

Re: Cached credentials and password expiration

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2005-01/0100.html

From: Herb Martin (*news_at_LearnQuick.com*)

Date: 01/04/05

Date: Mon, 3 Jan 2005 20:20:49 -0600

> *So are you referring here to a problem with the machine account
> password, or am I misunderstanding your suggestion?*

Actually I was thinking mostly of network issues, especially Name Resolution or routing, where the machine cannot even find/reach a DC.

I believe that when the machine account is hosed but the user reaches the DC that the domain account is NOT authenticated.

(I have seen this hear on our machines fairly regularly.)

> > *They key here is (I believe) that you can only use
> > cached credentials IF your computer cannot find
> > a DC to authenticate itself.*
>
> *We know that given the current VPN connection method, users DO NOT have
> access to a domain controller during the logon process. However, they
> are connected to the VPN on a very regular basis, since the VPN
> connection provides their *only* way to check e-mail and access other
> mission-critical enterprise applications. The real question is, does
> this regular (non-logon) network connectivity affect the cached
> credentials and how they behave over time?*

Well, users might not, but how about the IAS server?

Doesn't it authenticate the user through AD?

> *TIA.*
>
> --
> *Scott Lowe*
> *Mercurion Systems, Inc.*
>

microsoft.public.windows.server.active_directory: Re: Cached credentials and password expiration

--

Herb Martin

"Scott Lowe" <slowe-NOSPAM@NOSPAM-mercurionsystems.com> wrote in message news:33tharF4382pfU1@individual.net...

> On 2005-01-03 12:00:35 -0500, "Herb Martin" <news@LearnQuick.com> said:

>

> >> "Scott Lowe" <slowe-NOSPAM@NOSPAM-mercurionsystems.com> wrote in message

> >> news:33t5tqF3u0fboU1@individual.net...

>

> <snip>

>

> >> password expiration policies to be enforced. These remote users
> >> connect to the domain via VPN on a very regular basis, but are not able
> >> to logon "live" to a DC so that their cached credentials can be updated
> >> or so that they can receive password expiration notices. (There is a
> >> fix for that in the works, but it will be a while before that can be
> >> rolled out to everyone.)

> >

> > Why not? It is possible to authenticate through such,
> > in fact this has been going on with RRAS and it's
> > predecessors using dial for years.

>

> It's not a matter of technology. The specifics of this particular
> environment and this particular network are driving that timeline. For
> *this* environment, it will be a few months before "live" network
> logons over a VPN connection are possible.

>

> >> So, do the cached credentials also include password expiration
> >> information? If not, any one have any other suggestions as to why this
> >> may be occurring (users suddenly unable to logon to their workstation
> >> with cached credentials--error message is "No domain controller
> >> available to log you on" or similar).

> >

> > I don't believe so -- it is more likely the machine
> > is authenticating ITSELF with the domain, at that
> > point it CAN deny the user access.

>