

Re: System Restore Keeping Only One Restore Point

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help_and_support/2008-05/msg02372.htm

- *From:* "Danno" <danreardon@xxxxxxx>
 - *Date:* Sun, 25 May 2008 00:40:27 GMT
-

I opened those enormous SR restore point files and in one of them I found 190 .RDB files, each being 2.84Mb (all the same size).

And in the other huge SR file, I found 212 .RDB files and they were all the same size, also at 2.84 Mb each.

I've been searching on the net to find out what .RDB files are and to be quite honest, I'm none the wiser.

Anyway, I assume this wasn't supposed to happen? I wonder if it will happen again, next time the system automatically creates a restore point. By that I mean, next time the system creates a restore point automatically and not as a result of my causing it by downloading something... for example.

Can anybody tell me what an .RDB file is and why System Restore included them in those two huge restore point files... both on the same day? Just as an added point of interest, any defrag analysis I do always shows SR as the most fragmented files on my computer. Is this normal?

In all fairness to ZoneAlarm, I now doubt ZoneAlarm has anything to do with this.

Dan

"Bill in Co." <not_really_here@xxxxxxxxxxxxxxxx> wrote in message news:u6sehGfvIHA.5620@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Danno wrote:

Hi Bill in Co.,

Yeah, those two huge SR files are ginormous. I'm really interested in two things here:

First, what in hell would cause SR to store files that big?

Re: System Restore Keeping Only One Restore Point

Either something bad happened during the creation of those restore points (like some other task was running, that screwed it up, in process), OR (and this I think is a long shot – it was that large because of some HUGE amount of registry and file changes that were made since the previous restore point, and it needed that amount of disk space (but I really doubt this possibility). Well, those are the two possible explanations that come to mind for me, anyways.

Secondly, since I've found those files, would I be asking for trouble to delete them manually? My guess is yes, so obviously I wouldn't do that (even if I got the green light from experts. I'd just get rid of them using SR itself).

Do it that way (not manually). Your hunch is right – let System Restore remove them properly (like by the way I mentioned previously), and it will do the necessary housekeeping for System Restore and its bookmarking. Don't do it manually.

It's more a case of just wanting to know if that would be OK, or would that completely screw up the registry. I wouldn't be tempted to do it... it's just that I'm on a learning curve here. Those files are hidden for a reason, and I'm guessing it's to keep monkeys like me from playing with them.

As I said, I would NOT do it manually. Yes, there is a chance it could work, but I sure would NOT bank on it! (I think that could and probably would present problems for using the existing restore points that are left)

But ultimately, I'd like to know what's in those files to make them so big.

Outside of what I mentioned, I don't know. I suppose you could check the date–time stamps of those two bogus system restore points, and then search around on your hard drive for any suspicious file or folder activity around those dates (like the date stamps on files or folders that had changed somewhere around those dates), to see if something suspicious shows up. Kind of a long shot, however.

Re: System Restore Keeping Only One Restore Point

Dan

"Bill in Co." <not_really_here@xxxxxxxxxxxxxx> wrote in message
news:utqNOsevIHA.4952@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Those two *extremely large* (600+MB) system restore points sound suspicious, just as you said. Why not clear them all out (by temporarily turning off System Restore), and then turn System Restore back on again (and create a good one) to start afresh?

And 3% should be adequate space, and would be, with good restore points (which are normally like 60 MB each – NOT 600+ MB).

Danno wrote:

Hi Gerry,

It's not really a matter of "how many restore points I'm keeping".

It's more a case of my trying to keep more than just ONE restore point. At this moment, there are 4 restore points from yesterday, and that's it. None of those were created automatically by the system. As I mentioned, the event viewer is not actually cataloging any "errors" about system restore, but here are two examples of reports (not tagged as an "error") that are addressing what I'm experiencing:

Event Type: Information
Event Source: SRService
Event Category: None
Event ID: 107
Date: 5/22/2008
Time: 3:37:36 AM
User: N/A
Computer: DANS-COMPUTER
Description:
The System Restore service has been suspended because there is not

Re: System Restore Keeping Only One Restore Point

enough
disk space available on the drive
\\?\Volume{95e0434a-0fff-11dd-8ae4-806d6172696f}\.
System Restore will
automatically resume service once at least
200 MB of free disk space is
available on the system drive.

For more information, see Help and Support
Center at
<http://go.microsoft.com/fwlink/events.asp>.

Event Type: Information
Event Source: SRService
Event Category: None
Event ID: 108
Date: 5/22/2008
Time: 4:41:13 AM
User: N/A
Computer: DANS-COMPUTER
Description:
The System Restore service has resumed
monitoring due to space freed on
the
system drive.

For more information, see Help and Support
Center at
<http://go.microsoft.com/fwlink/events.asp>.

For now, I've disabled ZoneAlarm and have
increased the allocated disc
space
for SR to the maximum. As I mentioned
before, I would have hoped that
3%
or
1075 MB would have been plenty of space,
but apparently not. Anyway,
if
the
problem is corrected, I'd think I've probably
narrowed it down to those
two
suspects. I'll consider the problem corrected
if, two weeks from now,
I
can
still see an available restore point that was
recorded yesterday.

Re: System Restore Keeping Only One Restore Point

At your suggestion, I found the folders that hold the 4 volumes of SR points. Apparently they are the following sizes: 627Mb, 52MB, 52Mb and 567Mb. My lord, two of those are way too big. What could be the reason for that? That would explain why 1075Mb isn't enough space to store very many SR points... if they're going to be that huge.

Thanks again for your interest.

Dan

"Gerry" <gerry@xxxxxxxx> wrote in message
news:OihJBNevIHA.516@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Danno

How many restore points are you keeping? How large are individual restore points? You should not need an allocation so large!

Can you please post a copy of the Event Viewer Information Report you refer to.

A tip for posting copies of Error Reports! Run Event Viewer and double click on the error you want to copy. In the window, which appears is a button resembling two pages. Click the button and close Event Viewer. Now start your message (email) and do a paste into the body of the message. Make sure this is the first paste after exiting

Re: System Restore Keeping Only One Restore Point

from
Event Viewer.

--

Hope this helps.

Gerry

~~~~

FCA

Stourport, England

Enquire, plan and execute

~~~~~

Danno wrote:

Thanks
Kayman,

Of all the
links and
suggestions
you offered,
one of them
might be
surprisingly
helpful. Not
surprising
that Kelly's
Korner was
helpful, but
a surprise to
me at the
result.

On Kelly's
Korner, I
found the
category
discussing
missing SR
points,
specifically
this:

– Check the
event logs

Re: System Restore Keeping Only One Restore Point

to
investigate
System
Restore
service
errors:

1. Click Start, click Control Panel, and then click "Performance and Maintenance".
2. Click Administrative Tools, click Computer Management, double-click Event Viewer, and then click System.
3. Click the Source tab to sort by name, and then look for "sr" or "srservice." Double-click each of these services, and then evaluate the event description for any indication of the cause of the problem.

I followed
the advice
and lo and
behold,

Re: System Restore Keeping Only One Restore Point

there were descriptions of events that happened with SR. None of the events actually showed up as "errors", but none-the-less they described that SR was "suspending" and then "resuming" due to lack of space allocated and then more space being re-allocated. I was convinced that 3% or 1076MB would be plenty of space, but apparently not. If I'm not mistaken though, even when I accidentally had 12% allocated, SR was still only allowing one restore point. So I've now allocated 10% of disc space or

Re: System Restore Keeping Only One Restore Point

3700MB to
see what
happens.
That is an
outrageously
huge
amount of
space to
allow, but
I have to do
it for now.

I'll let you
know.
Thanks
again!

Danno

"Kayman"
<kaymanDeleteThis@xxxxxxxxxxxx>
wrote in
message
news:u7r5OCXvIHA.5448@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

On
Sat,
24
May
2008
01:23:55
GMT,
Danno
wrote:

<snip
for
brevity>

Maybe
I
should
disable
ZoneAlarm
altogether
for
3
or
4
days,

Re: System Restore Keeping Only One Restore Point

and
use
the
built
in
Windows
firewall...
just
to
test
if
ZA
is
involved
in
any
way
with
my
dilemma.

Very,
very
sensible
approach;
IMO,
ZA
is
not
worth
having.
I'd
uninstall
the
entire
ZA
suite
for
good
and
ask
for
a
refund.
If
uninstalling
via
the
Add/Remove

Re: System Restore Keeping Only One Restore Point

program
does
not
work
satisfactory
then
go
to:
<http://zonealarm.donhoover.net/uninstall.html>

Revo
Uninstaller
<http://www.revouninstaller.com/>
can
also
be
of
assistance

Consider
the
following:
For
the
average
homeuser,
the
Windows
Firewall
in
XP
does
a
fantastic
job
at
its
core
mission
and
is
really
all
you
need
if
you
have
an
'real-time'
anti-virus

Re: System Restore Keeping Only One Restore Point

program,
[another
firewall
on
your
router
or]
other
edge
protection
like
SeconfigXP
and
practise
safe-hex.
The
windows
firewall
deals
with
inbound
protection
and
therefore
does
not
give
you
a
false
sense
of
security.
Best
of
all,
it
doesn't
implement
lots
of
nonsense
like
pretending
that
outbound
traffic
needs
to
be
monitored.

Re: System Restore Keeping Only One Restore Point

Activate
and
utilize
the
Win
XP
built-in
Firewall;
Uncheck
all
Programs
and
Services
under
the
Exception
tab.
Read
through:
Understanding
Windows
Firewall.
<http://www.microsoft.com/windowsxp/using/security/internet>
Using
Windows
Firewall.
<http://www.microsoft.com/windowsxp/using/networking/secu>
Exploring
the
windows
Firewall.
<http://www.microsoft.com/technet/technetmag/issues/2007/06>
"Outbound
protection
is
security
theater—it's
a
gimmick
that
only
gives
the
impression
of
improving
your
security
without
doing
anything

Re: System Restore Keeping Only One Restore Point

that
actually
does
improve
your
security."

In
conjunction
with
WinXP
Firewall
use:

Seconfig
XP
1.0

<http://seconfig.sytes.net/>

(<http://www.softpedia.com/progDownload/Seconfig-XP-Do>

Seconfig
XP

is
able
configure
Windows

not
to
use
TCP/IP

as
transport
protocol
for

NetBIOS,
SMB

and
RPC,

thus
leaving
TCP/UDP

ports
135,
137-139

and
445

(the
most
exploited
Windows
networking
weak
point)
closed.)

Re: System Restore Keeping Only One Restore Point

Real-time
AV
applications
–
for
viral
malware.
Do
not
utilize
more
than
one
(1)
real-time
anti-virus
scanning
engine!
Disable
the
e-mail
scanning
function
during
installation
(Custom
Installation
on
some
AV
apps.)
as
it
provides
no
additional
protection.
Avira
AntiVir®
Personal
–
FREE
Antivirus
<http://www.free-av.com/>
You
may
wish
to
consider
removing
the

Re: System Restore Keeping Only One Restore Point

'AntiVir
Nagscreen'
http://www.elitekiller.com/files/disable_antivir_nag.htm
or
Free
antivirus
–
avast!
4
Home
Edition
It
includes
ANTI-SPYWARE
protection,
certified
by
the
West
Coast
Labs
Checkmark
process,
and
ANTI-ROOTKIT
DETECTION
based
on
the
best-in
class
GMER
technology.
http://www.avast.com/eng/avast_4_home.html
(Choose
Custom
Installation
and
under
Resident
Protection,
uncheck:
Internet
Mail
and
Outlook/Exchange.)
or
AVG
Anti-Virus
Free
Edition

Re: System Restore Keeping Only One Restore Point

<http://free.grisoft.com/>

(Choose
custom
install
and
untick
the
email
scanner
plugin.)

Why
You
Don't
Need
Your
Anti-Virus
Program
to
Scan
Your
E-Mail

<http://thundercloud.net/infoave/tutorials/email-scanning/index>

On-demand
AV
applications.
(add
them
to
your
arsenal
and
use
them
as
a
"second
opinion"
av
scanner).

David
H.
Lipman's
MULTI_AV
Tool

http://www.pctipp.ch/ds/28400/28470/Multi_AV.exe

<http://www.pctipp.ch/downloads/dl/35905.asp>

English:

<http://www.raymond.cc/blog/archives/2008/01/09/scan-your->

Additional

Re: System Restore Keeping Only One Restore Point

Instructions:

http://pcdid.com/Multi_AV.htm

and/or

BitDefender10

Free

Edition

<http://www.bitdefender.com/PRODUCT-14-en--BitDefend>

A-S

applications

-

for

non-viral

malware.

The

effectiveness

of

an

individual

A-S

scanners

can

be

wide-ranging

and

oftentimes

a

collection

of

scanners

is

best.

There

isn't

one

software

that

cleans

and

immunizes

you

against

everything.

That's

why

you

need

multiple

products

to

do

Re: System Restore Keeping Only One Restore Point

the
job
i.e.
overlap
their
coverage
–
one
may
catch
what
another
may
miss,
(grab'em
all).

SuperAntispyware

–
Free
<http://www.superantispyware.com/superantispywarefreevspro>
and
Ad-Aware
2007

–
Free
http://www.lavasoftusa.com/products/ad_aware_free.php
<http://www.download.com/3000-2144-10045910.html>

and
Spybot
Search
&
Destroy

–
Free
<http://www.safer-networking.org/en/download/index.html>
and
Windows
Defender

–
Free
<http://www.microsoft.com/athome/security/spyware/software>
WD
monitors
the
start-registry
and
hooks
registers/files
to
prevent

Re: System Restore Keeping Only One Restore Point

spyware
and
worms
to
install
to
the
OS.
Interesting
reading:
<http://www.pcworld.com/article/id.136195/article.html>
"... Windows
Defender
did
excel
in
behavior-based
protection,
which
detects
changes
to
key
areas
of
the
system
without
having
to
know
anything
about
the
actual
threat."

This
may
solve
your
original
problem:
System
Restore
for
Windows
XP
http://www.kellys-korner-xp.com/xp_restore.htm

And

Re: System Restore Keeping Only One Restore Point

routinely

practice

Safe-Hex.

<http://www.claymania.com/safe-hex.html>

Hundreds

Click

on

'Click

Here

to

Get

Infected'

Ad

<http://www.eweek.com/article2/0,1895,2132447,00.asp>

Good

luck

:)