

## Re: Windows authentication query

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2004-04/0269.html>

---

**From:** Ken Schaefer (*kenREMOVE\_at\_THISadOpenStatic.com*)

**Date:** 04/13/04

Date: Tue, 13 Apr 2004 19:06:51 +1000

Hi,

Kerberos Authentication works fine with FQDN. The reason that it is commonly mentioned as not working over the internet is that the client (IE) needs to be able to contact the KDC (Key Distribution Center – a Domain Controller in the Windows world) in order to get the Kerberos tickets (TGT and Session Tickets). Usually, a client on the internet would not be able to connect to a DC because a firewall would be in the way (or IPSec rules or similar would prevent internet based clients from connecting to the internal DCs)

There is a bug in IIS5 where it sends the Negotiate and NTLM headers in the wrong order, resulting in IE picking NTLM instead of Kerberos, but that is fixed in IIS6.0. In IIS5.0 I can't remember when it was fixed. Verify that IE is using Kerberos not NTLM.

The KB article cited in the URL you posted is no longer available. I also don't believe that it's accurate (i.e. I think it's wrong).

Cheers  
Ken

"Madhu Gopinathan" <madhugops@rediffmail.com> wrote in message news:up9vGETIEHA.828@TK2MSFTNGP12.phx.gbl...

: Hi Ken,

: Yes, ideally setting the SPN should be fine, but it did not work.

: Seemingly, IE checks the path for "." in the path, and decides that any

: dotted path does not belong to the intranet, resulting in the error for

: cases of Windows authentication (because, Windows authentication cannot span

: over an intranet).

: This possibility was suggested from the link below

:

: <http://www.netsys.com/fwtk/2000/11/msg00000.html>

:

: Could that be the case? Because adding the FQDN and the IP address to the intranet sites did solve the problem.

:

: WRT the trust problem, I faced the problem in both the cases, one-way

as  
: well as two-way.  
:  
: Thanks again,  
: Madhu  
:  
: "Ken Schaefer" <kenREMOVE@THISadOpenStatic.com> wrote in message  
: news:#rNgrkSIEHA.940@tk2msftngp13.phx.gbl...  
: > Hi,  
: >  
: > Setting an SPN once should be enough in most cases. Why is it a "per  
: client"  
: > setting in your case? The Kerberos ticket must have an SPN, and when you  
: > install IIS, only the NetBIOS name of the IIS server is registered with  
: the  
: > KDC. The use of SetSPN allows you to register other service names (e.g.  
a  
: > FQDN) with the KDC (i.e. with your Domain Controllers). so you'd have to  
: do  
: > this once for each FQDN that IIS is using, and once for each FQDN of the  
: > remote service(s) that IIS has to access.  
: >  
: > Let me investigate WRT to question 2. Do you have a two-way trust? or  
just  
: a  
: > one-way trust? (I'm not whether that's relevant, but it's the only think  
I  
: > can think off OTOH)  
: >  
: > Cheers  
: > Ken  
: >  
: >  
: > "Madhu Gopinathan" <madhugops@rediffmail.com> wrote in message  
: > news:u%23ejacSIEHA.3848@tk2msftngp13.phx.gbl...  
: > : Hi Ken,  
: > : Thanks for your prompt reply. I investaigated the links you sent,  
: and  
: > it  
: > : started working when I started using the NetBIOS name of the IIS  
: machine.  
: > : Thanks a million!!  
: > :  
: > : However, I have a few further queries, and I hope you can solve  
them  
: > for  
: > : me.  
: > : 1. Just adding the SPNs using SetSPN was not enough for using IP  
address  
: > and  
: > : FQDNs in my machine path. I had to add the IP address and the FQDN of

: the  
: > : IIS server in the list of sites that would be available in the  
intranet.  
: > : Since this is a per-client setting, this would be a cumbersome  
solution.  
: > Is  
: > : there any way for accesses to sites using IP address and FQDNs without  
: > : having to resort to a per-client setting? Maybe a GPO level setting or  
: > : something?  
: > :  
: > : 2. Delegation is succeeding only for users accounts residing in the  
same  
: > : domain as the IIS server. For users from trusted domains, the  
: > impersonation  
: > : level is Impersonate and not Delegate. I verified this by examining  
the  
: > : impersonation level of the thread token in the DLLHOST process. Is  
there  
: > : something still amiss in my settings somewhere? Is it not supposed to  
: > : delegate credentials from domains trusted by the domain that the IIS  
: > server  
: > : resides in?  
: > :  
: > : Thanks again,  
: > : Madhu  
: > :  
: > : "Ken Schaefer" <kenREMOVE@THISadOpenStatic.com> wrote in message  
: > : news:OIWOp#GIEHA.3536@TK2MSFTNGP09.phx.gbl...  
: > : > Hi,  
: > : >  
: > : > You need to configure both the computer and user accounts for  
: > delegation.  
: > : > Then you may need to use the SetSPN.exe tool to register the service  
: > : > principal name if you are accessing the site under anything other  
than  
: > the  
: > : > NetBIOS name of the machine. Try the following links:  
: > : >  
: > : > <http://support.microsoft.com/default.aspx?scid=kb;en-us;810572>  
: > : > HOW TO: Configure an ASP.NET Application for a Delegation Scenario  
: > : >  
: > : > <http://support.microsoft.com/?id=294382>  
: > : >  
: > : > Authentication May Fail with "401.3" Error If Web Site's "Host  
Header"  
: > : > Differs from Server's NetBIOS Name  
: > : >  
: > : > <http://support.microsoft.com/default.aspx?kbid=325894>  
: > : > HOW TO: Configure Computer Accounts and User Accounts So That They  
Are  
: > : > Trusted for Delegation in Windows Server 2003 Enterprise Edition

(also

:> :> includes Windows 2000 instructions)

:> :>

:> :>

:> :> Cheers

:> :> Ken

:> :>

:> :>

:> :>

:> :> "Madhu Gopinathan" <madhugops@rediffmail.com> wrote in message

:> :> news:erhW21GIEHA.3848@tk2msftngp13.phx.gbl...

:> :> Hi,

:> :> I have a setup of IIS 5.0 on a Windows 2000 server. I have  
created

: a

:> : web

:> :> site to run under Windows authentication. The default asp in this  
site

:> :> accesses active directory objects. Now I want this setup to support  
delegation, so I have trusted the computer account of the IIS server

: for

:> :> delegation and made sure that the user being delegated is not a

:> sensitive

:> :> account. However, in my event viewer on my DC (which is not the IIS

:> : server),

:> :> I get logon/logoff events under ANONYMOUS LOGON context.

:> :>

:> :> What is wrong here? I have tried everything to get a delegation

:> setup,

:> :> however it just does not seem to succeed. I have also updated the

:> :> EnableNegotiate key on the client browser machine, this also does

not

:> : help.

:> :>

:> :> Thanks,

:> :> Madhu

:> :>

:> :>

:> :

:> :

:>

:>

:

: