

Re: iis lockdown & admin logout

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2003-03/0479.html>

From: David Wang [Msft] (someone@online.microsoft.com)

Date: 03/06/03

From: "David Wang [Msft]" <someone@online.microsoft.com>
Date: Wed, 5 Mar 2003 21:56:37 -0800

I asked around, and I was told that if you used the administrator account as the "Anonymous User" on any vdir, you will get into this state. All Anonymous Users are placed in a web_anonymous group, which is then denied access to the System32 directory (so it can't run cmd.exe, etc to even log in). Once in this state, if you don't have another administrative account, you're hosed.

You can get out of any NTFS ACL situation, though, by physically moving the affected HDD to another machine that's also running NTFS. You log in as the administrator on the other machine and reset ACLs on the affected HDD.

--

//David

This posting is provided "AS IS" with no warranties, and confers no rights.

//

"lt" <tighe@brandeis.edu> wrote in message
news:054801c2e34f\$8b718770\$3401280a@phx.gbl...

David,

Running Windows 2000 Server + all latest service packs and hotfixes. It's running only the webservice (no active directory or other services). We had run the IIS lockdown when we originally set the machine up. Since then, we had made a number of changes to the site, and I thought maybe it would be good to "re-run" the IIS lockdown tool. It detected that it had already been run and said it would revert settings to default (or original?) settings before re-running. I said "okay". It went through the process of reverting and then while it was running to re-apply is when the runtime error occurred. So, my guess is that it had to do with re-running it since we had run it originally on the machine and had no problems. And, another user suggested that it's switching the admin account into the "web_anonymous" group, which has no log on locally privileges. When one tries to logon with any valid account on the machine, it loads all the local settings and then logs you out. So, that log-on locally security settins were changed does appear to be the issue.

>-----Original Message-----

>Hmm, I have not heard about this, but I will check on getting an

>investigation on it so that we can release possible

microsoft.public.inetserver.iis.security: Re: iis lockdown & admin logout

workarounds (either
>programmatic fix, or how to get out of the situation).
>
>So, it's just running NT4 Server + latest IIS Lockdown
results in a runtime
>error?
>
>--
>//David
>This posting is provided "AS IS" with no warranties, and
confers no rights.
>//
>"Wayne & Carr" <NoSpam@spam.net> wrote in message
>news:uRNBpve4CHA.2296@TK2MSFTNGP10.phx.gbl...
>You have just ran into a Major problem, That myself had
in my network
>On my server, that usually gets about 500+ hits per day.
>I tried everything that everyone told me to do, And it
did not work.
>If you are running the "WinNT 4.0 Server" And the
new "iis lockdown"
>Then, I think that there seems to be an issue with it and
running it on NT4.
>Not sure, this is just my own personal opinion.
>
>Though I got a log of good suggestion from people in the
newsgroup(s),
>known of them worked.
>I indeeded up having to reinstall my server from
scratch "AGAIN".
>
>Because there is one thing that you have to look at.
>When you installed the "iis lockdown" tool, and you got
the runtime error,
>>From that point on, you basically have lost all rights to
your server.
>Which is a pain in the A**, but there is basically
nothing that I am aware
>off
>And that all the suggestions that I got in, no one was
able to tell me,
>Yes this worked for me, It was all just,"Try this, Read
more into the iis
>lockdown next time,
>and so forth,"
>
>So, unless you can find someone that has "Successfully"
fixed this issue,
>There is not much that
>you can do, But I would wait, and if you are running a
productive server,
>(Like I am here)
>Then you are most likely wanting to get it back LIVE
a.s.a.p.
>Think about doing to reinstall,
>It takes me about 4 hours, from shut down, to being back
Fully online again,
>To do mine.
>Then pointing records, and setting up DNS, is an
additional 1 hour.
>So basically about 5hours, and it is ready.
>

microsoft.public.inetserver.iis.security: Re: iis lockdown & admin logout

>Sorry that this is not what you are wanting to hear.
>
>Take Care
>Wayne
>
>
>
>
>
>