

Re: ADFS June 2006 Step-by-step guide

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-08/msg01127

- *From:* Noremac <Noremac@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 2 Aug 2006 08:08:02 -0700
-

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 user 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@xxxxxxxxxx` in the resource forest. I'm kind of guessing on that. It 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.

Re: ADFS June 2006 Step-by-step guide

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: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@xxxxxxxxxxxx

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 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

Re: ADFS June 2006 Step-by-step guide

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
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.

—

Re: ADFS June 2006 Step-by-step guide

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

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 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.

Re: ADFS June 2006 Step-by-step guide

"Joe Kaplan (MVP – ADSI)" wrote:

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

--

"Noremac"

<Noremac@xxxxxxxxxxxxxxxxxxxxx>

wrote in message

news:40DDB753-C4AA-41FD-B1CC-70A390D686BF@xxxxxxxxxxxxxxxxxxxxx

Hi Joe,

I think that

Re: ADFS June 2006 Step-by-step guide

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 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)"

Re: ADFS June 2006 Step-by-step guide

wrote:

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

Re: ADFS June 2006 Step-by-step guide

the
authenticated
user.

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

Re: ADFS June 2006 Step-by-step guide

operations
section
of
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
how
you
are
doing
the
token

Re: ADFS June 2006 Step-by-step guide

mapping
(user-to-user
or
group-based
using
claims
and
resource
groups).

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:B1305559-AB09-493C-9C42-C4E08B48A80F@xxx>

Hi
Nick,

I've
been
on
holidays
and
I
just
got
your

Re: ADFS June 2006 Step-by-step guide

post.

I
would
definitely
like
an
existing
sample
on
a
non-portal
token
app.

I
am
hoping
my
issue
relates
to
configuration
that
your
instructions
on
the
Windows
NT
token-based
app
will
help
me
find.

Thanks!

"Nick
Pierson
[MS]"
wrote:

Noremac,

Susieber
alerted
me
to

Re: ADFS June 2006 Step-by-step guide

your
post.
I'm
the
author
of
the
ADFS
Step-by-Step
Guide.

Unfortunately,
this
guide
has
never
been
tested
at
Microsoft
using
a
VM
environment.
At
some
point
I
would
really
like
to
try
this
myself
and
then
update
the
guide
accordingly.
I'm
in
the
process
of
writing
the
deployment
guide
so

Re: ADFS June 2006 Step-by-step guide

I'm
not
exactly
sure
when
I
will
be
able
to
get
to
this.

I
can
tell
you
that
this
step-by-step
guide
has
been
thoroughly
tested
using
4
computers,
and
that
in
this
situation
it
does
result
in
setting
up
a
successful
ADFS
test
lab
environment.

Since
I
have
not

Re: ADFS June 2006 Step-by-step guide

personally
set
up
the
step-by-step
guide
using
VMs,
I
would
recommend
that
you
acquire
4
computers
and
then
follow
the
step-by-step
guide
from
start
to
finish
(the
appendixes
are
not
required
to
get
a
functional
demo
working).
Make
sure
to
follow
the
IP
addressing
scheme
and
other
naming
schemes
to
the

Re: ADFS June 2006 Step-by-step guide

letter.
If
you
don't
want
to
go
through
it
again,
I
understand.

Also,
if
you
are
interested
in
setting
up
a
non-SharePoint
app
for
your