

impersonation, SQL und mein Verstand...

Source: <http://www.tech-archive.net/Archive/German/microsoft.public.de.sqlserver/2007-01/msg00159.html>

- *From:* "carsten lahme" <carsten@xxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 8 Jan 2007 18:13:16 +0100
-

.... der langsam über den Jordan geht!

Tach zusammen,

folgende Ausgangssituation:

W2k3 Domäne

W2k3 SP1 Server mit SQL 2000 SP4

W2k3 SP1 Server mit IIS 6

Bisher habe ich Datenbankapplikationen immer auf einem Server laufen lassen (Web und SQL zusammen) was die Anmeldung leicht machte. Jetzt möchte ich endlich von diesem System runter und ordentlich trennen. Das hat aber ein kleines Problem eröffnet. Die Anwender sollen keine interaktive Anmeldung beim Benutzen der Applikation erfahren (integrated Authentication). Https möchte ich an dieser Stelle auch nicht verwenden –Basic Auth mit SSL würde das Problem lösen, ich weiß.

Ich möchte auch nicht, daß die Datenbankverbindung über einen dedizierten Account geführt wird.

Der Benutzer soll am IIS angemeldet werden und der soll das Token an den SQL Server weitergeben.

Bisher habe ich folgendes unternommen:

Im ApplicationPool des IIS eine Applikation angelegt, welche mit der Identität eines Domänen Benutzers läuft (WP_Shiftplaner)

Der Benutzer ist Mitglied der lokalen Gruppe IIS_WPG.

Das Web mit der Applikation wurde dem Pool zugeordnet.

Das Web steht auf Integrated Auth only.

Im eventlog des Webservers sehe ich, das der WP_Shiftplaner erfolgreich anmeldet.

Ebenso sehe ich, wenn ich das Web auf meiner Workstation lade, daß ich an dem WEB-Server angemeldet werde.

Auf dem SQL-Server hingegen kommt eine Anonymous Anmeldung und damit die Meldung im Web:

Microsoft OLE DB Provider for ODBC Drivers Fehler "80040e4d"

[Microsoft][ODBC SQL Server Driver][SQL Server]Fehler bei der Anmeldung für den Benutzer '(null)'. Ursache: Keiner vertrauten SQL Server-Verbindung zugeordnet.

In der Web.Config steht

```
<configuration>  
<system.web>  
<compilation debug="true" />  
  
<authentication mode="Windows"/>  
<identity impersonate="true"/>  
  
</system.web>  
</configuration>
```

Mittlerweile habe ich

<http://support.microsoft.com/kb/319723/en-us>

und

<http://support.microsoft.com/kb/215383/en-us>

studiert und ausgeführt.

leider bringt auch das Sampel nur ein Benutzer 'NUL' zurück.

KerbTray zeigt Tickets an aber die Anmeldung am IIS btw am SQL kommen immer noch mit NTLM.

Allerdings ist mir in dem Artikel aufgefallen, daß hier dem SQL-Account Delegationsrecht gegeben wird. Müsste es nicht umgekehrt sein und dem IIS Account vertraut werden?

Ist die Welt doch eine Scheibe?

verwirrter Gruss

Wo liegt mein Fehler?

Dank und Gruss

Carsten

PS: Dieses ist kein Crosspost. Ich habe zwar einen identischen Thread im IIS.ASP aufgemacht, aber vielleicht könnt Ihr SQLer ja auch noch etwas beitragen.

.