

Re: Keep admins off of client machines

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2006-01/msg00524.html>

- *From:* "Gregg Hill" <bogus@xxxxxxxxxxxx>
 - *Date:* Wed, 4 Jan 2006 08:54:20 -0800
-

Good point about the email notification. Kind of hard to go grab that sucker!

Gregg Hill

"Ray Collins" <ray.collins@xxxxxxxxxxxxxxxxxxxx> wrote in message news:Ocu1mkSEGHA.3820@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

- > yes he could, but if you have your auditing set correctly there will be
- > an entry when he changed or disabled the settings then there will be
- > entries after they are turned back on. It is not impossible (nothing ever
- > is) to remove individual entries from the logs but it is extremely
- > difficult.
- >
- > There are a number of products (including what is built into SBS) that can
- > monitor the event logs and then do some action such as e-mail or page you.
- > You could set monitoring events for specific security log events and have
- > the system e-mail you immediately.
- >
- > As part of your overall security you would have auditing on computer room
- > access and floor/building access. So you know who changed the auditing
- > settings at what time, when they were turned back on and who was in the
- > building. You didn't stop him but you know he was there and that is the
- > important thing.
- >
- >
- > HTH
- >
- >

- > "Gregg Hill" <bogus@xxxxxxxxxxxx> wrote in message
- > news:O4kmcSNEGHA.1312@xxxxxxxxxxxxxxxxxxxxxxxxxxxx
- >> Thanks for the links! But if the person is knowledgeable, cannot he just
- >> delete the setting you have made, does his snooping, then reset your
- >> settings?
- >>
- >> Gregg Hill
- >>
- >>

Re: Keep admins off of client machines

>> "Ray Collins" <ray.collins@xxxxxxxxxxxxxxxxxxxx> wrote in message

>> news:e1PweUdDGHA.412@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

>>> Turning off auditing can generate on audit event and you can create an
>>> auditing group and give it access to the security log while denying
>>> administrators access. Administrators are not as Omnipotent as you
>>> think, yes they may do something but you can track what they do.

>>>

>>>

>>>

>>> A couple of articles to get you started:

>>>

>>>

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/bc9f1bed-1c85-413a-869e-9>

>>>

>>>

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/5658fae8-985f-48cc-b1bf-bc>

>>>

>>> <http://www.windowsecurity.com/articles/Auditing-Users-Groups-Windows-Security-Log.html>

>>>

>>> By the way you can specify in Active Directory that specific accounts
>>> can only log onto certain machines so you can restrict the admins to
>>> only the servers and if they change the settings you catch them in the
>>> audit logs.

>>>

>>>

>>> HTH

>>>

>>>

>>> "Gregg Hill" <bogus@xxxxxxxxxxxx> wrote in message

>>> news:OTewCbbDGHA.1384@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

>>>> Even if you audit, an admin who is determined can turn off auditing,
>>>> snoop around, then turn it back on, leaving no trace of the snooping.

>>>>

>>>> Gregg Hill

>>>>

>>>>

>>>> "Nick" <nickmirro@xxxxxxxxxxxxxxxx> wrote in message

>>>> news:u9oltmXDGHA.312@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

>>>>> Well this is eye opening. The discussion is informative. The issue
>>>>> first came up due a ways back following an apparent pointless
>>>>> sharrepoint admin logon to a local laptop. A new profile was created
>>>>> under D&S. This was unsettling.

>>>>>

>>>>> I think the Audit route would be best. The admins do periodically
>>>>> need access to various machines, so we can't rely on inventorying
>>>>> profiles. Being I'm not an developer myself (though with admin
>>>>> privileges) how do I audit admin activity?

>>>>>

>>>>>

>>>>>

>>>>> "Nick" <nickmirro@xxxxxxxxxxxxxxxx> wrote in message

