

Re: Ghost in the Recycle Bin

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help_and_support/2004-04/1736.html

From: Wesley Vogel (123WVogel955_at_comcast.net)

Date: 04/04/04

Date: Sun, 04 Apr 2004 17:37:27 GMT

Start | Run | Type: gpedit.msc | OK |

Local Computer Policy\Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy\

- Audit account logon events
- Audit account management
- Audit directory service access
- Audit logon events
- Audit object access
- Audit policy change
- Audit privilege use
- Audit process tracking
- Audit system events

--

In the details pane, right-click the attribute or event you want to audit. In Properties, select the options you want, and then click OK.

=====

- Settings for Event Log
- Maximum application log size
- Maximum security log size
- Maximum system log size
- Prevent local guests group from accessing application log
- Prevent local guests group from accessing security log
- Prevent local guests group from accessing system log
- Retain application log
- Retain security log
- Retain system log
- Retention method for application log
- Retention method for security log
- Retention method for system log

To reset an event log to default settings
In the console tree, click the log you want to reset.
On the Action menu, click Properties.
On the General tab, click Restore Defaults.
To clear the log, click Clear Log.
Under Log size, select one of these options:
If you do not want to archive this log, select Overwrite events as needed.

To filter events in an event log

microsoft.public.windowsxp.help_and_support: Re: Ghost in the Recycle Bin

In the console tree, select the log you want to filter.
On the View menu, click Filter.
On the Filter tab, specify the characteristics you want.

=====

--

Hope this helps. Let us know.

Wes

In news:uv7gWHlGEHA.3880@TK2MSFTNGP09.phx.gbl,
TCEBob <tcebobc@comcast.com> hunted and pecked:

> Ok, the Event Viewer is functional. But nothing new is being added to
> the app log or the sec log. I activated and deactivated some programs
> (including OE), deleted and restored some files. Emptied the Recycle
> Bin. No additions. Also went through the services and turned on
> anything with the word "log." In desperation I looked in help.

>

> Here's what I learned:

> "The application log contains events logged by applications or
> programs."

> : Basically the application has to want to log the events.

>

> "The security log records events such as valid and invalid logon
> attempts, as well as events related to resource use such as creating,
> opening, or deleting files or other objects."

> : This looks like the place to see what's up with the Recycle Bin.

>

> "The system log contains events logged by Windows XP system
> components."

>

> I'm headed for Google to see if there is a log program that will
> record and annotate every file i-o action.

>

> rs

>

>

> "Wesley Vogel" <123WVogel1955@comcast.net> wrote in message
> news:BqTbc.66872\$gA5.821900@attbi_s03...

>> : -)

>>

>> It just goes to show ya, it's always something.

>>

>> --

>> Hope this helps. Let us know.

>> Wes

>>

>> In news:OUV4%235dGEHA.3940@tk2msftngpl3.phx.gbl,

>> TCEBob <tcebobc@comcast.com> hunted and pecked:

>>> Thank you. It was disabled.

>>>

>>> rs

>>>

>>> "Wesley Vogel" <123WVogel1955@comcast.net> wrote in message

>>> news:FFCbc.172583\$Cb.1673077@attbi_s51...

>>>> From:

>>>> http://www.kellys-korner-xp.com/xp_abc.htm

>>>>

>>>> Click the "E"

>>>> Scroll down to: Event Log

>>>>

>>>> Event Log

>>>>

>>>> [[One of the administrative tools in Microsoft Management Console,

>>>> Event Viewer maintains logs about program, security, and system

microsoft.public.windowsxp.help_and_support: Re: Ghost in the Recycle Bin

```
>>>> events on your computer. You can use Event Viewer to view and
>>>> manage the event logs, gather information about hardware and
>>>> software problems, and monitor Windows security events.
>>>>
>>>> If Event Viewer reports on startup that one or more of your log
>>>> files is corrupt, you can remedy the situation as follows:
>>>>
>>>> Disable the Event Log service. Restart Windows XP. Delete the
>>>> corrupt log(s)-AppEvent.evt, Secevent.evt, and/or Sysevent.evt-from
>>>> %SystemRoot%\System32\Config (or wherever they may be).
>>>>
>>>> Your existing event data will be lost, but a new log file will be
>>>> created when the service is restarted, and that log will start to
>>>> accumulate new events. Re-enable the Event Log service, and start
>>>> the service. If the Event Log service doesn't restart successfully,
>>>> then restart Windows XP. You cannot delete or rename the log files
>>>> while the Event Log service is running.]]
>>>>
>>>> --
>>>> Hope this helps. Let us know.
>>>> Wes
>>>>
>>>> In news:00sV2aZGEHA.1884@TK2MSFTNGP11.phx.gbl,
>>>> TCEBob <tcebobc@comcast.com> hunted and pecked:
>>>>> Thank you, Wesley.
>>>>>
>>>>> 1) Scheduled Tasks is empty.
>>>>>
>>>>> 2) There are bytes in the Application, Security and System but
>>>>> they cannot be read. Error comment: "Unable to complete the
>>>>> operation of "Application". The interface is unknown." I groped
>>>>> around in \windows\system32\config and found AppEvent.evt but
>>>>> could not read it in english. The best I could do was view in
>>>>> unicode mode. There seems to be a lot of Norton entries. I kicked
>>>>> norton out several months ago so I'm thinking that the log is not
>>>>> being updated. Is there a service pertaining to logs that might
>>>>> not be active?
>>>>>
>>>>> rs
>>>>>
>>>>> "Wesley Vogel" <123WVogel955@comcast.net> wrote in message
>>>>> news:l_Abc.168572$_w.1801894@attbi_s53...
>>>>>> 1) This will open Scheduled Tasks.
>>>>>> Start | Run | Type: control schedtasks | OK |
>>>>>> Anything listed?
>>>>>>
>>>>>> 2) You already have a log. This will open your Event Viewer.
>>>>>> Start | Run | Type: eventvwr | OK |
>>>>>> Look at:
>>>>>> Application
>>>>>> Security
>>>>>> System
>>>>>> Look at Wednesday AM.
>>>>>>
>>>>>> --
>>>>>> Hope this helps. Let us know.
>>>>>> Wes
>>>>>>
>>>>>> In news:%23uAMJDXGEHA.3772@TK2MSFTNGP12.phx.gbl,
>>>>>> TCEBob <tcebobc@comcast.com> hunted and pecked:
>>>>>>> A malevolent power is emptying my recycle bin every Wednesday
>>>>>>> morning. Ok, I know it's scheduled somewhere, but I can't find
```

microsoft.public.windowsxp.help_and_support: Re: Ghost in the Recycle Bin

```
>>>>>> where. Aside from XP Pro service pack 1 I have AVG anti virus,
>>>>>> Zone Alarm, and AdSubtract running. Windows firewall is
>>>>>> disabled.
>>>>>>
>>>>>> 1. Any educated guesses where the scheduled event is?
>>>>>>
>>>>>> 2. Can I set up a log of events to try and pin it down?
>>>>>>
>>>>>> rs
>>>>>>
>>>>>>
>>>>>> ---
>>>>>> Outgoing mail is certified Virus Free.
>>>>>> Checked by AVG anti-virus system (http://www.grisoft.com).
>>>>>> Version: 6.0.644 / Virus Database: 412 - Release Date: 3/29/2004
>>>>>
>>>>>
>>>>> ---
>>>>> Outgoing mail is certified Virus Free.
>>>>> Checked by AVG anti-virus system (http://www.grisoft.com).
>>>>> Version: 6.0.644 / Virus Database: 412 - Release Date: 3/29/2004
>>>>
>>>
>>> ---
>>> Outgoing mail is certified Virus Free.
>>> Checked by AVG anti-virus system (http://www.grisoft.com).
>>> Version: 6.0.644 / Virus Database: 412 - Release Date: 3/29/2004
>>
>
>
> ---
> Outgoing mail is certified Virus Free.
> Checked by AVG anti-virus system (http://www.grisoft.com).
> Version: 6.0.648 / Virus Database: 415 - Release Date: 3/31/2004
```