

Re: PROBLEM: ASP on IIS 5 secured via "Windows Integrated Authentication" accessing "Integrated Security" SQL Server (seperate boxes)

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2002-10/4822.html>

From: Tom Rogers (rogerst@approach.com)

Date: 10/10/02

From: "Tom Rogers" <rogerst@approach.com>

Date: Thu, 10 Oct 2002 09:19:49 -0400

That helps a lot. I assumed we were doing everything correctly.

I will try to push our customer towards using Basic Auth no the server...the only issue that I see for them is that they will get the password popup, as we will still map the authentication to the domain accts. But, the customer really wanted to use "Integrated Security" to avoid the logon dialog for their internal users.

The customer has already invested heavily into a design and strategy that uses NT group based permissons on the SQL Server, so moving to SQL Security in our ADO connections really isn't an option.

Regards,

Tom Rogers

Approach Inc.

"Thomas Deml [MS]" <thomad@online.microsoft.com> wrote in message news:e0vBE1BcCHA.2624@tkmsftngp09...

> Tom,

>

> I answered the question in a similar thread (you might want to look for it).

>

> In a nutshell:

>

> Delegation is a very privileged operation an is therefore disabled by

> default. Let's suppose you are the author of the ASP page and you get an

> Domain Administrator to enter your URL in the browser. Windows Integrated

> authentication would automatically authenticate the domain admin. Now you

> could do whatever you want in your ASP page on behalf of the Domain Admin.

> For him it looks like you're going against a SQL Server but under the covers

> you could create a new domain account with Domain Admin privileges.

> Therefore it works only on the local box and as soon as you try to hop

Re: PROBLEM: ASP on IIS 5 secured via "Windows Integrated Authentication" accessing "Integratdd Security"

er.iis.security: Re: PROBLEM: ASP on IIS 5 secured via "Windows Integrated Authentication" accessing "Integrated Security"

onto

> *the network you get downgraded to an anonymous user.*

>

> *Workarounds:*

>

> *1) use Basic auth (over SSL). In this case the username/password get*

> *transferred to the IIS box and IIS does a local logon. You buy yourself*

> *another hop. With all other protocols no credentials (username/password)*

are

> *transferred and the user identity can't be proven.*

>

> *2) make sure you have a Kerberos end-to-end infrastructure and enable*

> *delegation for all accounts. Risky. The best description how to do this*

can

> *be found in Michael Howards book "Designing Secure Web-based applications"*

> *2) pass the user as a SQL parameter and do your authorization logic in*

SQL

> *server*

>

> *3) if you only have a few users use local accounts (domain accounts won't*

> *work) and create them on the IIS box as well as on the SQL box. Have the*

> *same passwords! Due to the nature of Windows auth it would work. Keep the*

> *accounts in sync.*

>

> *4) use Windows.NET and IIS 6.0. We have a feature in Windows.NET called*

> *"constrained delegation". As a domain admin you can specify to which*

> *machines another machine can delegate to. In your case you would configure*

> *that the IIS Box can delegate to the SQL box. Only delegation to the SQL*

box

> *would succeed and all other delegation attempts would fail. Plus: You can*

> *come in with whatever protocol you want (digest, basic, windows auth, ssl*

> *client certs).*

>

> *Hope this helps.*

>

>

> --

> *Thomas Deml*

> *Lead Program Manager*

> *Internet Information Services*

> *Microsoft Corp.*

>

>

> *"Tom Rogers" <rogerst@approach.com> wrote in message*

> *news:u88rnp8bCHA.2524@tkmsftngp10...*

> *> Here is our scenario:*

> >

> > *o We have a W2K domain.*

> >

> > *o We have a W2K IIS 5.0 server in the domain (one machine).*

> > *– It has a website secured via "Windows Integrated authentication"*

Re: PROBLEM: ASP on IIS 5 secured via "Windows Integrated Authentication" accessing "Integrated Security"

er.iis.security: Re: PROBLEM: ASP on IIS 5 secured via "Windows Integrated Authentication" accessing "Integrated Security"

> > – ASP pages load just fine, that's not our problem.
> >
> > o We have a SQL 2K server in the domain (seperate machine).
> > – It has been set up in mixed mode security.
> > – We can use query analyzer to hit the web apps database on the
> machine
> > using integrated
> > security and the credentials of a web user, that's not our
problem.
> >
> > The problem is that when we run ASP pages on the IIS box that hit the
SQL
> > box via ADO, we get the infamous error:
> > Microsoft OLE DB Provider for ODBC Drivers error '80040e4d'
> > [Microsoft][ODBC SQL Server Driver][SQL Server]Login failed for user 'NT
> > AUTHORITY\ANONYMOUS LOGON'.
> >
> > It seems that the token/credentials that are being used for the login to
> the
> > website are not making their way to the SQL server via the ADO
connection.
> > This works JUST FINE if we use Basic Authentication.
> >
> > We have tried AD delegation between the servers and that didn't help. I
> > tried mucking with IUSR, but we really don't want anonymous access to
our
> > site.
> >
> > I have spent most of the day reading newsgroups about this problem. AD
> > delegation seems to be the way to solve it, but it didn't help in our
> case.
> > Of course, going back to Basic Authentication would solve the problem or
> > combining the SQL Server and IIS Server on the same box would solve the
> > problem...but those are available options for us.
> >
> > Regards,
> >
> > Tom Rogers
> >
> >
> >
>
>

Re: PROBLEM: ASP on IIS 5 secured via "Windows Integrated Authentication" accessing "Integrated Security"