

## Re: Kerberos delegation

---

*Source:*

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2006-12/msg00039.html>

---

- *From:* "Joe Kaplan" <[joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Thu, 7 Dec 2006 12:10:28 -0600
- 

If I had to guess, I'd say that some of your web browser users are getting Kerberos authentication successfully, but some of them are not and are getting NTLM authentication with IIS. That breaks Kerberos delegation.

To verify this, enable logon auditing on the web box and try to correlate the failures with security event log logon events that indicate an NTLM logon.

To fix this may be difficult, as the negotiate protocol is designed to select NTLM if Kerb isn't available. The first thing to do is to try to figure out what is different that is preventing Kerb from working. SPN problems are the root of many Kerberos auth failures, but if everyone uses the exact same host name in the URL for the web app, that should not be happening. Sometimes there may be a problem with connecting the DC on the Kerberos port (88), so that might be another thing to look at.

You can get more flexibility if you can migrate to 2003 server (and 2003 native AD) because then you could use protocol transition on the web tier and it wouldn't matter why type of authentication the browser client got (could be basic or digest as well as NTLM or Kerberos). However, that might not be an option for you.

Best of luck figuring this out. Unfortunately, troubleshooting these can be very painful. There is an excellent document on TechNet called something like "Troubleshooting Kerberos Errors" that actually covers all of this stuff in a lot of detail. I'd suggest finding it and reading it.

Joe K.

--

Joe Kaplan-MS MVP Directory Services Programming  
Co-author of "The .NET Developer's Guide to Directory Services Programming"  
<http://www.directoryprogramming.net>

--

"Scott Elgram" <[SElgram@xxxxxxxxxxxxxxxx](mailto:SElgram@xxxxxxxxxxxxxxxx)> wrote in message  
[news:O4PHOiiGHHA.3468@xxxxxxxxxxxxxxxx](mailto:news:O4PHOiiGHHA.3468@xxxxxxxxxxxxxxxx)

Hello,

Re: Kerberos delegation

I'm not sure if this is the right forum for this question but it is security related so hopefully someone in here can help.

I have two servers,

Web01: Windows 2k Adv. Server running IIS 5.

Sql01: Windows 2k Adv Server Running SQL 7

I am trying to get user credentials to flow through Web01 to Sql01 so that I can make use of the permissions that are already on the tables.

For

the most part, about 70% of the time, everything is working just peachy and

there are no issues. However, that remaining 40% people are receiving the following error:

---

Message: Login failed for user 'NT AUTHORITY\ANONYMOUS LOGON'.  
Stack Trace: at  
System.Data.SqlClient.ConnectionPool.GetConnection(Boolean& isInTransaction)  
at  
System.Data.SqlClient.SqlConnectionPoolManager.GetPooledConnection(SqlConnection options, Boolean& isInTransaction)  
at System.Data.SqlClient.SqlConnection.Open()  
at DataCollections.DirectEdit.AddPractice.Page\_Load(Object sender, EventArgs e)  
at System.Web.UI.Control.OnLoad(EventArgs e)  
at System.Web.UI.Control.LoadRecursive()  
at System.Web.UI.Page.ProcessRequestMain()

---

If I turn on auditing of successful logons for both Web01 and Sql01 I can follow the flow down to Sql01 where I find the following entry in the security log:

---

Date: 12/06/2006 Source: Security  
Time: 14:52 Category: Logon/Logoff  
Type: Success Event ID: 538  
User: NT AUTHORITY\ANONYMOUS LOGON  
Computer: Sql01  
Description:  
User Logoff:  
User Name: ANONYMOUS LOGON  
Domain: NT AUTHORITY  
Logon ID: (0x0,0x6B5095F)  
Logon Type: 3

---

If anyone can offer any advice on why this is only happening some of the time or how to fix/further trouble shoot this issue would be greatly appreciated.

Thanks,

---

Re: Kerberos delegation

-Scott