

Re: ADFS June 2006 Step-by-step guide

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-08/msg01212

- *From:* Noremac <Noremac@xxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 3 Aug 2006 09:16:02 -0700
-

Okay, I am still stuck but this is where I am so far.

Again, I am trying to work with the step-by-step guide.

I went back to seeing how a claims-based app can work and I have abandoned the token app for the moment.

I got the guide's step-by-step claim app to work where I see its default.aspx page that shows all of the stuff of the user.identity.

Again, my partner user id (Adatum) is getting to my claim app even though that user id is not in the partner's active directory group that I have mapped to the resource claim app.

What looks like to me is happening is that the UPN claim is overriding the Group claim. Infact, on the resource server's fs settings, I went to where I had setup the trust policy for my claim-app and disabled the adatum group claim. The adatum user can still see the page.

So my question is what did I miss in the guide so that only the group claim will be used for authorization? This is a confusing point for me because if I try and disable the UPN claim, fs always complains that there must be one Identity Claim.

"Joe Kaplan (MVP – ADSI)" wrote:

Funny you should ask. I put together a blog post that shows exactly how to do that. :) My blog is likely to be full of fun and useful ADFS stuff for some time to come, so if you are a blog reader, you might consider subscribing or visiting occassionally. I have a whole series of things planned if I can get around to writing it all down.

<http://www.joekaplan.net/HowToGetVSNETIntegrationForADFSClaimsBasedApps.aspx>

Note that this technique is useful for doing not only claims apps, but also claims transform modules and LS pages customization.

Re: ADFS June 2006 Step-by-step guide

Unfortunately, I was a little reluctant to actually put the final MSI package out there as I wasn't sure how MS would feel about me repackaging their installer and I didn't get a clear reading from the product team on whether they thought it was cool. As such, the instructions require you to build the MSI package with WiX, which isn't too hard but it is a bit of a PITA. If it seems like too much to you, email me offline and I'll send you the MSI I created.

As the article states, this DOESN'T actually make ADFS work on your machine. All it does is let's you compile and give you a good VS integration experience.

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>

--

"Noremac" <Noremac@xxxxxxxxxxxxxxxxxxxx> wrote in message
news:DA8F6DD1-6D57-44BC-BEC8-AFFCA8E11487@xxxxxxxxxxxxxxxxxxxx

I really do appreciate all of your help Joe.

I was trying to write some code against the ADFS API but on my development Windows XP machine, I don't have the library. Do you know what assemblies I can copy over from my Win2K3 machine or the ADFS library install for XP?

"Joe Kaplan (MVP - ADSI)" wrote:

Getting the claims app up first is a good idea, because that's the only straightforward way to see what claims you are getting.

The type of error you are receiving looks familiar. The error code 1317 decodes to "no such user", so that probably means that ADFS is trying to create a token for a use instead of based on group claims in the federation token. The "no such user" is probably a result of the fact that there is no alansh@xxxxxxxx in the resource forest. I'm kind of guessing on that.
It

Re: ADFS June 2006 Step-by-step guide

also looks like there might be some UPN mapping going on since you have a user with an adatum UPN that was issued by treyresearch. BTW, search for "err.exe" on the microsoft.com. Very helpful!

The question here is then whether you want the Windows token generated by ADFS to map to a specific user in your forest or if you want a token based only on groups that map to group claims. If you want to map to a user, you should make sure that the UPN of the user matches a UPN in the resource forest.

If you want a Windows token based on groups, you should make sure that the user has at least one group claim that maps to a resource group. Also, you have the ability in your trust policy on the resource side to specify what type of mapping you want to do.

The claims app will help you debug all this stuff and the quick start sample app has a nice test page for dumping out the claims.

Once you get all of your troubleshooting tools lined up and know what you are looking at, this will all start to make sense and work predictably. It takes a little while though.

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>

--
"Noremac" <Noremac@xxxxxxxxxxxxxxxxxxxx> wrote in

Re: ADFS June 2006 Step-by-step guide

message

news:0FB28DA0-0F50-40E4-BB1B-D572FBDA35EE@xxxxxxxxxxxxxxxxxxxx

I will turn on the extra logging to the log files and go over what you said.

In the meantime, this is the Security Failure Audit that it generated on the resource web server:

The client presented a valid XML token, but an error occurred during the attempt to generate a Windows NT token from the security IDs (SIDs).

The error code was 1317.

Token ID:

_857d7b3b-3d41-4460-94c1-f667a9c36e0b

Issuer: urn:federation:treyresearch

Identity: alansh@xxxxxxxxxxx

Error code: 1317

Nothing showed up on a google search. I am sure it is something silly

on

my

part. I may try and see if I can get the claim-app working since that

is

not

mixed up with Sharepoint in the step-by-step guide.

"Joe Kaplan (MVP - ADSI)" wrote:

Under ADFS, the app (site or virtual directory) needs to be set to anonymous auth. The ADFS web service extension actually "intercepts" the request and creates a Windows security token based on the claims in the FS token for

Re: ADFS June 2006 Step-by-step guide

IIS

to use before your code actually gets to execute against the request.

The

whole "anonymous" thing in IIS takes a little getting used to, but

that's

the way a lot of other SSO products like this actually work.

The contents of the

windows token you'll get depends entirely on the claims

supplied to the app from ADFS and the type of user mappings you are allowing

in your trust policy. If you are allowing only user to user mapping,

then

the claim must contain a UPN claim that matches the UPN of a user in

your

forest. If you just allowing groups, then the user must have at least

one

resource FS claim with a resource group associated with it their

federation

token. There are also the hybrid settings as well.

Typically, I use

user-to-user for accounts in the resource FS and use groups-only mapping for users from foreign account partners.

From what it sounds like though, it doesn't seem like ADFS was working at

Re: ADFS June 2006 Step-by-step guide

all. If the authenticated user
from the test page isn't an
ADFS user,
then
something is weird indeed.
For a user from a foreign
federation
account
partner, it usually looks like:

urn:federation:foreignpartner\someuser@upndomain

I'm not sure what happens if
you don't supply a UPN
claim though. I
haven't
tried that.

Make sure you've got all the
logging going and that
you've got all the
audits going as well.
Enabling Object auditing
(success and failure)
in
the
local security policy will
allow the ADFS Web
Extension to tell you
what
it
is doing for federation token
authentication in the
Security event
log.

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>

--

"Noremac"

<Noremac@xxxxxxxxxxxxxxxxxxxx>

wrote in message

news:3ECF25E2-2EC2-4F9D-B03C-3342E24773CA@xxxxxxxxxxxxxxxxxxxx

Re: ADFS June 2006 Step-by-step guide

Hi Joe,

I am sure I
messed
something
up from my
conversion
of the
guide.
That
is
why
I was
looking for
Nick's
non-Sharepoint
sample.

I am trying
to do it
through the
file system
as this
accurately
represents
old
non-.NET
web apps
we will
need to
protect.

When I run
your sample
code from
my
federated
partner, the
Windows
Identity
is NT
Authority.
There is no
Identity and
no groups.
When I call
the
same
page right
from the
resource

Re: ADFS June 2006 Step-by-step guide

web server,
I get the
Windows
Identity
of
NT
Authority
and the
Identity of
the logged
in person
and its
groups.
So
this
told me I
was coming
in
anonymous.
I checked
my IIS
settings and
sure
enough,
anon was
on. So I
turned it off
and turned
on
Windows
Authentication.
Now
it
will not
allow me to
login at all
from either
the resource
web
server
or
partner
client.

"Joe Kaplan
(MVP –
ADSI)"
wrote:

Re: ADFS June 2006 Step-by-step guide

Give
me
a
few
hours
and
I'll
stick
it
on
my
blog
(www.joekaplan.net).

In
your
token
app,
how
are
you
trying
to
restrict
access?
Are
you
using
some
sort
of
.NET
role-based
mechanism
like
the
UrlAuthorizationModule
(i.e.
the
<allow>
and
<deny>
tags
in
web.config)
or
are
you
trying
to
use

Re: ADFS June 2006 Step-by-step guide

file
system
ACLs
or
what?

In
any
event,
the
first
step
is
knowing
what
groups
are
in
you
token
and
my
page
can
help
with
that,
so
hopefully
it
will
give
you
the
clue
you
need.

Joe
K.

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

Re: ADFS June 2006 Step-by-step guide

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

--
"Noremac"
<Noremac@xxxxxxxxxxxxxxxxxxxx>
wrote
in
message
<news:40DDB753-C4AA-41FD-B1CC-70A390D686BF@x>

Hi
Joe,

I
think
that
would
be
very
helpful.
I
have
a
simple
web
page
too
that
spits
out
Windows
Identity
principal
so
I'll
take
anything
that
I
can
get
my
hands
on
to

Re: ADFS June 2006 Step-by-step guide

try
and
trouble
shoot
this.

I
agree
it
was
simple
to
setup
the
ADFS'd
website.
But
I
have
something
wacky
when
anyone
on
the
"account"
domain
can
get
to
the
site
(without
anyone
belonging
to
the
"account"
resource
group).

Thanks,
Noremac

"Joe
Kaplan
(MVP
-
ADSI)"
wrote:

Re: ADFS June 2006 Step-by-step guide

Do
you
want
my
test
page
that
I
use?
Actually
creating
the
non-SharePoint
token-based
app
in
IIS
is
pretty
trivial.
You
just
create
a
web
site
and
configure
ADFS
on
it
in
the
IIS
MMC.

My
test
page
just
spits
out
the
user
name
and
groups
of
the
authenticated
user.

Re: ADFS June 2006 Step-by-step guide

It
isn't
much
to
look
at,
but
it
is
helpful
for
debugging,
since
that's
the
stuff
you
need
to
know.
I'll
put
it
up
on
my
blog
or
something
if
you
are
interested.

Also,
enabling
logging
for
token-based
apps
is
sometimes
helpful.
The
troubleshooting
section
of
the
operations
section
of

Re: ADFS June 2006 Step-by-step guide

the
ADFS
TechNet
docs
explains
all
the
registry
flipping
you
have
to
do
to
turn
it
on.

The
other
important
thing
is
whether
you
are
accessing
the
token
site
from
an
account
partner
or
the
resource
partner's
own
account
store
and