

Re: Registry corruption, can't login

Re: Registry corruption, can't login

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2005-09/msg08180.html>

- *From:* Rock <rock@xxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 29 Sep 2005 09:18:13 -0700
-

TonyG wrote:

(Original issue from July 23rd, 2005)

Two months later I'm having the same problem:

- Registry took a hit and user profiles, including name/password, are corrupted.
- Registry is set to AutoLogon, but when the registry is corrupted it can't login, so I have no way to get into the system, even in safe mode, to fix the problem.
- This time, during login, lsass.exe reports memory error -1073741819 at 0x7c914d1a. There is also a "handle is invalid" error from login itself. (No, this isn't the work of sasser...)

Solution is indicated below, but I'd like to know if there is any new wisdom on this from Microsoft or anywhere else:

- Is there any new utility or XP setting that will force an audit of the registry before shutdown? Anything that will halt the shutdown and allow repair before the files are committed to disk for the next boot?
- Using "Last known good configuration" never works. I can write some code to save the hive from the most recent boot. Where can I put it so that LKGC actually finds a good config? That is, where does LKGC get its info? (And why can Microsoft do the same honkin thing!??)
- For the next time this happens, as time permits, which is very little, I'll check out BartPE to see if I can recover the registry without removing the hard drive from my system. Learning how to build BartPE and related plugins seems like a time consuming process. Comments?
- Outside of turning off AutoLogon, is there some way around this dilemma of locking myself out? How does safe mode log you in if the profile is messed up? I'm wondering if there is a simple ditty to zap the ForceAutoLogon in registry from a floppy? (Maybe I should write it?)

Thanks!

On Sat, 23 Jul 2005 23:07:15 -0700, TonyG wrote:

Re: Registry corruption, can't login

Re: Registry corruption, can't login

On Sat, 23 Jul 2005 21:46:46 -0500, "Kelly" <kelly@xxxxxxxx> wrote:

Place your XP CD in and go to the Recovery Console.

Added info:

Recovering XP using the Recover Console (Line 333) Right hand side:

http://www.kellys-korner-xp.com/xp_tweaks.htm

Before responding I just wanted to say Kelly - even before your response here I kept coming back to your site during this event and I appreciate all the links and info you've made available.

Like I said in the OP, the problem that all documented solutions seem to skip by is that if the password for Administrator and other users has been corrupted then you the password isn't recognized as indicated on the page that you've linked to, so you can't get to a command prompt even when booting with the XP CD.

The solution to my problem was found here:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;307545>

I put the drive into another system and was able to recover yesterday's system32/config files with a current registry.

I'm virus scanning now but I don't think I was hit with malware, I've seen Win32 flakyness like this before. Without knowing exactly what the problem was and is, I still feel vulnerable and may do a complete reinstall at some point soon anyway. As an MSDN Universal subscriber and developer with a LOT of utilities installed, that's always a very painful process so this whole event is very unnerving.

Thanks and regards,
Tony

On Sat, 23 Jul 2005 16:12:02 -0700, TonyG wrote:

Re: Registry corruption, can't login

I have a scenario described here many times. System looked fine yesterday, no problems at all, running NAV and SP2 with firewall up, shutdown for the night, today I can't boot. The registry has been corrupted and I need to get back in via Safe Boot or System Recovery to fix it. The problem is that with this corruption the Login/Logon process doesn't validate passwords for Administrator or my user accounts. All of the docs that talk about fixing the registry from SR assume that you can get past the prompt for Administrator password after you specify the C:\Windows location. Catch 22 there.

I tried going back to Last Known Good setting - when booting before it would at least ask for a password and now it doesn't. I think someone said here recently that the accounts profile data isn't backedup in the registry like this, so I didn't expect success here.

(Microsoft, please learn from these reports and fix them for Longhorn/Vista.)

I export the registry to a backup folder once per week as files HCC.reg, HCR.reg, HCU.reg, HLM.reg, and HU.reg. I know this isn't the most effective way of fixing things, but to get back to a runnable state I'd have no problem importing the files to the registry - if only I can get to a command prompt to do it. Again, any attempt I make to Safe Boot or otherwise get to cmd fails because I'm prompted for a password.

I have other systems and would gladly hook up the hard drive with the bad registry, import the reg files, then reload the drive back to the right system, but how can I import to a hive other than the current system hive? I don't want to put the drive on a good system and import all the keys into that new system, I want to update the inactive hive.

I do not have a Automatic System Recovery disk because I've read too many times in the past that there is a good chance that it will fail or make things worse, so I've tried to create homegrown backup policies - but I didn't consider this scenario.

My plan so far is to ensure I have a complete data backup (should be good as of yesterday) and maybe try using the the Bootdisk utility

from Petter Nordahl-Hagen to patch the registry or
zap the password

Re: Registry corruption, can't login

but without knowing what kind of damage is there I don't have a lot of faith that this will solve the problem.

Any other suggestions or am I looking at a full install? And how do I/we prevent this from happening in the future?!?!

Thanks!
Tony

Use ERUNT to backup the registry. It can be restored easily.

<http://www.larshederer.homepage.t-online.de/erunt/>
<http://www.larshederer.homepage.t-online.de/erunt/erunt.txt>

[Installing & Using ERUNT]
http://www.silentrunners.org/sr_eruntuse.html
<http://www.winxptutor.com/regback.htm>

[ERUNT] - Direct download
<http://www.aumha.org/downloads/erunt.zip>
<http://www.aumha.org/downloads/erunt-setup.exe>

--
Rock
MS MVP Windows - Shell/User