

Re: track user logons

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2004-05/4508.html

From: Carey Frisch [MVP] (mrxp2004_at_nospamyahoo.com)

Date: 05/28/04

Date: Fri, 28 May 2004 08:49:16 -0500

You can monitor many different types of events on a Windows XP Professional system, including user actions such as logging on and logging off, and the success and failure of key application events. Administrators need to monitor these events to track security, system performance, and application errors.

You can set up audit policies to track authorized and unauthorized access to resources. By default, auditing is not enabled. Before you enable auditing, it will be important for you to define exactly what needs to be audited and why you want it to be audited. Auditing can slow down system performance, and it will also require effort on your part to evaluate audit logs; therefore, advanced planning is recommended to ensure that you track appropriate system events without creating excess administrative overhead.

For example, if you decide to audit account logon sessions, you need to consider what the information will be used for. Your security administrators group might be interested in logging failed logon events because this can indicate that someone is trying to log on with an account for which he or she does not have the correct password. Alternatively, you might want to log successful logon attempts to determine whether users are accessing workstations in areas of the network that they are not permitted to use.

To enable auditing, use the Microsoft Management Console with the Group Policy snap-in focused on the local computer. To see the different types of objects for which auditing can be configured, navigate to the following folder: Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy.

The Security log, in Event Viewer, if configured to do so, records security events, such as valid and invalid logon attempts.

Events that are related to resource use, such as creating, opening, or deleting files, can also be logged. An administrator can specify the events that are recorded in the security log policy.

Ref: Microsoft Windows XP Resource Kit

<http://www.jsiinc.com/SUBN/tip6800/rh6880.htm>

--

Carey Frisch
Microsoft MVP
Windows XP - Shell/User
Be Smart! Protect your PC!
<http://www.microsoft.com/security/protect/>

"C.D." <anonymous@discussions.microsoft.com> wrote in message:

Re: track user logons

microsoft.public.windowsxp.security_admin: Re: track user logons

news:74A0365C-0A17-4CDC-A55B-4A7507E2A367@microsoft.com...

| Hello all,

| My boss wants me to track the user logons in the company to discern what times they are logging of their workstation. I know how to set up audit policies to track this, but is there any other way to accomplish this instead of having to sift through the event logs every day?

| TIA!

|

| C.D.