

Re: Computers lose domain trust

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-11/msg00203

- *From:* Meinolf Weber <meiweb(nospam)@gmx.de>
 - *Date:* Fri, 2 Nov 2007 20:42:07 +0000 (UTC)
-

Hello isworks,

Search for Event id 647 Computer account deleted

Here is a nice overview:

<http://www.ultimatewindowssecurity.com/Encyclopedia.aspx?catId=11>

Best regards

Meinolf Weber

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

** Please do NOT email, only reply to Newsgroups

** HELP us help YOU!!! <http://www.dts-1.org/goodpost.htm>

Meinolf,

Got it!

So this is what I have now.

Policy Policy Setting

Audit account logon events Success

Audit account management Success, Failure

Audit directory service access Success, Failure

Audit logon events Success

Audit object access No auditing

Audit policy change Success, Failure

Audit privilege use No auditing

Audit process tracking No auditing

Audit system events Not Defined

Some of this was already configured so perhaps I can go back and find when the computer was deleted. Is there an event ID I should be looking for specifically?

Thanks!

"Meinolf Weber" wrote:

Re: Computers lose domain trust

Hello isworks,

No i mean the Default Domain controllers policy (you find it in the Domain controllers OU), but this config will generate a lot of entries in the event viewer of the dc's. I would take out the:

Audit account logon events success, failure
Audit loon events success, failure
Audit system events success, failure
Best regards

Meinolf Weber

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

** Please do NOT email, only reply to Newsgroups

** HELP us help YOU!!! <http://www.dts-1.org/goodpost.htm>

Meinolf,

If I have understood you correctly I have modified the following in

the

default domain policy:

Local policy>audit policy:

Audit account logon events success, failure

Audit account management success, failure

Audit directory service access success, failure

Audit loon events success, failure

Audit policy change success, failure

Audit system events success, failure

Does that cover it?

Thanks!

"Meinolf Weber" wrote:

Hello isworks,

Enable account management in the default domain controllers gpo, to see who has deleted the computer account, if it happens again.

Best regards

Meinolf Weber

Disclaimer: This posting is provided "AS IS" with no warranties,

Re: Computers lose domain trust

and
confers
no rights.
** Please do NOT email, only reply to
Newsgroups
** HELP us help YOU!!!
<http://www.dts-l.org/goodpost.htm>

It would appear that it was
deleted but there are only
two people
who have access to that
function and neither of us
were logged in
last night.

"Meinolf Weber" wrote:

Hello
isworks,

What do
you mean
with gone
out?
Deleted
from AD or
moved to
another
OU?

Best regards

Meinolf
Weber
Disclaimer:
This posting
is provided
"AS IS"
with no
warranties,
and
confers
no rights.
** Please
do NOT
email, only
reply to
Newsgroups
** HELP us

Re: Computers lose domain trust

help

YOU!!!

<http://www.dts-1.org/goodpost.htm>

I
have
had
an
issue
4
times
in
the
past
3
weeks
where
a
computer
"loses"
it's
domain
account.
In
two
instances
the
computer
was
gone
out
of
the
Computer
list
and
the
other
two
were
still
there.
This
is
Server
2003
SP2.
Has
anyone
else
had

Re: Computers lose domain trust

this
happen?
Thanks!