

Re: Issue with ASP.NET client, COM Interop, and Identity impersonation

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.interop/2004-10/0091.html>

From: Willy Denoyette [MVP] (*willy.denoyette_at_pandora.be*)

Date: 10/04/04

Date: Mon, 4 Oct 2004 21:25:00 +0200

Ok, back to your requirements.

"aspcompat" is not an option, and running the process under a domain account either.

When you COM object is a threadingmodel=apartment (STA), it will be created in a the default process STA, and use the process token when accessing network resources, now the process runs as a local account (ASPNET) and as such has no network access privileges.

Your only option left is:

- Spawn a new thread and set it's apartment state to STA before starting (this solves the inter-apartment marshaling issue).

- In your threadproc. you need to get a logon token by calling Win32 API "LogonUser" and use this token to impersonate the current thread token by calling WindowsIdentity.Impersonate(). When done you call Undo().

Note that on W2K calling "LogonUser" requires TCB privileges (run as part of the Operating system), something you need to consider with care, as ASPNET will run with elevated privileges when doing so. Windows XP and W2K3 don't need TCB privileges to call "LogonUser".

Willy.

"Anil Krishnamurthy" <akrishnamurthy@nospam.air-worldwide.com> wrote in message news:%23w6KHQkqEHA.2612@TK2MSFTNGP15.phx.gbl...

> Yes, but that would affect all applications. We cannot do that especially

> on

> client machines. We need impersonation to work only for this web

> application.

>

> The problem is that the approach to impersonation through retrieval of the

> thread's token and calling ImpersonateLoggedOnUser() works on my machine

> only but not on other machines. :(We are unable to understand the reason

> for that. We have tried to compare the user permissions, settings etc. but

> no avail.

>

> Anil

>

> "Willy Denoyette [MVP]" <willy.denoyette@pandora.be> wrote in message
> news:OGBGSIkqEHA.1152@TK2MSFTNGP11.phx.gbl...
>> When you need to run the asp.net worker process under a specific domain
>> account (not aspnet), you have to change the processModel attributes
>> userName and password in your machine.config file (not web.config).
>>
>> userName=="Domain\UserName", password="...."
>>
>> Willy.
>>
>>
>>
>> "Anil Krishnamurthy" <akrishnamurthy@nospam.air-worldwide.com> wrote in
>> message news:uMSFc9jqEHA.2696@TK2MSFTNGP15.phx.gbl...
>> >I was trying to use that diagram to describe the problem and looks like
>> > there was some problem formatting it properly.
>> >
>> > This is what the web.config looks like
>> >
>> > <identity impersonate="true" userName="Domain\UserName"
>> > password="password"/>
>> >
>> > When I print the identities on ASP.NET side and COM object side, this
>> > is
>> > what I get.
>> >
>> > [ASP.NET]
>> > Domain\UserName
>> >
>> > [COM]
>> > Machine\IUSR_Machine
>> >
>> > When I switch off impersonation, the identity on COM side is
>> >
>> > [COM]
>> > Machine\ASPNET
>> >
>> > Hope I have made it clear now ;) So, either way, the code in COM object
>> > runs
>> > under a local machine account and thus, cannot access network resource.
>> >
>> > Thanks
>> > Anil
>> >
>> > "Willy Denoyette [MVP]" <willy.denoyette@pandora.be> wrote in message
>> > news:emzER8hqEHA.1164@TK2MSFTNGP10.phx.gbl...
>> >> ASPNET, that means that your config file is not like you said in your
>> >> original post.
>> >> / snip
>> >> ASP.NET
>> >> {Web app} -----Interop ----->{COM Library}

>>> (Domain\NetworkUser)
>>> (LocalHost\IUSR_MachineName)
>>> /end snip
>>>
>>> Here you say that asp.net runs as (Domain\NetworkUser), but this is
>>> not
>>> the
>>> case. So please change your web.config file to run the worker process
> as
>>> Domain\NetworkUser.
>>>
>>> Willy.
>>>
>>>
>>> "Anil Krishnamurthy" <akrishnamurthy@nospam.air-worldwide.com> wrote
>>> in
>>> message news:%23udstyhqEHA.4008@TK2MSFTNGP14.phx.gbl...
>>>>
>>>> "Willy Denoyette [MVP]" <willy.denoyette@pandora.be> wrote in
>>>> message
>>>> news:e1wifEGqEHA.376@TK2MSFTNGP14.phx.gbl...
>>>>> With impersonation turned off, all threads in the asp.net worker
>>> process
>>>>> use the process token when accessing remote resources, and because
>>>>> your
>>>>> in-proc COM object runs in the same security context of the caller
>>>>> (the
>>>>> executing thread) it will use the same token, problem solved.
>>>>>
>>>>> When impersonation is turned off, the identity is ASPNET and since
> that
>>> is
>>>>> a
>>>>> local account, how can you access remote resources?
>>>>>
>>>>>> About your "aspcompat" remark. If your COM object is a
> threadingmodel
>>>>>> =
>>>>>> apartment type object (STA) you better run in "aspcompat" mode.
>>>>>> If you don't, your object will run on the default STA thread
> provided
>>> by
>>>>> the
>>>>>> asp.net worker process, this will negatively impact the performance
> as
>>>>>> all
>>>>>> calls have to get marshaled.
>>>>>> Just curious, why can't you set aspcompat=true?
>>>>>>
>>>>>> Actually, the web application team informed me that they have
> switched

>> > to
>> >> > *AspCompat mode and it does not help much. The problem is that the*
> *call*
>> > to
>> >> > *COM object comes from Java script and identity impersonation does*
>> >> > *not*
>> > *work*
>> >> > *in this case. I mentioned that AspCompat flag could not used because*
>> > *there*
>> >> > *is another application, a web service, that uses the same set of COM*
>> >> > *objects.*
>> >> >
>> >> > *Anil*
>> >> >
>> >> >>
>> >> >> > *"Anil Krishnamurthy" <akrishnamurthy@nospam.air-worldwide.com>*
>> >> >> > *wrote*
>> >> >> > *in*
>> >> >> > *message news:007jprAqEHA.3760@TK2MSFTNGP09.phx.gbl...*
>> >> >> >
>> >> >> > > *"Willy Denoyette [MVP]" <willy.denoyette@pandora.be> wrote in*
>> >> >> > > *message*
>> >> >> > > *news:eYcNdGAqEHA.1816@TK2MSFTNGP09.phx.gbl...*
>> >> >> >>
>> >> >> >> > *How is that possible? if asp.net is running in a domain identity*
>> >> >> > *context*
>> >> >> > > *AND*
>> >> >> >> > > *you don't have impersonation enabled, the in-proc COM object*
> *should*
>> >> >> >> > *run*
>> >> >> > > *with*
>> >> >> >> > > *the same domain user's credentials, where else would the local*
>> > *account*
>> >> >> >> > *identity come from?*
>> >> >> >>
>> >> >> >
>> >> >> > > *Impersonation is enabled in Web.config and it is set to use a*
> *domain*
>> >> >> > > *account. But on COM object side, when I try to get the user name,*
> *it*
>> > *is*
>> >> >> > > *IUSR_MachineName and that is not what I want. Also, I cannot use*
>> >> >> > > *AspCompat="true".*
>> >> >> >
>> >> >> > > *Anil*
>> >> >> >
>> >> >> >
>> >> >>
>> >> >>
>> >> >
>> >> >
>> >> >

>> >>
>> >>
>> >
>> >
>>
>>
>
>