

RE: SIDS show instead of user names

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2006-06/msg00421.html

- From: v-xuwen@xxxxxxxxxxxxxxxxxxxxxx (Vincent Xu [MSFT])
 - Date: Tue, 27 Jun 2006 09:15:11 GMT
-

Hi,

Honestly, it is a weird issue. The reason I suggest you run sidname is that I'd like to make sure the sid can be resolved at the same time you see SID in ACL. Please let me know the results in detail (If there are any error messages.)

Thanks.

Best regards,

Vincent Xu
Microsoft Online Partner Support

=====
Get Secure! – www.microsoft.com/security
=====

When responding to posts, please "Reply to Group" via your newsreader so that others may learn and benefit from this issue.

=====
This posting is provided "AS IS" with no warranties, and confers no rights.
=====

Thread-Topic: SIDS show instead of user names
thread-index: AcaZNhcLx49xnCVqT66a1eAuT/T2Bw==
X-WBNR-Posting-Host: 136.167.76.86
From: =?Utf-8?B?Q2hhcmxpZQ==?= <baboon@xxxxxxxxxxxxxxxx>
References:
<D97EA440-62A7-48DF-85BF-76B2082048E5@xxxxxxxxxxxxxxxx>

<4cAln0blGHA.4908@xxxxxxxxxxxxxxxx>
<4F433889-5407-4A02-8E93-BEBE56FCB18A@xxxxxxxxxxxxxxxx>
<AcQOcYplGHA.5184@xxxxxxxxxxxxxxxx>

RE: SIDS show instead of user names

<EE786F60-D9BF-4CF6-9FDA-E524AA8600F7@xxxxxxxxxxxxxx>
<13Wv5K0mGHA.5164@xxxxxxxxxxxxxxxxxxxxxx>

Subject: RE: SIDS show instead of user names
Date: Mon, 26 Jun 2006 08:35:02 -0700
Lines: 321
Message-ID:
<2E09F3F8-6FCA-4462-ABB7-F1C7C8E72AFE@xxxxxxxxxxxxxx>
MIME-Version: 1.0
Content-Type: text/plain;
charset="Utf-8"
Content-Transfer-Encoding: 7bit
X-Newsreader: Microsoft CDO for Windows 2000
Content-Class: urn:content-classes:message
Importance: normal
Priority: normal
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.1830
Newsgroups: microsoft.public.win2000.active_directory
Path: TK2MSFTNGXA01.phx.gbl
Xref: TK2MSFTNGXA01.phx.gbl

microsoft.public.win2000.active_directory:114617

NNTP-Posting-Host: TK2MSFTNGXA01.phx.gbl 10.40.2.250
X-Tomcat-NG: microsoft.public.win2000.active_directory

Vincent -

Thanks for the help. 136.167.2.233 is also a DC (we have 4).

136.167.2.235

has all the domain level operations masters, but it is not a GC. A

different

DC has the forest wide operations masters and the other 2 are GCs. I

again

want to stress that there is no WAN involved and only one AD domain, so

there

is plenty of connectivity with the GCs, etc.

I did not use the Sid2name tool because I got the impression that you

wanted

me to use it to confirm whether or not the accounts were deleted. Since

RE: SIDS show instead of user names

RE: SIDS show instead of user names

I

know the accounts were not deleted (remember, I was able to see them remotely

using showacl), I didn't use Sid2name. See my latest response to Paul Bergson below. He suggested I run LDP from the server. I did that and

was

able to see every user name in a particular OU. If you still think that

I

should run Sid2name, let me know.

Regards.

"Vincent Xu [MSFT]" wrote:

Hi,

Thanks for sending me the trace data.

I also found that in SID.cap, it contacts 136.167.2.235 and in Name.cap, it

contacts 136.167.2.247. However, I found in Name.cap, an IP:

136.167.2.233.

What IP is this?

Since the problem seems to be related to 136.167.2.235, I suggest you shutdown this DC temporarily to see if the problem happens again.

Also, did you see the tool sid2name I attached? I'd like to suggest you

run

it when the problem occurs to verify at the same time, if the sid can

RE: SIDS show instead of user names

be

resolved. The syntax like:

Sid2name
S-1-5-21-583907252-688789844-725345543-1344

Let me know the detailed output.

Thanks.

Best regards,

Vincent Xu
Microsoft Online Partner Support

=====
Get Secure! – www.microsoft.com/security
=====

When responding to posts, please "Reply to Group" via your newsreader

so

that others
may learn and benefit from this issue.

=====
This posting is provided "AS IS" with no warranties, and confers no

rights.

=====

Thread-Topic: SIDS show
instead of user names
thread-index:
AcaW0afIQ6U8H4otSAWIo/blJC3BXA==
X-WBNR-Posting-Host:
136.167.76.86
From:
=?Utf-8?B?Q2hhcmxpZQ==?=
<baboon@xxxxxxxxxxxxxxxx>
References:
<D97EA440-62A7-48DF-85BF-76B2082048E5@xxxxxxxxxxxxxxxx>

RE: SIDS show instead of user names

<4cAln0blGHA.4908@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
<4F433889-5407-4A02-8E93-BEBE56FCB18A@xxxxxxxxxxxxxxxx>
<AcQOcYplGHA.5184@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Subject: RE: SIDS show
instead of user names
Date: Fri, 23 Jun 2006
07:31:03 -0700
Lines: 261
Message-ID:
<EE786F60-D9BF-4CF6-9FDA-E524AA8600F7@xxxxxxxxxxxxxxxx>
MIME-Version: 1.0
Content-Type: text/plain;
charset="Utf-8"
Content-Transfer-Encoding:
7bit
X-Newsreader: Microsoft
CDO for Windows 2000
Content-Class:
urn:content-classes:message
Importance: normal
Priority: normal
X-MimeOLE: Produced By
Microsoft MimeOLE
V6.00.3790.1830
Newsgroups:
microsoft.public.win2000.active_directory
Path:
TK2MSFTNGXA01.phx.gbl
Xref:
TK2MSFTNGXA01.phx.gbl

microsoft.public.win2000.active_directory:114567

NNTP-Posting-Host:
TK2MSFTNGXA01.phx.gbl
10.40.2.250
X-Tomcat-NG:
microsoft.public.win2000.active_directory

Thanks for the help. I may
not be able to get to this
today, but I

certainly

will do the NetMon trace. I
was thinking of using
NetMon, but it

will be

RE: SIDS show instead of user names

RE: SIDS show instead of user names

very helpful for someone
else to look at the output.

As far as the accounts being
deleted in AD, keep in mind
that this

affects

every single account (other
than the one I'm logged on
with) in every

ACL

and

group, so I already know
that isn't the problem. Even
if I add a new

account

to a group, that user's name
disappears as soon as I click
OK.

"Vincent Xu [MSFT]"
wrote:

Hi,

Thanks for
your reply
and
clarifying.

Let's
perform
some
troubleshooting
steps:

2. Please
use the tool
sid2name.exe
tool
(attached)
to
determine

RE: SIDS show instead of user names

RE: SIDS show instead of user names

the name of
those
unknown
accounts.
Please run
the below
one-by-one
and
check the
output:

Sid2name
S-1-5-21-583907252-688789844-725345543-1344
Sid2name
S-1-5-21-583907252-688789844-725345543-24842
Sid2name
S-1-5-21-583907252-688789844-725345543-24843
Sid2name
S-1-5-21-583907252-688789844-725345543-37443

Could you
find the
account
names from
sid2name.exe?
If it cannot
be

found,

the user
accounts are
probably
deleted and
cause this
problem. If
the

username

can

be shown
from
sid2name,
please
search the
user
accounts in
AD users

RE: SIDS show instead of user names

RE: SIDS show instead of user names

and

computers to

ensure
it is there.

3. If you
can find the
user
accounts
name and it
is existed in
AD

users

and

computers,
please help
to capture
netmon
trace on the
problematic

file

server.

A. Install
the built-in
network
monitor
tools on the
problematic

file

server.

Windows
2000:
(Add/Remove
Program
-->
Add/Remove
Windows
Components

-->

RE: SIDS show instead of user names

RE: SIDS show instead of user names

Management
and
Monitoring
Tools -->
Network
Monitor
Tools -->
no need to

reboot

machine)

B.
Synchronize
the time
between file
server and
DC
(otherwise
it is
difficult to
check in
netmon)

C. Run the
netmon tool
on the file
server.

D. Go to
Capture
-->
Networks to
choose the
correct
network
card by

MAC

address

E. Go to
Capture
--> Buffer
Settings and
set 100MB
as buffer
size

RE: SIDS show instead of user names

(this

setting is
to avoid the
trace
overwrite
itself)

F. Go to
Capture
--> Start to
start capture
the network
traffic on

both

machines.

G.
Reproduce
the problem
by checking
the ACL.

H. Stop the
capture in
network
monitor
after the
unknown
account

shown.

(Please
note the
system time
<hh:mm:ss>,
we need it
to check the
netmon

trace)

I. Save the
network
trace and
send to me,
please also

RE: SIDS show instead of user names

tell me the

IP of

the

machine.

my email is:

v-xuwen@xxxxxxxxxxxxxx

Thanks.

Best
regards,

Vincent Xu
Microsoft
Online
Partner
Support

=====
Get Secure!

-

www.microsoft.com/security

=====
When
responding
to posts,
please
"Reply to
Group" via
your

newsreader

so

that others
may learn
and benefit
from this
issue.

=====
This posting
is provided
"AS IS"
with no
warranties, and

RE: SIDS show instead of user names

RE: SIDS show instead of user names

confers no

rights.

=====

Thread-Topic:
SIDS
show
instead
of
user
names
thread-index:
AcaWFVZsDXP9mpt8TPuuWrsXdSUfxQ==
X-WBNR-Posting-Host:
136.167.76.86
From:
=?Utf-8?B?Q2hhcmxpZQ==?=
<baboon@xxxxxxxxxxxxxxxx>
References:
<D97EA440-62A7-48DF-85BF-76B2082048E5@

<4cAln0blGHA.4908@xxxxxxxxxxxxxxxxxxxxxxxx>

Subject:
RE:
SIDS
show
instead
of
user
names
Date:
Thu,
22
Jun
2006
09:03:01
-0700
Lines:
117
Message-ID:
<4F433889-5407-4A02-8E93-BEBE56FCB18A@
MIME-Version:
1.0
Content-Type:

RE: SIDS show instead of user names

text/plain;
charset="Utf-8"
Content-Transfer-Encoding:
7bit
X-Newsreader:
Microsoft
CDO
for
Windows
2000
Content-Class:
urn:content-classes:message
Importance:
normal
Priority:
normal
X-MimeOLE:
Produced
By
Microsoft
MimeOLE
V6.00.3790.1830
Newsgroups:
microsoft.public.win2000.active_directory
Path:
TK2MSFTNGXA01.phx.gbl
Xref:
TK2MSFTNGXA01.phx.gbl

microsoft.public.win2000.active_directory:114542

NNTP-Posting-Host:
TK2MSFTNGXA01.phx.gbl
10.40.2.250
X-Tomcat-NG:
microsoft.public.win2000.active_directory

Hi
Vincent
-

Thanks
for
the
response.
The
NBT
Helper
service
is
started

RE: SIDS show instead of user names

13

RE: SIDS show instead of user names

and

yes,

this

problem
is
persistent.
It
is
not
something
that
is
resolved
by

waiting.

If

I
open
a
window
for
a
group
membership
or
ACL,
I
can
leave
it

open

for 10

minutes
and
it
still
only
shows
SIDs.

I
don't

RE: SIDS show instead of user names

RE: SIDS show instead of user names

think
it's
a
network
issue
and
it
is
not
intermittent.

The

reason I

don't
believe
it
is
network
related
is
because
of
the
following

that

I

said

in
my
post:
"I
tried
using
the
showacls
command
line
utility
and
as
long
as

it is

RE: SIDS show instead of user names

RE: SIDS show instead of user names

used

remotely,
I
DO
then
see
the
friendly
names
in
ACLs.
Also,
when

logged

onto
the
server
I
can
see
the
name
of
my
own
domain
account,
but

it

is

followed
by
the
SID."

One
more
thing
that
may
or
may
not
apply:
File

RE: SIDS show instead of user names

RE: SIDS show instead of user names

MacIntosh

is

start

and

don't

Server
for

supposed
to
be
running
on
that
server,
but
the
service
will
not

both
of
these
problems
may
have
started
around
the
same
time.
We

really
need
FSM
because
the
Mac
users
can
connect
using
SMB

RE: SIDS show instead of user names

RE: SIDS show instead of user names

instead,

but

I

thought
I
should
mention
it
for
troubleshooting
purposes.

Thanks.

"Vincent
Xu
[MSFT]"
wrote:

Hi

,

This
issue
can
occur
because
the
SIDs
in
ACL
are
not
resolved

into

friendly

user
name
immediately.
Therefore,
there
will
no

RE: SIDS show instead of user names

RE: SIDS show instead of user names

access
denied

issue. If

the

problem
occur
continually
or
always,
please
check
if
the
TCP/IP

NetBIOS

Helper
service
set
to
disabled
on
the
member
server.
If
so,

please

enable

it.

If
the
problem
happens
intermittently,
not
very
frequently,
I

think

it

RE: SIDS show instead of user names

RE: SIDS show instead of user names

is

the
intermittent
network
issue.
The
troubleshooting
process
may

be

time-consuming
and
troublesome.
However,
please
rest
assured

that I

will

try
my
best
to
provide
assistance.

Thanks.

Best
regards,

Vincent
Xu
Microsoft
Online
Partner
Support

=====
Get
Secure!

—
www.microsoft.com/security

=====
When

RE: SIDS show instead of user names

responding
to
posts,
please
"Reply
to
Group"
via
your

newsreader

so

that
others
may
learn
and
benefit
from
this
issue.

=====
This
posting
is
provided
"AS
IS"
with
no
warranties,and
confers

no

rights.

=====

Thread-Topic:
SIDS
show
instead
of
user

RE: SIDS show instead of user names

RE: SIDS show instead of user names

names
thread-index:
AcaVdane96zSt6CoQHmY7
X-WBNR-Posting-Host:
136.167.76.86
From:
=?Utf-8?B?Q2hhcmxpZQ==
<baboon@xxxxxxxxxxxxxxxx>
Subject:
SIDS
show
instead
of
user
names
Date:
Wed,
21
Jun
2006
14:00:02
-0700
Lines:
23
Message-ID:

<D97EA440-62A7-48DF-85BF-76B2082048E5@xxxxxxxxxxxxxxxx>

MIME-Version:
1.0
Content-Type:
text/plain;
charset="Utf-8"
Content-Transfer-Encoding:
7bit
X-Newsreader:
Microsoft
CDO
for
Windows
2000
Content-Class:
urn:content-classes:message

RE: SIDS show instead of user names