

## Re: detecting cached credentials on NT/2K/XP/03

**Source:**

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.kernel/2004-12/0215.html>

---

**From:** Chuck Chopp (*ChuckChopp\_at\_rtfmcsi.com*)

**Date:** 12/09/04

Date: Thu, 09 Dec 2004 12:34:20 -0500

Peter Huang [MSFT] wrote:

- > *Hi*
- >
- > *Thanks for your quickly reply!*
- >
- > *Based on my test, the LOGONSERVER environment variable will be the logon*
- > *DC's name whether or not we are logon with domain account with the cached*
- > *credentials or from DC.*
- >
- > *Also the LOGONSERVER will be local machine when we logon on the machine*
- > *with local account while not domain account.*
- >
- > *Can you have a test to see if there is any difference on your machine?*

I just repeated my test obtained the same results as before. Here's the configuration:

I have a Win2K Pro SP4 test workstation that is a member of a domain, and that domain also has a trust relationship with one other domain. One domain has a Win2K Server SP4 DC, and the other has a Win2K3 Server DC. I have logged on locally to the workstation using domain accounts from both domains, as well as using the local administrator account.

I shutdown both of the DC's so none are present to do the authentication for either of the domains. I then booted up my test workstation and proceeded to logon to it using cached domain credentials. Finally, I ran CMD.EXE and examined the environment variable LOGONSERVER, which identifies my local workstation as the the system that serviced the logon request. The USERDOMAIN and USERDNSDOMAIN env vars still show the proper domain name values for my domain account, but the local workstation is definitely being reported as having serviced the logon request when the cached credentials ended up being use to allow the logon to be performed.

So far, this is the only test I have found that I can do reliably to determine if cached credentials are being used. I'd still prefer something more sophisticated that directly interrogates my primary access token rather

microsoft.public.win32.programmer.kernel: Re: detecting cached credentials on NT/2K/XP/03

than relying on what appears to be a side-effect, but if this is all that is available for me to use then I'll make use of it.

I need to expand the test to include a WinNT v4.0 Workstation system and some WinXP Pro & Home workstations as well to make sure they behave identically in this same situation.

--

Chuck Chopp

ChuckChopp (at) rtfmcsi (dot) com <http://www.rtfmcsi.com>

RTFM Consulting Services Inc. 864 801 2795 voice & voicemail

103 Autumn Hill Road 864 801 2774 fax

Greer, SC 29651

Do not send me unsolicited commercial email.