

Re: IIS 6.0 and 401.2 and 401.1 Errors

Source:

<http://www.tech-archive.net/Archive/Internet-Server/microsoft.public.inetserver.iis/2004-11/0083.html>

From: David Wang [Msft] (*someone_at_online.microsoft.com*)

Date: 11/01/04

Date: Mon, 1 Nov 2004 14:35:53 -0800

Make sure that the Netmon capture is done between two machines -- not from host to itself.

Virtual PC has some interaction with the networking stack -- I recommend running NetMon on the non-Virtual PC machine involved to capture network traffic.

The capture should be small enough to send as attachment or HTTP URL link for download.

```
--
//David
IIS
This posting is provided "AS IS" with no warranties, and confers no rights.
//
<hpux9@nospam.nospam> wrote in message
news:E34B03B1-B833-4576-A5CE-480543656CE7@microsoft.com...
I ran some packet traces yesterday. Is there some way I can mail them
directly to you? I am doing my testing in virtual PC, and not using NLB.
The logs look the same so I guess we can rule out #1 below.
Thanks for the good information!!!
"David Wang [Msft]" wrote:
> Additionally, you should realize that NTLM is connection-based
> authentication -- client and server first negotiate authentication that
> first time as described earlier, and then subsequent requests over that
> authenticated connection is considered "authenticated" and directly
succeed.
>
> So, if you see repeated 401.2 for the same resource from the same client,
it
> means that the client and server are NOT keeping their previously
> authenticated connection and instead RENEGOTIATING a new connection. It
is
> this unnecessary renegotiation that is causing extra authentication trips
> and draining throughput.
>
> You can easily verify this by installing "Network Monitor" from Windows
> Server 2003 Add/Remove Programs, Windows Components and then watch the
> traffic between two distinct client/server machines. You will see the
> client and server continuously renegotiate and use different ports, which
> constitute different connections, and each are getting re-authenticated.
>
> Now, NTLM requires "connection keep-alive" to be enabled to function, and
```

microsoft.public.inetserver.iis: Re: IIS 6.0 and 401.2 and 401.1 Errors

```
> IIS6 will aggressively maintain connection keep-alive status whenever
> possible -- so repeated re-negotiation can suggest:
> 1. The load balancer is not maintaining clients to talk to the same web
> server (to minimize number of connection [hence authentication] attempts)
> 2. The application is explicitly closing connections (which IIS6 will
obey)
> 3. Browser uses HTTP Pipelining inefficiently -- I have observed this from
> IE with IIS6 and any authentication
> 4. Product bug in IIS6 regarding keep-alive
>
> Network Monitor is pretty much the only direct way you can distinguish
> between the above four possibilities. You will need to post a network
> capture illustrating the issue.
>
> --
> //David
> IIS
> This posting is provided "AS IS" with no warranties, and confers no
rights.
> //
> "WenJun Zhang[msft]" <v-wzhang@online.microsoft.com> wrote in message
> news:E45tg3VvEHA.2692@cpmsftngxa10.phx.gbl...
> Hi,
>
> This is expected behavior. The 401.2 and 401.1 response code isn't an
> error here. They come from 2 causes:
>
> 1) IE always tries anonymous access before than any kind of
> authentication attempts.
>
> 2) The 2nd 401.1 response is a part of the integrated authentication
> handshake.
>
> An entire integrated auth handshake(NTLM) need exchange 3 parts of
> hash between the server and client, which cannot be finished in 1
> http request/response.
>
> The whole scenario of NTLM is like:
>
> IE -----> IIS (anonymous access attemp)
>
> IE <----- IIS (401.2 authentication failed due to server
> configuration, list all allowed auth type in response header)
>
> IE -----> IIS (NTLM auth, the 1st hash)
>
> IE <----- IIS (401.1, the 2nd hash)
>
> IE -----> IIS (the 3rd hash)
>
> IE <----- IIS (200 or 304, authenticated)
>
> That's the reason why we always see the 401.2 - 401.1 - 200 sequences
> in IIS log. It's quite normal. :-)
>
> Best regards,
>
> WenJun Zhang
> Microsoft Online Support
> This posting is provided "AS IS" with no warranties, and confers no
> rights.
> Get Secure! - www.microsoft.com/security
```

microsoft.public.inetserver.iis: Re: IIS 6.0 and 401.2 and 401.1 Errors

>
>
>