

Re: IIS6.0 + SSL Breaks down!

Source:

<http://www.tech-archive.net/Archive/Internet-Server/microsoft.public.inetserver.iis/2005-02/0638.html>

From: Jportelas (Jportelas_at_discussions.microsoft.com)

Date: 02/07/05

Date: Mon, 7 Feb 2005 05:45:04 -0800

Hi David:

Thanks for your time once again.

Your last reply is just fine, I called PSS the friday to solve this problem and we did it by increasing the "UploadReadAheadSize" and "AspBufferLimit" size.

I didn't know about the "SSLAlwaysNegoClientCert" variable but it seems to be a new path to follow when dealing with this kind of problems.

Thanks a lot once again.

Bye.

Jairo Portela S.

"David Wang [Msft]" wrote:

- > *Ok, I asked the IIS SSL developer, and he gave me the details.*
- >
- > *Bottom line: bad public specification on SSL make SSL Client Certificates*
- > *Authentication tricky.*
- >
- > *To avoid the deadlock when a client sends a large POST over SSL and IIS's*
- > *requirement to renegotiate Client Certificate:*
- > *1. Allow IIS to drain the incoming request. Set W3SVC/UploadReadAheadSize*
- > *(global) or W3SVC/SiteID#/UploadReadAheadSize (per site) to something larger*
- > *than the largest SSL POST (as documented)*
- > *2. Force IIS to always re-negotiate up front before client even thinks about*
- > *POSTing. Set W3SVC/SSLAlwaysNegoClientCert (global) or*
- > *W3SVC/SiteID#/SSLAlwaysNegoClientCert (per site) to "true"*
- >
- >
- > *FYI: The reason that IIS5 does not have this problem is because it has a bug*
- > *that happens to make it accidentally work. IIS6 fixed that bug such that the*
- > *behavior is not "accidental" but controllable, and the default IIS*

microsoft.public.inetserver.iis: Re: IIS6.0 + SSL Breaks down!

> configuration favors security -- thus can cause failures. But, it is better
> off on IIS6 because you can actually configure it to be secure and
> reasonably functional as spec'd -- vs the accidental behavior on IIS5.
>
> --
> //David
> IIS
> <http://blogs.msdn.com/David.Wang>
> This posting is provided "AS IS" with no warranties, and confers no rights.
> //
> "Jportelas" <Jportelas@discussions.microsoft.com> wrote in message
> news:CEC65EF8-ED7B-4325-875B-B855CFD7FF70@microsoft.com...
> Hi David:
>
> Thanks for the reply and the patience. Also thanks for the explanation on the
> SSL desing failure.
>
> Well, about me saying I was using client certificates, I did it in the first
> message right here as you can see down below:
>
> "This is my environment:
>
> Windows2003, IIS6.0, SSL + Client Certificates, .NET Fmk 1.1, All the
> current Fixes released by MS."
>
> So, me question now seems to be: how can I increase the "SSL ReadAhead"
> value to make it bigger than the POST size?? Is it possible?
>
> Thanks.
>
> Jairo Portela.
>
>
> "David Wang [Msft]" wrote:
>
> > I still suggest you contact PSS.
> >
> > The 413 issue you listed is actually NOT a bug in IIS6 -- behavior is
> > by-design -- the bug is actually in the SSL spec regarding client
> > certificates. The bad design in the public spec is that SSL is at the TCP
> > level while Client-Certificate (for authorization/authentication purposes)
> > is at the HTTP level or above. Literally, IIS needs to complete SSL
> > handshake before being able to decrypt the URL, only to see that Client
> > Certificate settings require a re-negotiation of the SSL handshake... so
> > what happens if the client already started sending a large chunk of entity
> > body via POST ???
> >
> > If IIS accepts the POST and the client certificate handshake fails, we
> > just
> > wasted bandwidth. If IIS rejects the POST, the client is confused. To
> > allow you to configure how much bandwidth you are willing to waste before

microsoft.public.inetserver.iis: Re: IIS6.0 + SSL Breaks down!

> > rejecting the request, that value is tied to the UploadReadAhead value --
> so
> > if the entity body is > SSL ReadAhead, IIS simply rejects the POST with a
> > 413; if the entity body is < SSL ReadAhead, IIS can read in the entity
> body
> > to unblock the client prior to re-negotiating.
> >
> > So, IIS6 behavior is actually quite reasonable given the bogus spec
> > requirement.
> >
> >
> > You haven't stated that you are using client certificates (which is
> > necessary to get into this situation), so I'm not certain you're even
> > looking at the right info. If the suggested solution doesn't work for you,
> > it probably is not related.
> >
> > --
> > //David
> > IIS
> > <http://blogs.msdn.com/David.Wang>
> > This posting is provided "AS IS" with no warranties, and confers no
> rights.
> > //
> > "Jportelas" <Jportelas@discussions.microsoft.com> wrote in message
> > news:2961784B-51ED-4AD8-BD3F-0608A5361815@microsoft.com...
> > This is a Follow up:
> >
> > I was checking on the site's IIS Log and I found that the 413 - 'Request
> > entity too large' shows up every time the blank page is displayed in the
> > client's browser, even the client just posts a few bytes... I think this
> is
> > related with a know bug of the IIS6 when the client can't re-negotiate the
> > client certificate
> >
> > (<http://www.microsoft.com/resources/documentation/iis/6/all/proddocs/en-us/q>
> > [ss_wss_troubleshooting.msp](http://www.microsoft.com/resources/documentation/iis/6/all/proddocs/en-us/q/ss_wss_troubleshooting.msp)),
> > so I tried to increase the "UploadReadAheadSize" to 500 KB (big requests
> is
> > about 140 KB) but it still keeps displaying blank pages from time to time.
> > An other thing I noticed is that when I navigate frequently (small
> intervals
> > between click and click) the page works ok, but when I wait more than 2-3
> > minutes, blank page shows up once again.
> >
> > Please help on this.... anyone..
> >
> > Thanx
> >
> > "Jportelas" wrote:
> >
> > > Hi:

Re: IIS6.0 + SSL Breaks down!

> > >
> > > *Found someone with the same problem:*
> > >
> > > [http://www.i-eye.net/archive/27889-Strange IIS and SSL problems.php](http://www.i-eye.net/archive/27889-Strange_IIS_and_SSL_problems.php)
> > >
> > > *Still nobody seems to know the answer to this problem, it seems like*
> *I'll*
> > > *have to contact PSS and Pay to get this situation fixed.*
> > >
> > > *Oh something else on the problem, it happens with Host headers and*
> *without*
> > > *them, so this doesn't seem to be an issue on the problem.*
> > >
> > > *Bye.*
> > >
> > >
> > > *"Jportelas" wrote:*
> > >
> > > > *Hi David:*
> > > >
> > > > *thanks for the reply.*
> > > >
> > > > *Ok, I think we'll contact PSS for support in this case.*
> > > >
> > > > *About your questions:*
> > > >
> > > > > *1. What mode do you run IIS6 in -- IIS5 Compatibility or IIS6 worker*
> > *process*
> > > > > *isolation mode : It's running in the IIS6 default, it should be IIS6*
> > *Wp.*
> > > >
> > > > > *2. Do you run any custom ISAPI Filters (written by you or installed by*
> > *other*
> > > > > *server apps) -- if yes, what are they, and what filter events do they*
> > *listen*
> > > > > *to. : no, we don't. We don't have any custom ISAPI Filters, only the*
> > *ones*
> > > > > *installed by ASP.NET 1.1.4322.*
> > > >
> > > > > *3. Are you getting blank pages on small or large SSL POST requests:*
> > *Only in*
> > > > > *large SSL Posts David.*
> > > >
> > > > > *I hope the SP1 for Windows2003 solves this, cause this never happened*
> > *under*
> > > > > *IIS5 and Windows 2000.*
> > > >
> > > > > *Thanks for the help, I really appreciate it.*
> > > >
> > > > > *Jairo Portela S.*
> > > >

>>>>
>>>> *"David Wang [Msft]" wrote:*
>>>>
>>>>> *If you think you are seeing a product bug, contact Microsoft PSS for*
>>>>> *support.*
>>>>> *– If there is a fix, they can diagnose it and give you the QFE.*
>>>>> *– If it is a new bug, they can diagnose it and get it into the*
> *product*
>>>>> *team's hands for evaluation.*
>>>>> *– If it is known, they may have work-arounds available*
>>>>>
>>>>> *I will also note that there were some fixes with SSL/Certificates*
> *that*
>> *are*
>>>>> *slated to release with WS03SP1 -- not certain if it fixes your*
>> *situation.*
>>>>> *However, due to how support works, you have to call PSS to have a*
>> *chance to*
>>>>> *get a QFE.*
>>>>>
>>>>>
>>>>> *There are a couple of things that I must also ask:*
>>>>> *1. What mode do you run IIS6 in -- IIS5 Compatibility or IIS6 worker*
>> *process*
>>>>> *isolation mode*
>>>>> *2. Do you run any custom ISAPI Filters (written by you or installed*
>> *by*
>> *other*
>>>>> *server apps) -- if yes, what are they, and what filter events do*
>> *they*
>> *listen*
>>>>> *to.*
>>>>> *3. Are you getting blank pages on small or large SSL POST requests*
>>>>>
>>>>> *--*
>>>>> *//David*
>>>>> *IIS*
>>>>> *<http://blogs.msdn.com/David.Wang>*
>>>>> *This posting is provided "AS IS" with no warranties, and confers no*
>> *rights.*
>>>>> *//*
>>>>> *"Jportelas" <Jportelas@discussions.microsoft.com> wrote in message*
>>>>> *news:1F810F7C-DBD3-484A-9436-140DC47EBFF8@microsoft.com...*
>>>>> *Good morning:*
>>>>>
>>>>> *This is my environment:*
>>>>>
>>>>> *Windows2003, IIS6.0, SSL + Client Certificates, .NET Fmk 1.1, All*
>> *the*
>>>>> *current Fixes released by MS.*
>>>>>
>>>>>

microsoft.public.inetserver.iis: Re: IIS6.0 + SSL Breaks down!

>>>> *I have a production server that has some really big pages (lots of
>> data),
>>>> from time to time (but becoming more frequent everytime) I get blank
>> pages,
>>>> but requests never reach the .NET pages, the IIS replies with empty
>> HTML as
>>>> the one copied at the end of this message. I was reading on a forum
>> about a
>>>> similar
>>>>
>>
> case([http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.sec
>>>> urity/2003-08/0867.html](http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2003-08/0867.html)),
>>>> the proposed solution is not to use 'Client Certificates', and it
>> really
>>>> works!!! but I really need to use Client certificates? is there any
>> way to
>>>> work around this problem? any QFE package I can get?
>>>>
>>>> <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
>>>> <HTML><HEAD>
>>>> <META http-equiv=Content-Type content="text/html;
>>>> charset=windows-1252"></HEAD>
>>>> <BODY></BODY></HTML>
>>>>
>>>>
>>>> < i>Thanx for any help.
>>>>
>>>>
>>>>
>>
>>
>>
>
>
>*