

Re: Keep admins off of client machines

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2006-01/msg00377.html>

- *From:* "Gregg Hill" <bogus@xxxxxxxxxxxx>
 - *Date:* Tue, 3 Jan 2006 18:14:35 -0800
-

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

"Ray Collins" <ray.collins@xxxxxxxxxxxxxxxx> wrote in message <news:e1PweUdDGHA.412@xxxxxxxxxxxxxxxxxxxxxxxx>

- > Turning off auditing can generate an 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@xxxxxxxxxxxxxxxxxxxxxxxx>

- >> 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.

Re: Keep admins off of client machines

>>
>> Gregg Hill
>>
>>
>> "Nick" <nickmirro@xxxxxxxxxxxxxxxx> wrote in message
>> news:u9oltmXDGHA.312@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
>>> 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
>>> news:urp8i3PDGHA.812@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
>>>> We have an SBS admin, a Sharepoint admin and 2 others who go between
>>>> our SBS and local Linux server. Those helping administer the servers
>>>> should not have access to client machines as they contain patient
>>>> records, proprietary applications, etc. How can we prevent transient
>>>> administrators with admin status from logging onto client machines
>>>> (unless essential) since those machines contain sensitive data?
>>>>
>>>
>>>
>>
>>
>
>

• *Follow-Ups:*

- ◆ *Re: Keep admins off of client machines*
 ◇ *From:* Ray Collins

- Prev by Date: *RE: Setup error, Needs SQL 2000 SP3 when SP4 already installed*
- Next by Date: *RE: Domain & Workgroup Access on XP Pro SP2*
- Previous by thread: *Re: Client Log in after AD Migration*
- Next by thread: *Re: Keep admins off of client machines*
- Index(es):
 - ◆ *Date*
 - ◆ *Thread*