

Re: Design for ASP.Net w/ ComponentServices

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2002-11/2067.html>

From: Cenon Del Rosario (cenonmin@ihug.com.au)

Date: 11/30/02

From: "Cenon Del Rosario" <cenonmin@ihug.com.au>

Date: Sun, 1 Dec 2002 09:22:15 +1100

With regards to (2), I also found the code you posted on MSDN and that work quite well !

Just out of interest, do you know if there are any multi-threading issues/problems with that in terms of simultaneous impersonations from different user threads ? I am assuming that there is none...

Our plan is to set up a "Web" NT domain with these web users and do the impersonation for authenticated users as required. What are your comments on doing this (good and/or bad) ?

With regards to (3), if (2) works out then its a none-issue otherwise a bit more work for us....

Thanks again.

"nu-k-ar" <nospam@plz.com> wrote in message
news:uPfPAHHmCHA.2592@tkmsftngp02...

> 2.) k

> *what then would be the simplest is to impersonate the user in the
web.config*

> *file setting it to*

> `<authentication mode="Windows"/>`

> `<identity impersonate="true" />`

>

> *what this exactly does , it set's the process level user token to the user*

> *which interacts with the web...*

> *so it cloaks the IIS_User Identity*

>

> *i think what asp.net makes is the same as in iis5.0 and asp , u'll get the*

> *picture*

>

> `<code language="vb6.0"`

>

stolenFrom="<http://support.microsoft.com/default.aspx?scid=kb:en-us:Q248187>"

> *caveat="needsThe!@#°Password" >*

```
>
> Public Declare Function LogonUser Lib "advapi32.dll" _
> Alias "LogonUserA" (ByVal lpszUsername As String, _
> ByVal lpszDomain As String, ByVal lpszPassword As String, _
> ByVal dwLogonType As Long, ByVal dwLogonProvider As Long, _
> phToken As Long) As Long
>
> Public Declare Function ImpersonateLoggedOnUser Lib "advapi32.dll"
(ByVal
> hToken As Long) As Long
>
> Public Declare Function RevertToSelf Lib "advapi32.dll" () As Long
>
>
> Private Const LOGON32_LOGON_INTERACTIVE = 2
> Private Const LOGON32_PROVIDER_DEFAULT = 0
>
> Public Sub Logon(ByVal strAdminUser As String, ByVal _
> strAdminPassword As String, ByVal strAdminDomain As String)
> Dim lngTokenHandle, lngLogonType, lngLogonProvider As Long
> Dim blnResult As Boolean
>
> lngLogonType = LOGON32_LOGON_INTERACTIVE
> lngLogonProvider = LOGON32_PROVIDER_DEFAULT
>
> blnResult = RevertToSelf()
>
> blnResult = LogonUser(strAdminUser, strAdminDomain, strAdminPassword,
-
> lngLogonType, lngLogonProvider,
-
> lngTokenHandle) 'does a login in
> the ad
>
> blnResult = ImpersonateLoggedOnUser(lngTokenHandle)
> End Sub
>
> Public Sub Logoff()
> Dim blnResult As Boolean
>
> blnResult = RevertToSelf()
> End Sub
> </code>
>
> so the process token has the identity of the user , when the ii's connect
to
> the serviced component the service component will see the user wich has
> impersonated/cloaked the web-server
>
> u're serviced componet now runs as server , so it checks the the Identity
on
```

microsoft.public.dotnet.framework.aspnet.security: Re: Design for ASP.Net w/ ComponentServices

- > (depending on what ever u have choosen too in the mmc snap-in)
- > u'll have too implement the securityCallContext
- >
- >
- > <http://www.dotnet247.com/247reference/System/EnterpriseServices/SecurityCallContext.aspx?v=2>
- >
- > which means that the serviced component can check againnst their own roles
- > (in the snap in) on which u can assign windows accounts/roles
- >
- > the base security
- > <http://www.dotnet247.com/247reference/guide/80.aspx>
- >
- > just do a search com+ security
- >
- > this is the base
- >
- > 3.) u can do that if u like too
- >
- >
- >
- > "Cenon Del Rosario" <cenonmin@ihug.com.au> wrote in message
- > news:eZkdpJ#lCHA.1928@tkmsftngp07...
- >> With regards to (2):
- >>
- >> This could be what we need ! Is the scenario for this like the following:
- >> 1) A user is authenticated by some means we have written.
- >> 2) Whenever our ASP.Net code needs to access a secure (ie. Checks for roles)
- >> ServicedComponent, the ASP.Net worker process will cloak itself to look like
- >> the web user and thus access the components under the web user's id.
- >>
- >> If this is the case, then this is exatly what we need. Have you got some sample code that shows how to do this and what configuration is required.
- >>
- >> With regards to (3):
- >> What I meant was that we would pass the ASP.Net User object (or something)
- >> down to the ServicedComponents whenever some role checking was required
- >> and
- >> we would then use our custom code to validate the user's access rights against a ServicedComponent.
- >>
- >> I guess the main reason for all of this is that we want to centralize the
- >> security check in the ServicedComponents tier because we want to use them
- >> with other application outside ASP.Net and don't want to have to

Re: Design for ASP.Net w/ ComponentServices

> administer
>> two of them. Also, not all our web clients use IE on windows which rules
> out
>> kerberos...
>>
>> Hope you can help...
>>
>> "nu-k-ar" <nospam@plz.com> wrote in message
>> news:eyPHhNrlCHA.1464@tkmsftngp07...
>>> 1) Does this imply that the user accessing the ASP.Net system has to
be
>>>> using IE and Windows (We are looking for a way to do this regardless
> of
>>> the
>>>> browser) ?
>>>
>>> yes , cause kerberos only works inside the domain or trusted domain
>>> this should change in .net server
>>> <http://www.secdadministrator.com/Articles/Index.cfm?ArticleID=26450>..
>>>
>>> this is due the KDC (kerebros Distribution center is tied into the
>> AD -port
>>> 88)
>>> if u want to get a ticket outside the domain u have to proxy theTGT
> Ticket
>>> Granting Server to the Net , and Kerberize u're apps
>>>
>>> which u should do with web-services and ws-security/SAML
>>> there's a nice paper of that on
>>>
>>
>
<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwssecur/h>
>>> tml/securitywhitepaper.asp
>>>
>>>
>>> 2) If this is the case, does it mean that we will have to impersonate
> the
>>>> user on the ASP side when accessing the ServicedComponents ?
>>>
>>> depends on your scenario
>>> u can cloak the user, which means that the serviced components runs
> under
>>> his own identity (server) and uses this Identity too accses the
> Resources
>>> i use it this way a lot.
>>> if u're happy with that, it's ok
>>>
>>> in fact if u using a mandat based sql-server in which the data is
>> displayed
>>> in context of your role/Identity u'll have to use

> *impersonation/delegation*
>>> *to the remote server (3-tier)*
>>>
>>>
>>> 3.)
>>> *never done ...*
>>>
>>>
>>> "Cenon Del Rosario" <cenonmin@ihug.com.au> wrote in message
>>> news:en4gnAllCHA.1464@tkmsftngp07...
>>>> *Some questions:*
>>>> 1) *Does this imply that the user accessing the ASP.Net system has to*
> *be*
>>>> *using IE and Windows (We are looking for a way to do this regardless*
> *of*
>>>> *the*
>>>> *browser) ?*
>>>> 2) *If this is the case, does it mean that we will have to*
impersonate
>> *the*
>>>> *user on the ASP side when accessing the ServicedComponents ?*
>>>> 3) *If this is still the case, is it then easier to design and use*
our
>> *own*
>>>> *security system when doing checks at the ServicedComponent level ?*
>>>>
>>>> *Thanks.*
>>>>
>>>> "nu-k-ar" <nospam@plz.com> wrote in message
>>>> news:uewiX\$f1CHA.1216@tkmsftngp02...
>>>>> <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q325894>
>>>>>
>>>>> *By default, Microsoft Windows 2000 uses the Kerberos*
>>>>> *protocol for authentication. The Kerberos protocol supports*
> *delegation*
>>>> *and*
>>>>> *resolves an NTLM authentication limitation from Microsoft Windows*
NT
>>> 4.0.
>>>>> *This article explains how to use delegation in Windows 2000 with*
> *COM+.*
>>>>>
>>>>>> <http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q283201>
>>>>>>
>>>>>>
>>>>>>
>>>>>> "Cenon Del Rosario" <cenonmin@ihug.com.au> wrote in message
>>>>>> news:ubsytrf1CHA.1588@tkmsftngp02...
>>>>>>> *I was wondering if anyone can suggest a design for using ASP.Net*
>>>>>>> *together*
>>>>>>> *with ServicedComponents particularly in the area of security*

> *between*
>>> *the*
>>>>> > *two.*
>>>>>>
>>>>>> *Thank you.*
>>>>>>
>>>>>>
>>>>>
>>>>>
>>>>
>>>>
>>>
>>>
>>>
>>
>>
>
>