

## Re: kerberos the story so far

---

*Source:*

[http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active\\_directory/2005-10/msg00505.html](http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2005-10/msg00505.html)

---

- *From:* "Laurence" <[laurence.pull@xxxxxxxxxxxxxxxxxxxx](mailto:laurence.pull@xxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Thu, 20 Oct 2005 09:28:54 +0100
- 

Sorry for the slow reply Brandon, thanks for your information

I have put the IIS machine into a local group and assigned it owner in the appropriate database.

One the I have noticed is that running the AuthDiag tool on the SQL box says that the Domain\IIS\_WPG group does not have 'Impersonate a client after authentication' priviledges. This is a group policy setting – so how do i set this for a domain\group on a specific server

"Brandon McGarvey" <[BrandonMcGarvey@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:BrandonMcGarvey@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message [news:DE64500D-33E7-40A1-B19F-D184F820AEAC@xxxxxxxxxxxxxxxxxxxx](mailto:news:DE64500D-33E7-40A1-B19F-D184F820AEAC@xxxxxxxxxxxxxxxxxxxx)

- > Did you get my reply on the message you posted yesterday? I encountered
- > this
- > same issue, where my IIS front end server could not obtain a kerberos
- > ticket
- > for the SQL back end. I was getting "Login failed for user 'null'".
- >
- > It looks like you registered the SPN for the SQL service user account. Did
- > you make sure you granted the IIS server's domain account permissions to
- > the
- > database?
- >
- > To do this, create a new local group on the SQL server. Go into the group
- > like you are adding a user. In the "Select Users..." window, click the
- > "Object Types" button and check the "Computers" box and hit OK. Type in
- > the
- > name of the IIS server below, and click "Check Names" to verify the
- > object,
- > and hit OK to add the computer to the group. In SQL, simply grant that
- > local
- > group whatever access rights (public, dbo, etc.) it needs to the database.
- > Now try to authenticate to the db from the IIS server.
- >
- > "Laurence" wrote:
- >
- >> Hi,

Re: kerberos the story so far

>>  
>> I have been pulling my hair out for ages on this one, so please help.  
>>  
>> I am trying to connect to a SQL server throu IIS using impersonation.  
>>  
>> I am sure I have done 99% of what is needed to do this and still can not  
>> get  
>> it to work.  
>>  
>> So what have I done.  
>>  
>> I have a pure 2003 domain  
>> I have DNS configured and working (as far as I can see correctly)  
>> I have set all the computers to be able to delegat  
>> I have set all the computer accounts to be able to delegate  
>> I have a web site based in windows sharepoint services that works quite  
>> happily when only doing a single hop.  
>> I have used the adsutil.vbs to set the NTAAuthenticationProvider to  
>> Negotiate,NTLM  
>> I have made sure the SQL server service account has an SPN  
>>  
>> using ADSI edit on the service account user the servicePrincipalName  
>> looks  
>> like this  
>>  
>> MSSQLSvc/MYSQLServer.MyDomain.CO.UK:1433  
>>  
>> However when I try to do a double hop I get the dreaded 'Login failed for  
>> user (null)' – implpying its a double hop issue.  
>>  
>> I have set SPN's (I think) for all services and users.  
>>  
>> Using the Microsoft AuthDiag diagnostic tool (after much sorting out), I  
>> get  
>> no error messages for keberos authentication. HOORAY!  
>>  
>> But I still can't get to the SQL server....AAAAAAAAAAAAHHH  
>>  
>> So where from here....  
>>  
>> 1). monitoring the IIS connection with the default login, it seems to be  
>> using Negotiate protocol but defaulting back to NTLM  
>> 2). If you force a kerberos windows login the IIS seems to use kerberos  
>>  
>> bot I still don't know if I am getting a kerberos ticket issued ???  
>> or  
>> do I still not have rights from the iis machine \ a user to get to the  
>> sql  
>> server  
>>  
>> any assistance appreciated

Re: kerberos the story so far

Re: kerberos the story so far

>>  
>>  
>>  
>>

.

---

• **References:**

- ◆ **kerberos the story so far**  
    ◇ From: Laurence
- ◆ **RE: kerberos the story so far**  
    ◇ From: Brandon McGarvey

- Prev by Date: **Re: New user accounts**
- Next by Date: **Re: AD not inheriting admin permissions**
- Previous by thread: **RE: kerberos the story so far**
- Next by thread: **Re: Removing domain local groups from Wind XP local administrato**
- Index(es):
  - ◆ **Date**
  - ◆ **Thread**