

Re: Local caching of AD-based Group Policy

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.group_policy/2006-09/msg00402.html

- *From:* "Frank" <fvbarger@xxxxxxxxxxxx>
 - *Date:* Thu, 28 Sep 2006 13:23:41 -0700
-

Darren –

I wasn't aware of the Windows Source Code thing for MVPs. That's a huge advantage, though MVPs typically do a lot of work to earn and maintain the designation. I greatly admire how you've succeeded in building a place for yourself which you fairly well own, by mastering a subject that one can get his arms around. Undoubtedly you know lots more besides Group Policy, but in that one area there aren't many like you. That's a good way for a man to live his life!

The removing the Win XP domain member from the domain question was one I was a little shy about asking, since I thought I should intuitively know the answer. Well, I am glad I asked. Maybe someday I'll be able to avert a problem.

Again, many thanks for your generosity with your knowledge and experience.

Frank

"Darren Mar-Elia (MVP)" <dmanonymous@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:eocbpUx4GHA.696@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Frank–

Glad I could help. It helps a great deal being an MVP, which allows us access to the Windows Source Code. Can't get any more authoritative than that when looking for an answer to why something works the way it does ;)

As to your question, my experience has been that if you just remove a machine from the domain, those policies stay "stuck" on the machine. Its kind of ugly in fact. The better way to do that, really, is, prior to removing the machine from the domain, move it to an OU that has no GPOs applying to it, sort of like a final resting place :). Then once GP has processed and been removed (i.e. once the settings that can be removed are removed—most security stuff won't be removed) then its safe to remove it from the domain.

Darren

Re: Local caching of AD-based Group Policy

—
Darren Mar-Elia
MS-MVP-Windows Server--Group Policy
<http://www.gpoguy.com> -- The Windows Group Policy Information Hub:
FAQs, Training Videos, Whitepapers and Utilities for all things Group
Policy-related
Group Policy Management solutions at <http://www.sdmssoftware.com>

"Frank" <fvbarger@xxxxxxxxxxxx> wrote in message
news:eUUKPIx4GHA.3600@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Darren –

I couldn't be more delighted that you are the one who answered my inquiry. In fact I hoped you would. Your Microsoft Press Group Policy Guide has been extremely useful it me. It's just that I was unable to localize an answer to this one question. The book is very readable and authoritative.

I do understand your explanation here, and it makes a lot more sense than what I've read from some other sources. Windows is a very logical system, particularly if one knows a bit of its history, so inaccuracies really stand out.

Now, with what you have told me, this leads to a rather minor follow-on question. If a Win XP Pro domain member is removed from the domain via the Computer Name tab in System Properties, I'd assume the AD-based Group Policy settings are removed too. Is that so?

Thanks for all your assistance!

Frank

"Darren Mar-Elia (MVP)"
<dmanonymous@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in
message [news:Q\\$5xmnr4GHA.3444@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:Q$5xmnr4GHA.3444@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Frank—
Group Policy settings are not cached in the sense that they are not processed when a domain member computer is not connected to the network. However, several things do occur in that scenario. First off, if GP settings are applied when you are connected to the domain, and then you disconnect and attempt to "muck" with your policy by editing the local GPO, you will find that to be ineffective. This is because

Re: Local caching of AD-based Group Policy

ALL GP

processing ceases to occur if a DC can't be contacted. So, any settings that were made by GP prior to disconnecting from the network are still there—not really cached because they are "live", just not updated.

Hope that makes sense. So the example below from Exam Cram is not correct. If you have a setting, like disabling the floppy, that's put in place when you're on the network, it will be retained when you're off the network, as long as the machine is part of a domain.

As for the role of ntuser.pol, you may have read me talking about it here or elsewhere. That file holds all registry policy that apply to the machine. Its role is to store all the merged policies when a computer or user is processing GP and then, to remove those policies during the next processing cycle, before re-applying new settings. That file is really the key behind registry non-tattooing behavior of true policies.

And really there is no relationship between cached creds, user profiles and policies.

Darren

—

Darren Mar-Elia
MS-MVP-Windows Server--Group Policy
<http://www.gpoguy.com> -- The Windows Group Policy Information Hub:
FAQs, Training Videos, Whitepapers and Utilities for all things Group Policy-related
Group Policy Management solutions at
<http://www.sdmssoftware.com>

"Frank" <fvbarger@xxxxxxxxxxxx> wrote in message
<news:O18fybq4GHA.4888@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Re: Local caching of AD-based Group Policy

I'm studying for the 70-270 exam and am confused about a point that I expect to be tested on. A couple of sources, particularly the Exam Cram 2 text, seem to strongly suggest that the SDOU settings will not be present if the Win XP Pro client is booted and the user logged in while disconnected from the domain. Thus if certain settings, like disabling the floppy, are to be in effect if the user is away from the network, they should be in Local Group Policy, not Domain-Based Group Policy. Other knowledgeable sources claim the opposite: That if the Win XP Pro client is booted and logged in on the domain network, and the SDOU settings have been processed to completion just once, then those settings (though not necessarily current) will be present ever more, under all circumstances, provided that the user has a domain account. Authoritative texts, such as ones about Win Server 2003, Active Directory, and Group Policy are silent on the point.

Now, if AD-based Group Policy settings ARE actually cached on the Win XP Pro client, could someone please tell me where they're stored? I'm actually acquainted with the NTUSER.POL files, but haven't been able to establish their exact function. From what I read somewhere in the distant past, it seems like they might be to remove discontinued policies.

I hope I can provoke a little discussion, just to see if I hear any agreement. It occurred to me that perhaps there has been confusion between Cached Logon Credentials, Cached User Profiles, and Cached AD-Based Group Policy. Well they are at least related, but do they actually go hand in hand?

Re: Local caching of AD-based Group Policy

I'd sure appreciate any help you can give me
on this matter.

Thanks!