

Re: Global Security Group members disappear

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-09/msg00722

- *From:* Jeremy <Jeremy@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sun, 16 Sep 2007 06:40:00 -0700
-

Virus scan run... no viruses found.

Thanks for the help so far. Any more ideas? This is still happening. I have two DCs and when the members disappear from one DC they disappear from the other too so I don't see it as one AD being overwritten by an older/newer version.

"Harj" wrote:

On Sep 12, 3:12 am, Jeremy <Jer...@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote:

OK, I now have a series of log entries as follows, one each for each group removed:

Event Type: Success Audit
Event Source: Security
Event Category: Account Management
Event ID: 633
Date: 12/09/2007
Time: 04:16:58
User: NT AUTHORITY\SYSTEM
Computer: SENIOR
Description:
Security Enabled Global Group Member Removed:
Member Name: CN=2007,CN=Users,DC=sion_domain,DC=local
Member ID: SION_DOMAIN\2007
Target Account Name: Students
Target Domain: SION_DOMAIN
Target Account ID: SION_DOMAIN\Students
Caller User Name: SENIOR\$\br/>Caller Domain: SION_DOMAIN
Caller Logon ID: (0x0,0x9588C9A)
Privileges: -

and

Event Type: Success Audit

Re: Global Security Group members disappear

Event Source: Security
Event Category: Account Management
Event ID: 641
Date: 12/09/2007
Time: 04:16:58
User: NT AUTHORITY\SYSTEM
Computer: SENIOR
Description:
Security Enabled Global Group Changed:
Target Account Name: Students
Target Domain: SION_DOMAIN
Target Account ID: SION_DOMAIN\Students
Caller User Name: SENIOR\$\br/>Caller Domain: SION_DOMAIN
Caller Logon ID: (0x0,0x9588C9A)
Privileges: –
Changed Attributes:
Sam Account Name: –
Sid History: –

How do I identify the Caller Logon ID?

"Steve B" wrote:

Ensure Audit Account management is set to Success and Failure in the Domain Controllers policy. Also ensure that you run gpupdate to force the policy to apply. I would then (at a suitable time) take out one of the groups and put it back in. You can then check the security log to ensure that everything is being logged.

If it happens again at least you know it should have been captured.

"Jeremy" wrote:

The only vaguely relevant entry in the security log is as follows:

Re: Global Security Group members disappear

Event Type: Success Audit
Event Source: Security
Event Category: System Event
Event ID: 516
Date: 10/09/2007
Time: 16:48:29
User: NT AUTHORITY\SYSTEM
Computer: SENIOR
Description:
Internal resources allocated for the queuing
of audit messages have been
exhausted, leading to the loss of some audits.
Number of audit messages discarded: 4

Mind you, I only had Directory Services
logging failures. I've reset it to
log successes as well now.

"Jorge Silva" wrote:

I agree with steve, you
should look at the logs to
check what is going on...

--

I hope that the information
above helps you.
Have a Nice day.

Jorge Silva
MCSE, MVP Directory
Services
"Steve B"
<Ste...@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
wrote in message
news:A2D67D5A-0EEC-4887-BD40-F0817041259D@xxxxxxxxxxxxxxxxxxxx

OK...have
you
checked the
security

Re: Global Security Group members disappear

logs on the
DC's. This
should now
tell
you who/the
process and
time that
the students
group was
removed.

"Jeremy"
wrote:

Moved
forest/domain
level
to
2003.

Members
of
"Students"
disappeared
again
overnight.
I
have
turned
on
auditing
of
management
as
Jorge
suggested
although
I
think
the
likelihood
of
anyone
other
than

Re: Global Security Group members disappear

me
being
able
to
edit
AD
is
low.

"Steve
B"
wrote:

Whilst
it
will
not
explain
why
your
groups
disappeared
–
I
would
suggest
you
investigate
switching
your
domain/forest
level
to
Windows
2003.
This
allows
you
to
take
advantage
of
all
the
AD
features.

Re: Global Security Group members disappear

Did
you
manage
to
check
what
auditing
was
turned
on?

"Jeremy"
wrote:

Hmmm...
okay,
further
investigation
reveals:

Domain
Functional
Level:
Windows
2000
native

Forest
Functional
Level:
Windows
2000

"Steve
B"
wrote:

Re: Global Security Group members disappear

What's
the
forest
functional
level?
Do
you
have
auditing
turned
on?
If
so,
what
are
you
auditing?

"Jeremy"
wrote:

I
should
add
that
this
is
W2k3
AD

"Jeremy"
wrote:

I
have
set
up
a
Global
Security
Group
called
"Students"

Re: Global Security Group members disappear

which
on
a
good
day
contains
Global
Security
Groups
"2000",
"2001"...
"2007".
I
recently
set
up
a
second
domain
controller.
Now,
every
morning
I
look
in
Students
and
all
the
Global
Security
Groups
supposed
to
be
members
("2000",
"2001"...
"2007")
have
disappeared
from
the
list
of
members.
There
are
no
errors

Re: Global Security Group members disappear

in
the
Event
Logs
and
RepAdmin
shows
replication
occurring
correctly.
To
apply
a
temporary
fix
I
visit
both
DCs
and
add
the
missing
groups.
I
also
use
ADUC
on
my
XP
Pro
workstation
and
re-apply
the
groups
using
that
too
if
they
are
not
showing.

Why
do
these

Re: Global Security Group members disappear

groups
disappear
from
the
membership
list
of
the
"Students"
group
and
how
can
I
stop
it
happening?–
Hide
quoted
text
–

– Show quoted text –

Hi,

Caller User Name: SENIOR\$

I would run a virus scan on this machine SENIOR to determine if it is not a virus causing this.

Good luck

Harj Singh
Power Your Active Directory Investment
www.specopssoft.com