

Re: Windows 2000 users accounts get locked out

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-05/1059.html>

From: Merrick (*anonymous_at_discussions.microsoft.com*)

Date: 05/19/04

Date: Wed, 19 May 2004 01:08:40 -0700

Hi Steve,

You have been a great help! I really appreciated it. As to my problem:

- 1.) I have disabled my accounts lockout policy in my domain controller security policy but i still get accounts locked out, yes the administrator is always locked out.
- 2.) I have included 644 and 642 in my eventcomb and for every 644 i got one 642. MS provide very little information on 642 and am still trying to gather information on that. it seems like my secure channel is leaking.
- 3.) I have also planted alockout.dll in one of my clients and one particular line is worrying me: C:\WINNT\system32\svchost,***StartServiceW Failed!*** (0), Service: Service: Background Intelligent Transfer Service (C:\WINNT\System32\svchost.exe -k BITSgroup), RC was: Incorrect function. (1), GLE was: Overlapped I/O operation is in progress. (997): Any comment?

Hope you can help! Many Thanks in advance!

>-----Original Message-----

>Hi again Merrick.

>

>If you have not done such, set your account lockout threshold for number of

>bad attempts to at least ten. You should be seeing failed logon attempts

>such as Event ID 529 on some computers in the domain.

These failed logons

>could be on any computer in the domain – not just domain controllers. Be

>sure you have auditing of "logon events" for failure which is different than

>account logon events enabled in Domain Security Policy and Domain Controller

>Security Policy. You may also need to configure it at the OU level if you

>are using *Organizational Units with their own Group Policies* that have
>*auditing disabled. You can check the Local Security Policy* of any domain
>*computer and look at the "effective" settings for auditing* to see if it is
>*enabled. Those failed logon events will give a lot of helpful info* on why
>*the logons are failing and from what computers the logon attempts are coming*
>*from.*
>
>*In addition I would run some diagnostics on the domain controller* and then a
>*couple domain computers. First run netdiag on the domain controller* looking
>*for any failed tests/errors/warnings particularly relating to dns, domain*
>*membership, and dclist. Then run dcdiag on the domain controller* looking for
>*failed tests again. After that do the same with netdiag on one of the domain*
>*members. On the domain controller and domain member run "*
netdiag
>/test:ipsec " which will show if an ipsec policy is assigned that can cause
>*problems in a domain. You can post results here in a reply* if any problems
>*are found. Those tools are found on the install cdrom in the support/tools*
>*folder where you will need to run the setup there. --*
Steve
>
>
>*"Merrick" <anonymous@discussions.microsoft.com> wrote in message*
>news:e7fb01c43cb0\$4343bd40\$a001280a@phx.gbl...
>> *Hi guys! thanks for the help. I have scan my firewall as*
>> *suggested by Steven and all my ports are secured. I have*
>> *also increase my password threashold to 10 minutes. I*
have
>> *patched all my software for my servers and users. All my*
>> *users are using Windows 2000 only. I have also rename my*
>> *administrator for my server. I have downloaded*
EventCombMT
>> *from MS and managed to search all my events log. I have*
a
>> *long list of event ID: 644. Yet when i go through the*
list
>> *I still don't understand why my users are getting locked*
>> *out! This happened suddenly and I have never changed any*

microsoft.public.win2000.security: Re: Windows 2000 users accounts get locked out

>> *thing to my servers. My accounts is still getting locked*
>> *out and yet I still dont know why! Please help. Many*
>> *thanks in advance!*
>> *Merrick*
>
>
>
>