

Re: How can I avoid using SQL Authentication with the Office Web Parts?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2005-01/0319.html>

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

Date: 01/29/05

Date: Sat, 29 Jan 2005 04:29:40 -0800

I've not directly dealt with your stated situation, but I'd like to offer some viewpoints that can hopefully point you to the right direction.

I think your problem is caused by the fact that your extranet users authenticate using Basic, yet you tell the web page (and web part) to authenticate via another authentication protocol (Integrated) to the backend SQL server. I'm not certain how IIS is supposed to translate between different authentication protocols unless you use something like protocol transition (see the URL below)

Although the following URL talks about IIS6 and UNC shares, the underlying issues that it addresses is the same that you face with SQL. Namely, user authenticates to IIS, which must authenticate to some remote server to access a resource (be it a UNC share or SQL).

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/webapp/iis/remstorg.mspix>

Your situation sounds like protocol transitioning is the solution.

FYI: using Integrated authentication with IIS6 in a domain will use Kerberos by default. So, you already have half the puzzle all set up (as evidenced by Intranet access working). Protocol transition allows IIS to take the basic auth'd credential and get a kerberos ticket out of it, so that kerberos can be used in Integrated authentication to access SQL.

--

//David

IIS

<http://blogs.msdn.com/David.Wang>

This posting is provided "AS IS" with no warranties, and confers no rights.

//

"DarrylR" <darrylr@nosspam.com> wrote in message

news:%23p3Iw6YBFHA.1452@TK2MSFTNGP11.phx.gbl...

We have a machine running Windows 2003 Server, IIS 6, and Windows SharePoint Services. The machine resides in our DMZ (outside the firewall), and is on a separate domain that has a one-way trust relationship with our intranet domain (separate forest; the extranet domain trusts accounts from our intranet domain).

We've created 2 separate virtual directories for a particular WSS site. The

microsoft.public.inetsrv.iis.security: Re: How can I avoid using SQL Authentication with the Office Web Parts?

virtual directory used internally uses Integrated Windows authentication. The one used by extranet users uses Basic authentication over SSL. Neither virtual directory has Kerberos Authentication enabled. The web.config files in both virtual directories contain the <authentication mode="Windows" /> and <identity impersonate="true" /> elements.

We are using Office Web Parts (specifically the PivotView) on several Web Part pages to display data retrieved from a SQL Server (SQL 2000 SP3 running under Windows 2000 Server SP4 on a different machine located behind our firewall, member of the intranet domain). The pages with Office Web Parts on them work correctly when accessed via our intranet (only from machines that belong to the intranet domain); users are logged on seamlessly using their domain credentials, and the PivotViews retrieve data correctly. When we access these pages via our extranet (or from a machine that is currently on the intranet but isn't a member of the intranet domain), even if the user supplies valid domain credentials when challenged by the WSS site, the Office Web Parts fail to retrieve data. According to SQL Profiler, this is due to a SQL login failure ("Login failed for user '(null)'. Reason: Not associated with a trusted SQL Server connection.").

Incidentally, I get the same error when I try to access the same SQL Server box using Windows Authentication from within Query Analyzer if I'm not logged in using domain credentials. Could it be that the Office Web Parts use your current identity despite what you supply when challenged by IIS? If so, how can I get them to use the credentials that I supply during the NTLM/Basic challenge?

We've opened the generally accepted ports on the firewall to support SQL Server (at least we know that WSS is able to access the SQL Server box to deliver all other portal content). The Office Web Parts fail to login (from the extranet) when we use connection strings similar to the following:

```
Provider=SQLOLEDB.1;Integrated Security=SSPI;Persist Security
Info=False;Initial Catalog=ourDB;Data Source=ourSQLserver;
Provider=SQLOLEDB.1;Trusted_Connection=Yes;Persist Security
Info=False;Initial Catalog=ourDB;Data Source=ourSQLserver;
```

So far, the only way that we've been able to get this to work from the extranet has been to use SQL Authentication and a connection string similar to the following:

```
Provider=SQLOLEDB.1;Persist Security Info=True;User
Id=ourUserId;Password=ourPwd;Initial Catalog=ourDB;Data Source=ourSQLserver;
```

Obviously, we'd rather not use SQL Authentication, since the Office Web Parts write the connection string to the page, where it is readable in the browser using the View/Source command. I researched the problem and discovered the following article (among others) which looked promising:

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/vbcon/html/vbtskaccessinqsqlserv>

However, the steps outlined in the article didn't correct the problem. I've also seen references to Kerberos authentication that suggest that it could solve the problem. However, rather than plow blindly ahead, I thought I'd seek input.

Any suggestions?

Thanks,
Darryl R.