

Re: Default Shares on Member Servers

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2006-10/msg00086.html>

- *From:* "Roger Abell [MVP]" <mvpNoSpam@xxxxxxx>
 - *Date:* Thu, 12 Oct 2006 15:58:42 -0700
-

Well, something is really toasty here.

If the C\$, etc. are indeed the administrative shares, then the access should be allowed for Administrators only.

A couple things to examine:

1. what is the membership in the Administrators group of the member that does not require authN ?
2. when you try to look in through the Permissions button for a drive root's share (in its properties, sharing tab) are you shown "This has been shared for administrative ... "
(one can shut off admin shares, and then define a C\$ that is permissioned other than expected)

The Logon on over the network user right only determines what accounts can try to access shares, but the permissions on each share still determines which of those allowed to try accounts will succeed.

Also, on the machine from which you are testing that allows unauthenticated access, make sure that you try this after a fresh login, that there are no persistent shares, and that running control keymgr.dll does not show that there are cached network credentials to use when accessing the member.

Let's start there, and after the more simple possibilities are ruled out, then post back.

Roger

"JB" <me@xxxxxx> wrote in message
[news:eKyXg.23231\\$pa.20155@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](news:eKyXg.23231$pa.20155@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

I'm trying to secure access to our servers. We have 2 domain controllers, 1 windows 2000, the other windows 2003 and 3 member servers, all running windows 2003.

Re: Default Shares on Member Servers

From a computer that is not a member of the domain, attempting to access an administrative share on a DC, we are presented with a prompt for a username and password.

The same computer connecting to an administrative share on a member server, there is no prompt and the access is allowed.

Our AV software uses administrative shares to update so I can't simply disable them.

I assumed this had something to do with the 'Access this computer from the network' policy but this appears not to be the case; The 'Everyone' group is assigned this permission on the DC's and authentication is required for those servers.

How can I prevent unauthenticated access to these member server shares, or even better, only permit Administrators access to the shares?

Do i need to manually create the shares with custom security?

Thanks.

--

JB