attempting
to
authenticate
the
users:

Error:
424
Description:
Object
Required

Error:
-2147023677
Description:
Object
Required

Re: ADSI Problem

Restarting
IIS
normally
fixes
it
until
it
stops
working
again.
Please
can
someone
tell
me
why
this
might
be
happening.
The
code
is
below:

Thanks
Robin

```
'Get  
the  
username  
and  
password  
from  
the  
form  
Dim  
strUserName  
strUserName  
=  
Request.Form("username")  
Dim  
strPassword  
strPassword  
=  
Request.Form("password")
```

Re: ADSI Problem

```
'Get  
the  
page  
action  
Dim  
act  
act  
=  
Request.Form("act")  
Dim  
iFlags  
iFlags  
=  
Request.Form("Flags")
```

```
'If  
the  
action  
is  
authenticate  
if  
act  
=  
"auth"  
then
```

```
'If  
the  
AD  
path  
is  
not  
empty  
if  
(not  
strADsPath=  
"")  
then
```

```
'Bind  
to  
the  
ADSI
```

Re: ADSI Problem

```
object  
and  
authenticate  
the  
user  
Dim  
oADsObject  
Dim  
objUser  
Dim  
objGroup
```

```
Dim  
accountDisabled  
Dim  
accessLevel
```

```
Dim  
isAdmin  
Dim  
isTeacher
```

```
Set  
oADsObject  
=  
GetObject(strADsPath)
```

```
Dim  
strADsNamespace  
Dim  
oADsNamespace  
strADsNamespace  
=  
left(strADsPath,  
instr(strADsPath,  
":"))  
set  
oADsNamespace  
=  
GetObject(strADsNamespace)
```

Re: ADSI Problem

```
Set  
oADsObject  
=  
oADsNamespace.OpenDSObject(strADsPath  
strUserName,  
strPassword,  
0)
```

```
'Set  
up  
a  
user  
object  
to  
enable  
information  
about  
the  
user  
to  
be  
obtained  
Set  
objUser  
=  
GetObject("WinNT://school.local/"  
&  
strUserName  
)
```

```
'Set  
up  
a  
group  
object  
to  
enable  
group  
information  
to  
be  
obtained  
Set  
objAdminGroup  
=  
GetObject("WinNT://school.local/"  
&
```

Re: ADSI Problem

```
adminGroup
)
Set
objTeacherGroup
=
GetObject("WinNT://school.local/"
&
teacherGroup
)
```

```
'Boolean
to
say
whether
a
user
is
a
member
if
the
given
group
isAdmin
=
objAdminGroup.IsMember(objUser.ADsPath)
isTeacher
=
objTeacherGroup.IsMember(objUser.ADsPath)
```

```
'If
there
was
an
error
if
not
(Err.number
=
0)
then
...
```

Re: ADSI Problem