The Old New Thing

What's the deal with the System Volume Information folder?

20 Nov 2003 4:24 PM | 53

In the root of every drive is a folder called "System Volume Information". If your drive is NTFS, the permissions on the folder are set so not even administrators can get in there. What's the big secret?

The folder contains information that casual interference could cause problems with proper system functioning. Here are some of the things kept in that folder. (This list is not comprehensive.)

- System Restore points. You can disable System Restore from the "System" control panel.
- Distributed Link Tracking Service databases for repairing your shortcuts and linked documents.
- Content Indexing Service databases for fast file searches. This is also the source of the `cidaemon.exe` process: That is the content indexer itself, busy scanning your files and building its database so you can search for them quickly. (If you created a lot of data in a short time, the content indexer service gets all excited trying to index it.)
- Information used by the Volume Snapshot Service (also known as "Volume Shadow Copy") so you can back up files on a live system.
- Longhorn systems keep WinFS databases here.

Blog - Comment List MSDN TechNet

Comments

Vladimir
20 Nov 2003 4:25 PM
#
So, it was not such a good idea to Take ownership of this folder and delete it after that?

H.M
20 Nov 2003 4:56 PM
#
Vladmir: Well, it's a great idea if you're *trying* to wreck the system.

Jeff
20 Nov 2003 6:15 PM
#
Hi Raymond - What is the file limit for any directory in Win2k using NTFS? Better yet, what's the O() notation for some basic file operations (directory listing, read, etc)? I've looked everywhere and I have not seen any definitive answers. For example, I have a directory on a website called "sounds" that has over 5,000 sounds in it and I want to (a) know how many more files I can add to that directory before I have a problem and (b)

predict the "performance" of certain file operations on the files in that directory. Thanks!

Karl
20 Nov 2003 6:33 PM
#

What exactly is the use of the tracking.log file? I just read Inside Microsoft Windows 2000 (an excellent book), and it said that the \$Extend\$ObjId metafile was responsible for link tracking. From what I understand, this file contains mappings from object IDs to file names. Does tracking.log do the same thing, except for files not on the same volume as the link?

MilesArcher
20 Nov 2003 6:49 PM
#

I don't want to try this and screw up my drive. Is it possible to give a user rights to this folder to look in it?

anp
20 Nov 2003 10:19 PM
#

MilesArcher Yes you can. I did. Not much to see on mine, so I set the permission back to the default. Neat though. For some reason it never occured to me to look at the file permissions for that folder.

Raymond Chen
21 Nov 2003 2:27 AM
#

Please don't submit the same question multiple times. Hey folks there's this great search engine called google. I asked google to search for "windows ntfs limits" and it found http://www.microsoft.com/technet/prodtechnol/winxppro/reskit/prkc_fil_tdrn.asp which gives the limits and also suggests that if you have more than 300,000 files in a directory you should look at the document "Optimizing NTFS Performance".

余啊雷
21 Nov 2003 3:16 AM
#

I don't think most of Jeffs questions were posted several times, it's just that it you get an exception and refresh too often you get lots of messages. Also if you don't know about google you can even do http://www.google.com/microsoft or http://www.google.com/linux if you want to narrow down your search before you even begin :)

Mike Dimmick
25 Nov 2003 12:06 PM
#

jeff: Raymond's comment doesn't quite cover what you wanted to know. The book "Inside Windows 2000" has a whole section on NTFS, where you can find out that NTFS directories are basically an index of the file names stored in the directory. This is a general indexing mechanism and can be applied to any kind of metadata that an index is defined on (for example, there's also an index which contains all the object identifiers for files assigned an object ID, so NTFS can locate files by object ID). The indexes are stored as a B+ tree (like a binary tree, but each node can have more than two direct children). This gives O(log N) performance for lookups and for inserts and deletes (I think). However, as the article Raymond pointed to notes, NTFS can start to struggle when looking for a unique 8.3 name in a large directory, since the way it works is to generate a name, try that, then generate the next, try that, etc. The algorithm seems to try to mitigate collisions by only using sequential numbers for the first four documents, switching to what looks like the same technique as GetTempFileName for characters 3-6 after this point (tested on Windows 2000). Unfortunately that only gives two characters based on the long name! If your system is anything like mine, you probably have a lot of folders called 'Microsoft'-something under Program Files - see for yourself. I have 18, but then this system has Office 2000, three versions of Visual Studio, two versions of eMbedded Visual Tools, ActiveSync, and the IntelliPoint software. You can show the short name with dir /x. It has to start from scratch each time because another thread could be trying to do the same thing, possibly on another processor. In terms of how many files you can add to the file system, the practical answer is 'until you run out of space'. The NTFS metadata grows as required. The Object ID mentioned above is a 16-byte GUID, so you'd have to create 3x10^38 before you started running out (although note that Object IDs are supposed to be globally unique).

Mike Dimmick
25 Nov 2003 12:39 PM
#

Extending my commentary further: the algorithmic complexity is O(M log[M] N) (where log[M] represents a logarithm in base M, i.e. the inverse operation of M^x). However, caching has an effect here - the non-leaf blocks are more likely to be cached than the leaf blocks (because they're accessed more frequently). The M term comes from a linear search of the leaf block in the classic implementation, but I believe NTFS keeps the leaf blocks sorted and uses a binary search on the block, so the overall complexity would be lower for lookups but slightly higher for inserts or deletes (reflecting the requirement to keep the leaf block sorted).

Norman Diamond
15 Dec 2003 2:11 AM
#

Regarding "System Restore points. You can disable System Restore from the "System" control panel." 1. That is partly true in Windows XP. The last time I did that on one system, the total size of files stored in the "System Volume Information" directory increased by 2 megabytes with every reboot. I don't know what was getting added with every reboot, but it was happening. (If you wonder how I knew, see below.) That particular system was one where the intention was to restore a ghosted image of the Windows XP partition every time a particular application needed to be tested, so on that system it was undesirable to have system restore points on that partition and it was undesirable to let that Windows XP installation write system restore points anywhere. 2. It doesn't seem to be true in Windows 2003. One of the first things I do after installing an OS that has System Restore is to disable storing System Restore stuff on partitions other than the partition where the OS is installed. I don't exactly want Windows XP storing restore points on the partition where Windows 2003 is installed and vice-versa.

But in Windows 2003 I have not found how to alter the System Restore settings. So the partition where I have Windows XP installed has some restore points that belong to Windows XP and some that belong to Windows 2003. 3. By the way Windows XP even created a restore point on an external hard disk that was connected for the first time by USB, before I remembered to open up the System Restore settings. I deleted the restore point from the USB disk. But I've had rare occasions to actually use system restores, and would have preferred to move the restore point to Windows XP's own partition, if there were some way to tell Windows XP to still know whatever it's supposed to know about the restore point. Regarding "The folder contains information that casual interference could cause problems with proper system functioning." In all except one case, I have added administrators with Read permissions and looked at the contents. (This is how I knew that on one system Windows XP was adding 2 megabytes of files to the System Volume Information directory on every reboot.) Now, you say "casual interference could cause problems with proper system functioning". Is this why Read permissions are not set by default? Is this really the reason for the default setting to irritate owners and usually tempt owners to max out their privileges and go tearing through deleting everything they don't want in it? Surely it would not be so bad to allow casual reading by default, just like in the \WINNT\INF folder.

Gaynor
24 Feb 2004 9:12 AM
#

I have recentyly found a Trojan virus in my System Volume Information folder. I try to open the folder and a message box comes up and says:
"C:\System Volume Information is not accessible"
"Access is denied"
I have run and updated various antivirus programs but none can get rid of it. How can I delete this virus?
So this is why i need to go into System volume infomation, ive only had my pc a short while but seem to be going in circle's :0(

Raymond Chen
24 Feb 2004 9:26 AM
#
Even administrators by default can't go into your System Volume Information folder; the trojan/virus must have installed a system service to get in there. (System services run at even higher privilege than administrators.)

You can take ownership of the folder and then grant yourself full access. Antivirus programs really should be taking care of this for you. You're deep into security brain surgery at this point.

CHESO
28 Feb 2004 4:56 AM
#
I had the same problem last night with my other computer. I could fix some of the other files with the antivirus, but the virus (trojan) got exactly to the same point Gaynor is saying System Volume Information)and I cant get into it to fix it....can anyone give a a better idea of how to take ownership and grant full acces...and after that how do I get

to it? I appreciate any help...

Raymond Chen
28 Feb 2004 10:07 AM
#
To take ownership, turn off "Hide protected operating system files" and turn on "Show hidden files and folders". Then right-click, Properties, Security, Advanced, Owner, and there you can take ownership.

Alan
1 Mar 2004 6:24 AM
#
I'm A NOVICE. My information is that the "restore" reference in the SVI folder is associated with the XP "System Restore" function. If you have a Virus in the SVI you will have it among one or more of your Sys Restore Points. Symantec advises that unless you turn off System Restore you cannot run your Virus scan on the SVI. System Restore removes all "restore points" when it is turned off. Do you want them anyway if they're pointing to infected files? I have Administrator Rights as my computer is a stand alone setup. I have XP set to the Classic GUID. My "hide system folders" is off and I access the SVI using the "Windows Explorer" page, just to look in it. After the Virus scan I opened "cleanmgr" using Run-Start-then type cleanmgr. Cleanmgr indicated about 300mb of obsolete files that the SVI of my Drives/Volumes D: E: F: pointed to, that I removed with cleanmgr. After I ran the Scan I also deleted the "quarantine backup" files, & the "protected Files" in the Waste Bin. My OS seems fine now. Al

Chris
1 Mar 2004 2:44 PM
#
The truly funny thing, is that my computer DOES have a virus in that folder...it's a fun time trying to figure out how to clean THAT one...thank you WORM_NETSKY.C

Alexei
4 Mar 2004 11:53 PM
#
I'd like the opinion of someone more knowledgeable than I. I happened to find out (through a defrag program) that my SVI folder was huge. After using the above method to look into it, I can see that it has 2.5 GB of stuff _restore* folders. Now, I've turned System restore off and on and off again, but it seems to have no effect. I think I'm going to just delete it, but if anyone has any comments as to why that happened, I'd like to know. Also, the RECYCLED folder had some 6 GB of stuff in it, which did not register in the Recycle Bin, and could not be emptied in the usual fashion. What's going on?

anonymous
6 Mar 2004 3:38 AM
#
hi you may not think this but the
\System Volume Information folder has really

got a(n) instance of spyware. I would reccomend
take ownership and delete the folder. Believe
me or not microsoft has got spyware in your pc
lets just take the "BigFix" codenamed a little
reporting service it runs off of a secret file
in "C:\System Volume Information" it is a hiddden file that your little eyes cannot see
even if you do have hide protected os files
turned off the filename's called
"BLF_10102004.CAB" and i've just found this 9
weeks ago but the tracking.log file is spuware
and take ownership and delete the
"System Volume Information" folder.

Raymond Chen
6 Mar 2004 8:22 AM
#

Um, "BigFix" is not a Microsoft product. If you go to their web site you can see that they're an independent company.

luky
11 Mar 2004 2:21 PM
#

AVG tells me that I have a virus in "System Volume Information" but cannot delete it.
I have enabled "Show Hidden Folders etc." but cannot get ownership only "access denied".
When I right click the SVI folder under "Properties" I do not see a label "Security" only "General, Sharing and Customize". I am running XP Home.

Raymond Chen
11 Mar 2004 2:28 PM
#

If you're running Home, then boot into Safe mode. The "Security" option should then appear.

Mike S
17 Mar 2004 5:21 PM
#

In XP Pro you can change the size of the SVI folder in the System Control Panel [System Restore] tab (Settings...) button. Take a look at the SVI folder contents on each drive to see how may days of restore you have. I cut mine in half and from 1.2GB to 0.6GB and 4 mo. to 2 months.

Alexei,
If your RECYCLED bin larger than your Recycled Bin may be running something like the Norton Protected Recycled Bin. You can also adjust the size allocation for this through Norton Works interface or whatever you might have.

Al
26 Mar 2004 8:46 AM
#

Macafee every 30 minutes tells me that I have a reg/seeker virus in one of subfolders my "system volume information" folder. Every time I delete it, it comes back again. Some time also mcafee says that can not delet it.

I gained access to the folder and tried to delete the file A0023903.reg but it told me that I can not delet it because it is used by teh system. Every time that I delet the infected file, the next time the number at the end of the file name is incremented by 1.
It looks like that the file is generated by some other process. But I could not find the origin of this file. I tried to check for reg/seeker information as I found on the internet, but none of those signs are in my PC!

How I can get rid of this?

Btw: I found that for each day theres is a separate folder in my PC. This infected reg file comes back every time to the same folder wich is for 3 days ago when I first detected this virus. Can I delete entire folder for that day?

gigi
29 Mar 2004 5:12 PM
#

C:\system volume information_restore{999563C0-67F2-4C6C-8CBA-99E9D28438DA}\RP251\A0020861.EXE

this is what i'm getting on my system when avg shield is running...

anyone know what to do?

gigi
30 Mar 2004 6:14 PM
#

ok i got to the file and deleted the a0020861 :)

kimatthews
31 Mar 2004 5:46 AM
#

Found exessive use on C:\ drive - located files with system Defrag util. I got hit with virus "BKDR_HACDEF.73B" - deleted "C:\Windows\hxdefdrv.sys" (Trend Micro latest detected. Took ownership of "C:\System Volume Information" directory as administrator, gave self full access and removed attributes at DOS prompt "Attrib -h -r -s *.* /s /d". Then mapped to drive from another machine (as ADMIN) and deleted offending files in "C:\System Volume Information\tracking\dll" directory as applicable (did not delete all files BTW ie. .dll, etc.) Re-applied default permissions, rebooted and checked - OK. Updated virus scanner and restricted quotas on disk for all users - we'll see.

Raymond Chen

5 Apr 2004 11:13 PM
#
Perhaps an easier way to remove viruses from the _restore* folders is to go to All Programs, Accessories, System Tools, Disk Cleanup. From there you can delete old System Restore checkpoints.

taywood
11 Apr 2004 3:18 AM
#
Me too novice with a trojan in SVI_restore.
Grandson says to Turnoff System Restore, click Apply and click OK, restart XPHome.
He claims all stored data including the trojan will be removed.
Then do reboot, reenable System Restore and
immediately do a fresh Restore Point.
So before I struggle with this will it work?

Raymond Chen
11 Apr 2004 6:01 AM
#
You don't need to turn it off. Just create a restore point then tell System Restore to delete all but the most recent restore point. (Via the Disk Cleanup utility.)

This is all maddening - virus checkers are supposed to know how to deal with SVI. Based on all this feedback, the people who work with virus checkers are going to remind them about SVI at the next meeting, since it seems that a lot of virus checkers still don't quite know how to manage that directory.

taywood
11 Apr 2004 10:10 AM
#
Thanks Raymond, will do AV scan later.

But, just noticed on the black reboot screen
invalid boot.ini file, booting from C:\windows

What wording should I search on please and am I likely to be snookered by removing previous Restore Points?

Raymond Chen
11 Apr 2004 10:21 AM
#
Removing old store points just means that you won't be able to return to a previous configuration. The invalid boot.ini file is troubling though.

taywood
12 Apr 2004 2:09 AM
#

Troubling for you is panic for me!!

I have no boot.ini in msconfig
How do I get it back please and should I be posting on another thread and if so what wording should I search on.

I have no previous Restore Points now, I dont have a WinXP CD but I have the PCmanufacturers Recovery CD. I've used this to instal after my last crash and see I can use it for repair using a Recovery Console. Would this help me now.

Whats more is there an immediate problem in my system booting from C:\Windows and could it stay like that?

Raymond Chen
12 Apr 2004 4:19 AM
#
Fortunately the format of the boot.ini file is pretty simple. Copying it from a good machine will work if the two machines have the same hard drive layout and have Windows installed into the same directory.

Pavel
26 Apr 2004 5:41 AM
#
I have the same problem with the Reg/seeker in the folder. What do I do?

john
28 Apr 2004 10:27 AM
#
i have the same problem. a virus in system volume info file. i cant gain acces to the file and cant get ownership of the file. please tell me how to take ownership. i read on this page: "" turn off "Hide protected operating system files" and turn on "Show hidden files and folders". Then right-click, Properties, Security, Advanced, Owner, and there you can take ownership. ""
HOW DO I DO THIS? please help me someone.....

Raymond Chen
28 Apr 2004 10:32 AM
#
From the Owner page there is a button called "Take ownership". Or just delete all your System Restore points and that should wipe it out. (System Restore can't tell what's a virus and what isn't so it just backs up everything. What you've found is the backup.)

But this is all something the virus checker programs are supposed to be doing automatically. It is rude of them to tell you about a file you can't do anything about. They should do it for you.

Reirei
28 Apr 2004 7:06 PM
#
But what is your system volume information is infected by virus? and you cant even do system restore because it's infected? that's what's happening to me. horrible i know. does anyone have any idea how to fix it?

Reirei
28 Apr 2004 7:13 PM
#
sorry, i just went over what you guys are talking about and realized that you guys are talking about the same thing im talking. sorry for not paying attention! and i have a question: where is the Owner page? how can i find it? the AVG scaner i have tells me that i have a virus calls PSW.bispy.B but when i run the AVG scaner it's unable to detect the virus although it's tell me that i have one. even norton anti-virus isnt' able to detect that virus! I really need help now...my computer is in a terrible shape...please help.

Raymond Chen
28 Apr 2004 11:02 PM
#
Sorry, the way to change the owner is to click on the new owner in the list and then click "Apply".

rjssr
6 May 2004 1:35 PM
#
Raymond:

I have the same issue as Reirei. Your last post to Reirei was confusing. She asked where is the "owner" page located? You answered with something about changing owners?

Please give a step by step procedure to access the SVI folder.

Thanks.

Raymond Chen
6 May 2004 1:43 PM
#
Rightclick, Properties.

From the Properties dialog, select the Security tab.

At the bottom of the Security page, click Advanced.

On the Advanced dialog, select the Owner tab. (Comes after Auditing.)

Under "Change owner to" click "Administrators".

Click OK.

I didn't mean for this entry to turn into "How to take ownership of a file". That's not my area. I'm just going on principles here.

rjssr
6 May 2004 2:34 PM
#
My fault, I should have been even more clearer.

I meant to include, how do we locate the SVI folder?

Thanks.

Raymond Chen
6 May 2004 2:45 PM
#
I'm going to stop giving support at this point since that wasn't the point of my entry. My purpose was to describe what's in it, not give people instructions on how to mess with it.

rjssr
6 May 2004 4:48 PM
#
Believe me, we are NOT trying to mess with anything. What we are attempting to do is clear out the #^$&$* that caused our systems t go haywire. Trust me when I say, we all hoped that our AV programs would do it, but that is NOT happening.

All your assistance has been appreciated, please continue.

Raymond Chen
6 May 2004 4:49 PM
#
If I keep going then the questions will keep coming. I'm just going to stop now.

R9 Handa
9 May 2004 6:07 PM
#
Restart windows on security mode in order to access the security tab

whiz_kid
11 May 2004 4:32 PM
#
How would you get into security mode?

AlanF
12 May 2004 6:15 AM
#

If you do a Google search on "system volume information" folder access, here's the very first result:

http://support.microsoft.com/default.aspx?kbid=309531

This shows how to gain access to the svi folder.

Also, if the virus or worm is only showing up in the svi folder, it's not running on the system; however, I wouldn't recommend doing a system restore to that point.

Right now, I'm using AVG and it's telling me many times a day about Bugbear in my svi folder. I know the Bugbear there was never run on my system, it comes from being in a quarantine file, but it's still quite annoying to have it keep popping up.

Now that I'm better informed, I'm going to remove all the old restore points when I get home, and I fully expect my AVG annoyance to go away.

Jamie
14 May 2004 3:44 PM
#

I found that to get access to the SVI file I went to the SVI folder, right clicked, properties,sharing tab. Then turned on network sharing/security. Then I was able to get into the SVI directory where instead of just the 1 virus in one of the restore point files I'm up to 5 and still scanning. I could have turned off or deleted the previous restore points but I wanted to see how many virus' had been archived with the restore points. I must agree that the anti-virus companies should be making their software go in and get these files since they, well at least AVG, would keep telling me , by way of popups, that I had a virus in there but when I scanned my system it didn't even see it.

ib
16 May 2004 4:44 AM
#

hey... i had the same problem... i got hit with the virus BKDR_HACDEF.73B...then deleted hxdefdrv.sys... now i cant restore my pc... know anywhere i could get the hxdefdrv.sys file?... please....

Raymond Chen
7 Jun 2004 10:22 AM
#

Comments on this article have been closed.

余啊雷
19 Apr 2005 9:03 AM
#

The arms race between hiding and showing.