

Re: GPO/AD NULL SID problems

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-05/msg00540

- *From:* "Joe Richards [MVP]" <humorexpress@xxxxxxxxxxx>
 - *Date:* Fri, 05 May 2006 19:14:59 -0400
-

Please download sectok from <http://www.joeware.net/win/free/tools/sectok.htm>

run it when you see this null sid and post back the results. That will dump your entire security token which I am curious to see. If you aren't comfortable with that, you can email them to me, my email address is listed on my website and in the sectok tool.

Joe Richards Microsoft MVP Windows Server Directory Services
Author of O'Reilly Active Directory Third Edition
www.joeware.net

---O'Reilly Active Directory Third Edition now available---

<http://www.joeware.net/win/ad3e.htm>

Matt Vogt wrote:

We are having a problem with Active Directory where computers are pseudo randomly being assigned to the 'NULL SID' security group instead of 'AUTHENTICATED USERS'.

On the majority of the workstations on our network the problem never occurs but very fast computers (high end single and dual core systems – examples: Dell Optiplex desktops (GX620) dual core 2.8GHz+, single core 3.2GHz+ with 1GB+ RAM, Dell Latitudes Pentium M 1.87GHz+ and Core Duo 1.67GHz+ with 1GB+ RAM) that have several group policies being applied will very consistently end up with a 'NULL SID' security group. This of course prevents all GPO's from applying. Occasionally when you stop applying group policy to the afflicted computer it will sometimes go back to the 'AUTHENTICATED USERS' group on reboot, but most of the time you have to remove the computer from the domain and add it again to get it out of the 'NULL SID' group.

The problem does not appear to depend on the content of the GPOs being applied or on the number of GPOs. A very fast machine with two GPO's being applied (a WSUS setup policy and a XP SP2 firewall policy) may immediately end up in the 'NULL SID' group or may go through 1 or 2 reboots before moving from 'AUTHENTICATED USERS' to 'NULL SID', never to return, whereas a slightly slower machine might go several 7–10 reboots before ending up in the 'NULL SID' group and then may return to the 'AUTHENTICATED UERS'

Re: GPO/AD NULL SID problems

group on subsequent reboots. On slower computers (single core sub 2.5GHz P4s, P3s, VMWare Virtual Machines, etc) the problem never seems to occur even when four or five GPOs are being applied.

All of the workstations having this problem are running XP SP2, patch levels vary somewhat but they are mostly up to date. Our Active Directory network consists of three Domain Controllers. Two of the domain controllers are 2003 Service pack 1 while the third is 2003 without the service pack. The non-SP1 DC holds all of the FSMO roles, although all three DC's are GC servers. The domain is running in Windows 2000 native mode. All of the domain controllers pass all of the default 'dcdiag' tests.

Below is the output of 'gpresult' on a machine that has gone into the 'NULL SID' security group.

We are quite baffled; any help would be greatly appreciated.

Matt Vogt and Jeff Harwell
MIS, Fuller Seminary

Microsoft (R) Windows (R) XP Operating System Group Policy Result tool v2.0 Copyright (C) Microsoft Corp. 1981-2001
Created On 5/4/2006 at 4:09:56 PM
RSOP results for xxxxxx\hdesk on FTS-B8DFW91 : Logging Mode

OS Type: Microsoft Windows XP Professional
OS Configuration: Member Workstation
OS Version: 5.1.2600
Domain Name: xxxxxx
Domain Type: Windows 2000
Site Name: xxxxxxxx
Roaming Profile: Local Profile: C:\Documents and Settings\hdesk
Connected over a slow link?: No

COMPUTER SETTINGS

CN=FTS-B8DFW91,OU=SOP,OU=Pasadena_Computers,DC=xxxxxx,DC=fuller,DC=edu
Last time Group Policy was applied: 5/4/2006 at 4:08:25 PM
Group Policy was applied from: DELILAH.xxxxxx.fuller.edu
Group Policy slow link threshold: 500 kbps
Applied Group Policy Objects

N/A

The following GPOs were not applied because they were filtered out

Default Domain Policy
Filtering: Denied (Security)
Pasadnea_ServicePack2_Policy
Filtering: Not Applied (Unknown Reason)
Pasadena_WSUS
Filtering: Denied (Security)
Pasadnea_ServicePack2_Test
Filtering: Not Applied (Unknown Reason)

Re: GPO/AD NULL SID problems

Local Group Policy

Filtering: Not Applied (Empty)

The computer is a part of the following security groups:

NULL SID

NT AUTHORITY\NETWORK