

Re: Error message: During a logon attempt, the user's security context

Re: Error message: During a logon attempt, the user's security context

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2009-03/msg01007

- *From:* "Richard Mueller [MVP]" <rlmueller-nospam@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 18 Mar 2009 21:25:08 -0500
-

"Carpenter" <Carpenter@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:22542F2D-79F0-427B-AF22-727E52D6EF08@xxxxxxxxxxxxxxxxxxxxx>

The problem is that some of our users experienced a problem during log on getting this message: Error message: During a logon attempt, the user's security context accumulated too many security IDs.

Have read some articles about the problem we've got to understanding that it is due to more than 1024 nested groups included in one account. We checked our problem users with ndsutil.exe – they have about 1150 nested groups (we really need it).

We see two problems here:

- 1.) LDAP MaxPageSize policy on DC controllers is by default set to 1000 which means that any LDAP Query can't get back more than 1000 AD objects. It's easy to avoid the limit by changing this policy so we have temporarily changed it to 10000 to be sure that there is no problem with this issue.
- 2.) MaxTokenSize for Kerberos is set by default to 12000 bytes (<http://support.microsoft.com/?kbid=327825>). We tried to set it to 65535 (both on two our DC servers and user's computer) and it seems to be set but users still can't log on. We tested our users with tokensz.exe utility it shows that 65535 should be quite enough for them to log on (for one of them it even shows: MaxTokenSize (incomplete context) : 11393).

What can we do wrong with setting MaxTokenSize or maybe you now other possible reasons for this error?

Thank you for your help in advance!

I don't know about increasing the token size, but the way to retrieve more

Re: Error message: During a logon attempt, the user's security context

Re: Error message: During a logon attempt, the user's security context

than 1000 records from AD is to turn on paging. You can do this by assigning a page size, like 100. The value is not that important (although the max is 1000). It just specifies the size of the data that is retrieved in each chunk.

More likely, your problem is that you cannot retrieve more than 1000 values of a multi-valued attribute, like the member attribute of a group or the memberOf attribute of a user. The limit is 1500 if the domain is at Windows 2003 functional level. The solution here is to use range limits.

If you query AD for all members of a large group, you may get more than 1000 records (rows), so paging is the solution. If you query AD for all groups a users is a member of, you should get one record with an array of values. You can reach the limit for multi-valued attributes, and range limits is the solution I use.

Richard Mueller
MVP Directory Services
Hilltop Lab – <http://www.rlmueller.net>

.