

Re: Integrated Windows Authentication Timeout?

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2007-04/msg00008.html>

- *From:* "Joe Kaplan" <joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 3 Apr 2007 18:10:59 -0500
-

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 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@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:D442C7C0-35FE-40A6-8897-C10A7004C306@xxxxxxxxxxxxxxxxxxxxx

Okay, so I have narrowed the problem down to Kerberos 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 the tickets and they all say 10 hours until expiration with 7 days of renewal.

Re: Integrated Windows Authentication Timeout?

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/b36b8071-3cc5-46fa-be13-280aa43f2fd21>

S4UTicketLifetime

Registry path

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters

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 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 of

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

"Joe Kaplan" wrote:

Re: Integrated Windows Authentication Timeout?

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 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
to Directory Services
Programming"
<http://www.directoryprogramming.net>

--
"anonymous"
<anonymous@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
wrote in message
<news:2B0B127F-D89B-4702-9450-A7D08F5A5908@xxxxxxxxxxxxxxxxxxxx>

Seems like this event
correlates to the error:

"Viewstate verification
failed. Reason: The
viewstate supplied
failed
integrity check."

Any idea what is going on?

"Joe Kaplan" wrote:

Like I said
before, I've
never seen
this, so I'm
not sure
what the
likely
culprit is.

Re: Integrated Windows Authentication Timeout?

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
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

Re: Integrated Windows Authentication Timeout?

Services
Programming
Co-author
of "The
.NET
Developer's
Guide to
Directory
Services
Programming"
<http://www.directoryprogramming.net>

--
"anonymous"
<anonymous@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
wrote in
message
<news:34C2A7A8-B2CA-4880-A024-08A1326CBE61@xxxxxxxxxx>

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

Re: Integrated Windows Authentication Timeout?

if
that
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

Re: Integrated Windows Authentication Timeout?

time
out,
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
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:76CA1BCC-67A8-462A-A41D-F3D082DB3>

Re: Integrated Windows Authentication Timeout?

Environment:

IIS

6.0

ASP.NET

2.0

Integrated

Windows

Authentication

Identity

impersonate=true

Constrained

Delegation

set

to

impersonate

user

while

connecting

to

SQL

Server

Problem

scenario:

Everything

above

works

perfectly

well

except

when

the

user

leaves

a

page

sit

idle

for

20

minutes

or

so.

At

that

point

if

they

come

back

and

Re: Integrated Windows Authentication Timeout?

click
a
link
on
the
page
the
following
error
is
thrown:

Login
failed
for
user
'NT
AUTHORITY\ANONYMOUS
LOGON'

I
do
not
use
any
session
data
so
the
session
timeout
should
not
be
the
problem.
I
tried
extending
the
session
timeout
anyway
as
an
experiment
and
it
did
not
have

Re: Integrated Windows Authentication Timeout?

any
effect.
I
know
there
are
other
timeouts
associated
with
Forms
Authentication,
but
are
there
other
timeouts
associated
with
Integrated
Windows
Authentication?
If
so,
how
and
where
do
I
configure
them.

Thank
you,

Bradley

Re: Integrated Windows Authentication Timeout?