

## Re: User accounts are being locked out

**Source:**

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.general/2004-10/2132.html>

---

**From:** Todd J Heron (*todd\_heron\_no\_spam\_at\_hotmail.com*)

**Date:** 10/22/04

Date: Fri, 22 Oct 2004 17:41:34 -0400

The computer name changing randomly looks like it is due to computers dropping in and out of the browse list. Could be laptop users. You might want to be concerned with who these laptop users are. Travelling Sales force? Telecommuters? Students? Think about that for a little it then review my "cookbook" recipe for determining the source of the lockout problem on multiple accounts.

Lockouts are common when there are replication problems between the PDC and BDCs. Open Server Manager > highlight the PDC > click on Computer > Synchronize the entire domain > check the system log of the Event Viewer on all DCs to determine whether synchronization was successful.

Password Policy and Account Lockout Policy are both domain-wide policies, so if only a small number of users are affected, it's unlikely that the policy itself is the problem. (For a single user, continuous lock-out situation, I always suggest that they find all workstations they have logged into recently and close Outlook, because it caches the password of the logged in account, and if it changes, then the old credentials will be denied and cause a domain controller to lock the account out based on bad password attempts). Look for a scheduled task or service running using the old password. It's also possible that some application or mapped drive is caching the old password. This can especially be a problem if users are logged into multiple machines. Here's an example scenario: User1 logs into machineA and machineB. User1 changes his password on machineA, but fails to logout of machineB. MachineB's antivirus software wakes up and attempts to download updated signature files located on a network share. MachineB's antivirus process cannot connect to the network share since User1's credentials on MachineB are now invalid, but continues to attempt to the network resource 3 times before giving up, which inadvertently locks out User1's account from MachineB. This scenario would be avoided simply by logging out of machineB and logging back into machineB once User1 updates his password from MachineA. Without knowing your current policy settings are, you may want to consider changing them, at least temporarily while troubleshooting. For example, increase the number of bad password logon attempts to 10 in 30 minutes, and unlock at 30 minutes. And check in all event logs on the DC's for any clues, and get the exact error message when this happens. If you decide to open an incident for this, this info will

microsoft.public.windows.server.general: Re: User accounts are being locked out

help the engineer assist you. Also, all Windows 2000 servers and workstations should be on Service Pack 3, if not already, because there were a number of fixes included in SP3 for lockout issues.

- 1) Get all NT 4.0 DC's out of environment as soon as possible if it is a mixed environment
- 2) Make sure all Win2k DC's have latest service pack (since many account lockout issues are resolved in SP2 , SP3)
- 3) Validate the account lockout policy settings on the Win2k domain
- 4) Is Web Sense installed anywhere on the network? Web Sense sends a logon prompt when accessing the web. An option is available to save password for this dialog and this is known to cause lock-out issues.
- 5) See: HOW TO: Prevent Network Share Shortcuts from Being Added to My Network Places <http://support.microsoft.com/?id=242578>
- 6) Check for persistent drive mappings using saved account\password. Increased Account Lockout Frequency in Windows 2000 Domain: <http://support.microsoft.com/default.aspx?scid=kb%3ben-us%3b264678>
- 7) Click here for a Account Lockout Status tool which will show the lockout status across a domain for a particular user:

L:\Utils\acctlockouttool.zip

Reference:

Verifying Domain Netlogon Synchronization

<http://support.microsoft.com/default.aspx?scid=kb:en-us:Q149664>

Account Lockouts and 5711 Events on the PDC

<http://support.microsoft.com/default.aspx?scid=kb:en-us:Q191828>

Using the Checked Netlogon.dll to Track Account Lockouts

<http://support.microsoft.com/default.aspx?scid=kb:en-us:Q189541>

--

Todd J Heron, MCSE

Windows 2003/2000/NT

"Ira Schmidt" <Ira.Schmidt@discussions.microsoft.com> wrote in message news:D3C11A5D-7B22-45BB-A913-E15D53793AD3@microsoft.com...

> User accounts are being locked out randomly in an NT domain. It appears  
> that  
> they are being locked out from computer names that do not exist on the  
> domain. The computer name changes randomly and has used names like  
> \\palnet  
> or \\acs and the names change every few days. Is there a way to find out  
> where these logon attempts are coming from? I have checked Wins manager  
> and  
> dhcp manager without finding the computer names. I suspect a trojan is  
> installed on one of the computers in the domain. I am migrating users to  
> Active Directory and those accounts are not effected.

Re: User accounts are being locked out