

## Re: Integrated Windows Authentication Timeout?

---

*Source:*

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2007-04/msg00017.html>

---

- *From:* Bradley Landis <[BradleyLandis@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:BradleyLandis@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Thu, 5 Apr 2007 14:20:04 -0700
- 

Thanks Joe,

I had no problem running the query. I think we did have some extra SPNs in there so we removed them.

Now when I do the first search, I only see HTTP/<WEBSERVER> and HTTP/<WEBSERVER>.<DOMAIN>.COM

When I do the second search you gave me, I get 0 results. Which I think is correct.

We are still having the problem.

Another problem we encountered was when we set the "Impersonate client after authentication" on our domain policy, many users experienced issues where programs that required administration privileges to run no longer functioned. These included virus scan, windows desktop search, word as e-mail editor, etc. So we took that out of the domain policy and are in the process of adding it to the local policy now. We cannot figure out why that would have affected users so badly. Any ideas there?

"Joe Kaplan" wrote:

I use an ldap query tool like ldp.exe to do this. If you do a search for the object in question (the user account) with a filter like:

(sAMAccountName=xxxxx)

where xxxxx is the username of the user account that runs the service. Have the LDAP search return these attributes:

servicePrincipalName;userAccountControl;msds-allowedToDelegateTo

You should then be able to see the SPNs that are on that account. The servicePrincipalName is the key value, but userAccountControl allows you to see what delegation permissions the account has and msds-allowedToDelegateTo shows what (if any) constrained delegation values are applied.

Re: Integrated Windows Authentication Timeout?

There is a chance that you have a duplicate SPN here with the machine account and that could be a problem. Searching with a filter like:

(servicePrincipalName=xxxxx)

where xxxxx is the NetBIOS SPN in question should reveal that. You should do the search at the global catalog level though if you have multiple domains in your forest.

I might be assuming too much if you've never done much LDAP searching though, so let me know and I'll try to provide more details if that info wasn't sufficient.

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>

---

"Bradley Landis" <BradleyLandis@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message  
<news:39E66674-BCDB-4788-A315-EFFC6691AC2F@xxxxxxxxxxxxxxxxxxxx>

Yes thank you very much for the info about the 30 minute behavior in IE.

I

think that is definitely related. But I do believe that we have both the FQDN and the NetBios set up with SPNs. One thing we cannot figure out is how to list them since they are associated to a domain account.

setspn -L <COMPUTER NAME>

will list them for the default account of the computer but doesn't seem to show those for the domain account.

Anyone know how to list them for the domain account?

"Joe Kaplan" wrote:

That's interesting info. Thanks Henning!

I think the behavior IE is showing is a bit bizarre, but it is good to know it exists. It sounds like the key thing is to make sure the SPN is registered for the NetBIOS name as well so it can do Kerb.

Re: Integrated Windows Authentication Timeout?

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>

--

"Henning Krause [MVP – Exchange]"

<newsgroups\_remove@xxxxxxxxxxxxxxxxxxxx>

wrote in message

<news:eLklU2sdHHA.4696@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Hello,

the Internet Explorer reverts from the  
domain name to the netbios name  
for  
some reason after 30 minutes. It's explained  
here:

<http://support.microsoft.com/kb/871179>

This might help.

Best regards,  
Henning Krause

"Joe Kaplan"

<joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote in

message

<news:ew67WVkdHHA.3632@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

That's pretty weird. Are you  
auditing logon success  
events on the web  
server? Do you see anything  
different for the NTLM  
requests? Is it  
possible that a different host  
name is being used (such as  
the IP  
address  
or something else) for one  
of the subsequent requests  
that would break  
Kerberos auth?

You might consider  
enabling protocol transition

Re: Integrated Windows Authentication Timeout?

authentication since  
you  
are using constrained  
delegation anyway. Then  
this wouldn't be a  
problem. However, it would  
still be good and useful to  
fix it.

If you have "Negotiate"  
authentication set in the  
metabase (the  
default),  
then this can still negotiate  
down to NTLM if for some  
reason the  
protocol thinks that  
Kerberos is unavailable.  
This is the aspect of  
Negotiate auth that makes it  
so functional for older  
clients that need  
NTLM and so frustrating for  
app developers that really  
need Kerberos  
auth. :)

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>

--

"Bradley Landis"  
<BradleyLandis@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>  
wrote in  
message  
<news:D442C7C0-35FE-40A6-8897-C10A7004C306@xxxxxxxxxxxxxxxxxxxx>

Okay, so I  
have  
narrowed  
the problem  
down to  
Kerberos

## Re: Integrated Windows Authentication Timeout?

Authentication.

When a user first visits the site all authentication is done via Kerberos.

After the period of inactivity, the next hit to the web site authenticates using NTLM for some reason.

Since we have Constrained Delegation set up as "Kerberos Only" it does not forward the NTLM credentials to the database server. This results in the "NT AUTHORITY\Anonymous logon" error.

So the question is why does it fall back to NTLM after a period of inactivity of about 30 minutes? I have used kerbtray.exe to look at

Re: Integrated Windows Authentication Timeout?

the  
tickets and  
they all say  
10 hours  
until  
expiration  
with 7 days  
of  
renewal.

Should I  
edit the  
Metabase  
on the web  
server to not  
allow  
NTLM?  
Would  
that  
force the  
authentication  
to Kerberos  
or would  
the  
authentication  
just  
fail?

Thanks,

Bradley

"anonymous"  
wrote:

I  
found  
this,  
do  
you  
think  
it  
could  
be  
related:

<http://technet2.microsoft.com/WindowsServer/en/library/b361>

S4UTicketLifetime

Re: Integrated Windows Authentication Timeout?

Registry  
path  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\C  
Version  
Windows  
Server  
2003  
This  
entry  
controls  
the  
lifetime,  
in  
minutes,  
of  
tickets  
obtained  
by  
S4U  
proxy  
requests.  
This  
entry  
does  
not  
exist  
in  
the  
registry  
by  
default.  
The  
default  
value  
is  
15  
minutes.

"anonymous"  
wrote:

Okay,  
I  
got  
rid  
of  
the  
viewstate

Re: Integrated Windows Authentication Timeout?

error.  
But  
I  
still  
get  
the  
authentication  
error  
after  
20  
minutes  
of  
inactivity.  
I  
have  
tried  
disabling  
the  
"shutdown  
idle  
worker  
processes",  
and  
"recycle  
worker  
processes"  
options  
on  
the  
application  
pool  
with  
no  
change  
in  
this  
behavior.

Does  
anyone  
have  
any  
ideas  
of  
what  
could  
be  
going  
wrong?  
Or  
suggestions

Re: Integrated Windows Authentication Timeout?

of  
specific  
things  
for  
me  
to  
audit  
or  
log  
that  
might  
point  
me  
in  
the  
right  
direction?

"Joe  
Kaplan"  
wrote:

No  
I  
don't.  
That's  
an  
interesting  
observation  
and  
I  
don't  
know  
if  
that  
is  
coincidence  
or  
not.  
The  
first  
thing  
to  
do  
would  
be  
to  
figure  
out  
how

Re: Integrated Windows Authentication Timeout?

the  
viewstate  
got  
corrupted,  
but  
I'm  
not  
really  
much  
of  
a  
viewstate  
expert,  
so  
I'm  
not  
really  
sure  
what  
the  
best  
bet  
is  
for  
troubleshooting  
that  
problem.  
Someone  
else  
will  
certainly  
know  
though.  
:)

Joe  
K.

--  
Joe  
Kaplan-MS  
MVP  
Directory  
Services  
Programming  
Co-author  
of  
"The  
.NET  
Developer's  
Guide



Re: Integrated Windows Authentication Timeout?

seen  
this,  
so  
I'm  
not  
sure  
what  
the  
likely  
culprit  
is.  
However,  
you  
might  
want  
to  
see  
if  
your  
app  
pool  
is  
recycling  
and  
if  
there  
is  
a  
correlation  
there.  
You  
should  
see  
events  
in  
the  
System  
event  
log  
indicating  
a  
recycle  
event.

Also,  
I'd  
suggest  
bumping  
up  
the  
auditing

Re: Integrated Windows Authentication Timeout?

on  
both  
the  
web  
server  
and  
SQL  
server  
so  
that  
you  
are  
auditing  
both  
logon  
success  
and  
failure  
messages.  
That  
way,  
you  
should  
get  
more  
diagnostic  
info  
in  
the  
security  
event  
log  
as  
to  
what  
is  
transpiring.

Joe  
K.

—  
Joe  
Kaplan—MS  
MVP  
Directory  
Services  
Programming  
Co—author  
of  
"The

Re: Integrated Windows Authentication Timeout?

.NET  
Developer's  
Guide  
to  
Directory  
Services  
Programming"  
<http://www.directoryprogram>  
--  
"anonymous"  
<anonymous@xxxxxxxxxxxxx  
wrote  
in  
message  
<news:34C2A7A8-B2CA-48>

Joe,

Thanks  
for  
the  
reply.  
It  
does  
happen  
on  
the  
attempt  
to  
connect  
to  
the  
SQL  
Server.  
I  
have  
not  
been  
able  
to  
reproduce  
it  
with  
the  
same  
setup  
on  
IIS  
5.0  
if  
that

Re: Integrated Windows Authentication Timeout?

helps.  
Can  
something  
with  
the  
Application  
Pool  
be  
timing  
out?

"Joe  
Kaplan"  
wrote:

Is  
that  
exception  
thrown  
by  
the  
connection  
attempt  
to  
SQL  
(thus  
an  
error  
in  
the  
delegation)  
or  
does  
that  
happen  
at  
the  
browser  
level?  
Can  
you  
show  
a  
stack  
trace?

IWA  
doesn't  
time  
out,

Re: Integrated Windows Authentication Timeout?

although  
Kerberos  
tickets  
can  
expire.  
20  
minutes  
sounds  
way  
too  
short  
to  
have  
anything  
to  
do  
with  
that  
though.

Joe  
K.

--

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

--

"Bradley  
Landis"  
<BradleyLan  
wrote  
in  
message  
<news:76CA1>

Re: Integrated Windows Authentication Timeout?

Envi  
IIS  
6.0  
ASP  
2.0  
Integ  
Win  
Auth  
Auth  
Iden  
impe  
Con  
Dele  
set  
to  
impe  
user  
whil  
conr  
to