

Re: Incoming E-Mail – cant create contact in OU

Source:

<http://www.tech-archive.net/Archive/SharePoint/microsoft.public.sharepoint.windowsservices/2007-09/msg00076.htm>

- *From:* "callahan" <cacallahan@xxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 6 Sep 2007 23:06:21 -0400
-

Did you give the account the same advanced access that the Administrators had to those keys, or did you just give them full control on the security tab?

–callahan

"Paul" <Paul@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:49EC2F48-4CB6-4B23-8942-336DD0AEC884@xxxxxxxxxxxxxxxxxxxx>

So I downloaded RegMon and FileMon from SysInternals. I took the user account out of local administrator to attempt to find any denied access.

I didnt see anything in the FileMon, but RegMon was coming up with a few denied hits.

Got a denied on OpenKey of:
HKLM\SYSTEM\ControlSet001\Services\W3SVC\Parameters

And denied when attempting to Createkeys for folders inside:
HKCU\Software\Policies\Microsoft\SystemCertificates\

I then added full permissions to my user account on both of these keys, rebooted and RegMon still shows denied access to these keys. I am wondering if Windows has some higher permissions for these beyond simply adding my account to their permission, such as only allow admin's to these areas no matter what?

"callahan" wrote:

Exactly Paul!! I too am worried about giving the app pool (and remember, that's for every app pool you create for every new web app on the farm) local admin rights to the server hosting incoming email.

I wrote it in the book because I had to, it's what works and that ain't no

Re: Incoming E-Mail – cant create contact in OU

lie. But I am so totally willing to be wrong if someone could really show what permission I need to give the app pool locally to avoid this issue.

I tried to think of what it might need, in terms of DMS and email, locally on the server that it can only get as the local admin.

Oh and by the way, Congratulations for getting it to work!

As I said, I had to move on to other things with the clients and with the book, so I couldn't continue my research. Things you might want to try:

1) maybe it's a permissions problem on the SMTP drop folder or some other smtp folder locally. Try adding the app pool to that. I always start with too many permissions, and if it works, start stripping them away until it breaks. ;)

2) maybe add the app pool to the WSS WPG groups that sharepoint creates locally. If your app pool account is also the farm account, then it will already be a member of those groups.

3) I know it may be crazy, but see if adding the app pool to the log folders or maybe the sharepoint folders (maybe starting at the12 folder) does the trick. I know that if the app pool is already a member of the WSS_admin_wpg group then it's got modify rights, but if you look at the advanced permissions, Administrators have full control, so maybe full control is what the account needed...

I just have a feeling that the app pool just needs access to something that only a local admin has on the sharepoint server, and if we can find that thing (or those things) we can give permission there directly and avoid the breach in security that giving the app pool local admin power can cause.

Congrats again! Outstanding that it works. However, it's not really optimal yet. I also don't like the permissions in terms of managing approval in Central Admin. It doesn't work quite as advertised and I am not sure if its a general bug or another undocumented permissions thing. Thanks for really working on it, and thanks for getting back to us about what, exactly, worked. I appreciate it. It's nice to see that what worked for me is working for someone else (although I am surprised about the full reboot,

Re: Incoming E-Mail – cant create contact in OU

maybe iisreset would have worked?).

–callahan

"Paul" <Paul@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:OCA8E517-1C66-479D-A4E4-827E32BC3D2B@xxxxxxxxxxxxxxxxxxxx

I followed your instructions and was able to get it to work.

What I needed to do was

1) Go to the OU in security/advanced I added my sharepoint
application

pool
and gave full rights.

2) On each WSS front end web server, I added the
application pool to

local
admin

Rebooted all WSS web servers and tried it again, and it
worked.

Now, I just need to determine the best way to give the local
WSS

permissions, as I am not so hip to have a website running as
a local

administrator!

"callahan" wrote:

Gotcha. I would strongly suggest that, in the
future you really make

the
central admin pool different than the web

app. It will really help
secure

that account a little (if the web app is
compromised or something,

central
admin will be okay and vice versa, that

central admin account is kind
of

precious). It also makes it easier for
troubleshooting.

However, under the pressures of production

I can see that just getting
the

darn thing to work is kind of critical. ;)

Re: Incoming E-Mail – cant create contact in OU

Now I understand that you have given the account "full rights" of the OU,
but if you don't do advanced security, you are still not giving them the same, critical rights that the domain admins get, so you will continue to have problems until the cows come home.

Or at least, that has been my experience. The thing is, it's solid as a rock if the permissions are right (although I must confess that I have only clients using DMS with exchange 2003). My only problem (and I feel it's another security problem) is getting approval to work completely. But that's an issue for another day.

So I started with giving the app pool account domain admins permissions then went backwards. in other words I checked the special permissions that Administrators and Domain Admins get for the OU (they get lotsa rights straight out of the box, even if you didn't put them there), and gave my app pool account all of the same rights (and yes, that is really out of hand but bear with me).

-->And don't forget to IISRESET /noforce every single time you make a change that you think with work to get sharepoint to notice.<--

Then, when I got it to work, I began to remove the permissions that I

Re: Incoming E-Mail – cant create contact in OU

didn't
think would matter, stripping down what the
app pool could do until I
figured out (I'm pretty sure, I might still be
giving it too much
power)
which permissions the app pool had to have
to do its job with DMS.
That's
why I know that you need extra permissions
to get that account to
work,
not
just delegating control, even full control. It
won't work, at least
it
didn't for me. Then, even when looking at
security, selecting full
control
in the dialog box is not the same as the
"special" permission settings
under
Advanced. Further, it seems to really, really
matter that you don't
just
allow permissions on that OU but the same
permissions on all of its
child
objects.

Keep in mind that if you got it to work with
the app pool as a domain
admin,
then it works. Period. It is only a
permissions issue. You are
right,
and
don't doubt it. It's just a matter of getting
those permissions
right.

I just finished writing a book on this stuff
and have been working on
these
settings (and much more) for months. I am
always open to being wrong
(as
a
matter of fact, if someone has a better way,
please let me know) but
this

Re: Incoming E-Mail – cant create contact in OU

is what has worked for me. And sometimes,
when push comes to shove,
we
can
only do what we know works, regardless of
what documentation has told
us.
Believe me, I know. ;)

And please don't be offended by this
question, but is there a reason
why
you
need to do Directory Management Service
for incoming email? If push
came
to
shove, would your environment support just
doing incoming email
without
DMS's contacts and distribution groups in
AD? Incoming email works
great
(really great) without DMS enabled at all.
As a matter of fact I use
enabling incoming email without DMS as a
troubleshooting technique to
isolate DMS problems all the time. I guess I
am just trying to let
you
know
if DMS is a pain, do without it. A lot of MS
documentation says (or
strongly implies) that you have to do DMS
to do incoming email with is
completely untrue.

–callahan

"Paul"

<Paul@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote in message

news:5D08D12F-671B-477B-A910-5FADC5812A76@xxxxxxxxxxxxxxxxxxxx

Thanks for your continued
help callahan,

To better explain my
situation, I am using WSS
3.0 and I have 3 WSS
web

Re: Incoming E-Mail – cant create contact in OU

servers connected to a SQL
2005 SP1 cluster.

On all WSS servers, the 2
application pools used are
"Sharepoint
Central
Administration" and
"SharePoint_Company".
Both of these application
pools
are running under the
domain user account of
"Domain\Sharepoint_AppID"

The windows service
"Windows Sharepoint
Services Timer" is also
running
under this same domain user
account
"Domain\Sharepoint_AppID"

On my domain controller, I
launched AD Users &
Computers and created
a
new
OU called "Sharepoint". On
this OU, I then delegated the
rights for
the
same
user
"Domain\Sharepoint_AppID"
for Create, delete and
manage user
accounts.

I
also added Read All user
Info for kicks.

This is my understanding as
the documented procedures
to make this
work.

I
have also gone a step further
and gone back to the OU
and made the
account

Re: Incoming E-Mail – cant create contact in OU

"Domain\Sharepoint_AppID"
with full rights to the OU,
and also made
this
account the local
administrator to all WSS
web servers.

I am still thinking the
problem is this account
"Domain\Sharepoint_AppID"
is
not having enough rights to
access AD in the first place,
to even
get
to
the
OU level and perform its
magic. Again, making this
account a domain
administrator solves the
problem, but not something
I am comfortable
with.

"callahan" wrote:

Okay, lets
see here,
you are
having
problems
getting
DMS to
work
and
you
already
have the
application
pool
delegated
rights to the
OU. It
worked
when you
had that

Re: Incoming E-Mail – cant create contact in OU

account set
as a domain
admin for
the domain,
but
not
when
it is a local
admin.

In my
experience
it is because
you didn't
quite
delegate
enough
rights
to
the account
in the OU.

Also
though,
before we
go further
with that,
Daniel was
wondering
if
you
would
delegate the
same rights
you gave
the
application
account to
the
OU
to
the account
that is being
used for the
central
administration
application
pool.

(Actually,
come to

Re: Incoming E-Mail – cant create contact in OU

think of it,
this does
bring us to a
little
empass.
There is a
question we
need to ask,
and that is if
you are
running
WSS
3
as
a single
server
install or a
Web Front
end, server
farm
install?)

I took it for
granted
(and
probably so
did Daniel)
that you had
a
server
farm
installation
of WSS
because
your
application
pool
account was
a
domain
account. I'm
going to
stay with
that
assumption
until you
tell us
otherwise.

If your
installation

Re: Incoming E-Mail – cant create contact in OU

of WSS 3 is
not a single
server
installation,
then
the
application
pool
account for
Central
Administration
(which is
considered
the
Farm
account
because it
also is the
account that
runs the
Sharepoint
Timer
Service, and
is critical to
the
functioning
of a
sharepoint
server
farm)
also may
need access
to the OU.
You can
figure out
what
account
that
is
a
couple of
different
ways: check
what
account
identity the
Sharepoint
Timer
service is
running in
the services

Re: Incoming E-Mail – cant create contact in OU

Re: Incoming E-Mail – cant create contact in OU

MMC; or
open IIS, go
to the
Central
Administration's
application
pool's
identity is.

Once you
figure out
what that
account is,
you could
try
delegating
it
rights
to the OU.
Specifically,
don't forget
to delegate
it delete
rights
so
it
can
delete
things from
the OU if
need be.

Overall, I
suspect that
what
happened
was that
you did not
delegate
enough
rights to
your web
application's
application
pool at the
OU.
Instead
of
using the
delegate
control

Re: Incoming E-Mail – cant create contact in OU

wizard, you might want to go to the View menu in the ADUC MMC and select Advanced features. That will let you, when you right click the OU, go to properties and see the Security tab (that you can't see without the advanced features view enabled). In the security tab you can see the permissions that are available. Check the domain admins rights, then click the Advanced button at the bottom. Notice that the domain admin actually has much more than just the

Re: Incoming E-Mail – cant create contact in OU

standard
full
control
of
the OU
(which is
above what
you
might've
given the
account
originally--
while a
domain
admin they
get stuff
that trumps
that
delegate
control
you
gave it),
they have
control of
all child
objects
under the
OU as
well
(not
because
domain
admins
explicitly
get that but
because
they are
members
of
the
Administrator's
group that
gets that).
It's the
domain
admin
like
control that
you need to
give the app
pool so it

Re: Incoming E-Mail – cant create contact in OU

Re: Incoming E-Mail – cant create contact in OU

can do its
work
with
the
OU—
without
giving it
that kind of
control
elsewhere
in the
domain.

Please
check that
out and see
if it works
for you.
Don't give
up
hope, I