System Volume Information

From Lunarsoft Wiki

System Volume Information (SVI) is the name of the data store where Windows XP and Windows Vista keeps its System Restore files and restoration databases. There is one SVI folder per drive being monitored by System Restore. You cannot access the SVI folder by default (except in Windows XP Gold, which was a security flaw and was patched in Service Pack 1), but the steps to grant access to this folder are listed below. You can also use the files in SVI to recover broken hives of your registry, if necessary.

Contents

If you were planning on performing a repair install, **don't**. Initiating a repair install may delete all of your restore points, making manual roll-back impossible. A repair install *almost never* fixes registry hive problems.

Also, disabling System Restore is not recommended. If you must, at least replace it with ERUNT (http://www.larshederer.homepage.t-online.de/erunt/) and allow it to perform automatic hive backups.

It appears that System Restore works a different way in Vista, and there may not be an easy way to copy individual hives out of System Volume Information. (DjLizard's note: I have not yet looked into this.) For the time being, all information here is in reference to Windows XP.

There are also several new registry mount points, including COMPONENTS, the boot configuration database (BCD), Machine SMI Schema, and possibly others depending on your system configuration.

Registry recovery

System Restore not only saves copies of critical system files, it also performs automated registry hive backup. You can use the hive snapshots in the SVI folder to replace broken registry hives. In short, **never turn off System Restore**.

Registry hives and their locations

The following is a list of hives from the SVI folder and their corresponding installation locations. The SVI snapshot name is on the left, and the destination location and file name is on the right.

NOTE: **%systemroot%** and **%allusersprofile%** are environment variables that point to important directories on your system. **%systemroot%** points to the Windows installation folder and drive letter. **%systemroot%** is normally **C:\WINDOWS** on most systems. **%allusersprofile%** points to **(drive):\Documents and Settings\All Users\\**. Note the **\\..\\** which indicates that the path is one directory higher than **%allusersprofile%** provides (meaning that **"Documents and Settings\All Users\\..\\"** becomes just **"Documents and Settings\\"**.) I have used **"%allusersprofile%\\..\\"** because there is no environment variable that points to just "Documents and Settings" alone.

Copy the file listed on the left and place it in the location listed on the right, making sure that you rename the file accordingly (i.e., **_REGISTRY_MACHINE_SAM** becomes just **SAM**).

Hive Name	Location
1 _REGISTRY_MACHINE_SAM	%systemroot%\System32\config\SAM
2 _REGISTRY_MACHINE_SECURITY	%systemroot%\System32\config\SECURITY
3 _REGISTRY_MACHINE_SOFTWARE	%systemroot%\System32\config\SOFTWARE
4 _REGISTRY_MACHINE_SYSTEM	%systemroot%\System32\config\SYSTEM
5 _REGISTRY_USER_.DEFAULT	%systemroot%\System32\config\DEFAULT
6 _REGISTRY_USER_NTUSER_S-1-5-18	%systemroot%\System32\Config\systemprofile\NTUSER.DAT
7 _REGISTRY_USER_NTUSER_S-1-5-19	%allusersprofile%\..\LocalService**NTUSER.DAT**
8 _REGISTRY_USER_NTUSER_S-1-5-20	%allusersprofile%\..\NetworkService**NTUSER.DAT**
9 _REGISTRY_USER_NTUSER_S-1-5-21-*	%userprofile%**NTUSER.DAT**
10 _REGISTRY_USER_USRCLASS_S-1-5-19	%allusersprofile%\..\LocalService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
11 _REGISTRY_USER_USRCLASS_S-1-5-20	%allusersprofile%\..\NetworkService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
12 _REGISTRY_USER_USRCLASS_S-1-5-21-*	%userprofile%\Local Settings\Application Data\Microsoft\Windows\**UsrClass.dat**}}

NOTE: In rows 9 and 12 of the above table, the asterisk replaces a group of numbers appended to the filename called the SID, or Security IDentifier. In this case, it is used to identify local users of the system without referencing them by username (which can be changed, and is thus unreliable as an identifier). A SID cannot (normally) be changed. There may be multiple copies of this file with multiple SIDs in a multi-user system.

Hive purposes

- The **SYSTEM** hive stores all of the data that you see in **HKEY_LOCAL_MACHINE\SYSTEM**, including multiple "ControlSet"s (hardware and services profiles and their backups, including Last Known Good), the raw device names for all of the volumes and drives on the system, Windows Product Activation (WPA) data, and more. You can change the "CurrentControlSet" to whichever ControlSet you desire, by modifying the **Default** value (not to be confused with the empty "(Default)" value) in the **Select** key of the **SYSTEM** hive. You can also change (or inspect) the ControlSet that gets used when you invoke *Last Known Good*. Last known good is no good when your SYSTEM hive is corrupt.

- The **SOFTWARE** hive stores all of the data that you see in **HKEY_LOCAL_MACHINE\SOFTWARE**, which is where all global application settings are located. All products/programs that are built into Windows also have settings stored here. This is in contrast to **NTUSER.DAT**, which is the name of a local user's **SOFTWARE** hive (more commonly known as **HKEY_CURRENT_USER**). **HKEY_CURRENT_USER/NTUSER.DAT** contains all environmental settings (desktop wallpaper, colors, and other preferences), overrides to some **HKEY_LOCAL_MACHINE** policies, and all per-user application settings. The **HKEY_CLASSES_ROOT** "hive" is really just a REG_LINK* (http://www.jsifaq.com/SUBM/tip6100/rh6143.htm) to **HKEY_LOCAL_MACHINE\SOFTWARE\Classes**, so **SOFTWARE** is the hive to replace if you are having problems with **HKEY_CLASSES_ROOT**.

- **SAM** contains local user account usernames and passwords. It's mounted as **HKEY_LOCAL_MACHINE\SAM** but with limited permissions (it is **not** an empty key). You would have to add yourself with *Full Control* in order to see the sub-keys that HKLM\SAM contains.

- The **SECURITY** hive has security descriptors for filesystem objects, password policies, and memberships of local groups. The SAM hive needs the SECURITY hive in order to function properly. Because of this, it is highly recommended that registry recovery for these hives be performed in tandem: *always* copy SAM when you copy SECURITY, and vice versa. Additionally, they should both come from the same restore point (see below). FIXME: I do not know where the SECURITY hive is mounted, if at all.

- The **UsrClass.dat** (S-*_CLASSES) files make up the respective portions of the **HKEY_USERS** hive. **"%userprofile%\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat"** (your user account), for instance, makes up the **HKEY_USERS\S-1-5-21-*-*-*-1033_Classes** key (where the asterisks are the unique parts of your SID). The LocalService and NetworkService "accounts" do not typically have their own classes in the registry, but there's a hive for them too, just in case they ever do.

Registry recovery via NTFSDOS Pro or Recovery Console

If one or more of your registry hives are damaged, or you are not able to access System Restore, you can use the Recovery Console feature of the Windows XP installation CD or the popular third-party NTFS read/write driver called NTFSDOS Pro (http://www.winternals.com/Products/AdministratorsPak/Default.aspx#ntfsdosprofessional) (which comes with the Winternals (http://www.winternals.com) Administrator's Pak (http://www.winternals.com/Products/AdministratorsPak)). This wiki will only cover the Recovery Console method. Technicians who have the Administrator's Pak should be able to adapt the following directions to NTFSDOS Pro. Of course, if you're so inclined, you could also use a Linux live CD with NTFS write support, or the Vista boot DVD (which has a regular cmd.exe prompt). Those two are actually the best methods to use.

If you are using NTFSDOS Pro, you will have to replace each instance of `dir` with `dir /a` so that hidden files will show. Recovery Console doesn't have this problem, as it shows all files by default (and in R.C., there are no command-line switches for `dir`.)

If Recovery Console crashes (blue screens, etc) then you'll need to find an alternate method, such as the aforementioned Linux live CD. Recovery Console may blue screen if your SYSTEM or SOFTWARE hives are corrupted in an unusual way (such as a hard drive bad sector).

You could also connect your drive to another machine (via USB or directly as a slave) and use that machine's Windows installation to aid in your copy - but you'll have to look at the bottom of this guide so you can give yourself access to your System Volume Information folder. Don't forget that you need to use the SVI folder on *your* drive, not the host machine's C: drive.

1. Boot your Windows XP installation media. If your hard drive is **not** connected to the primary or secondary built-in IDE channels found on your motherboard (such as tertiary/quaterniary IDE channels, built-in RAID IDE connectors, or SATA) then you **must** press **F6** at the blue screen when setup first initializes so that you can specify a driver for the controller (which must be on a floppy diskette). If Recovery Console is unable to detect your drive, and you do not have a floppy disk with the SATA/IDE controller driver on it, contact your system manufacturer or a local PC technician so you can get a disk.
2. Press **R** at the first prompt to choose Recovery Console.

If you are unable to login to Recovery Console, seek technical assistance. If you can login successfully or you were dropped to a prompt, type the following commands (including quotes) and press **Enter** after each line:

1. `cd "\System Volume Information"`
2. `dir`

If (and only if) you get an **access denied** error while trying to `cd` into System Volume Information, then do the following:

1. `cd "\windows\system32\config"`
2. `ren system system.123`
3. `exit`

(Replace "windows" with the name of your installation folder if "windows" is not correct.) The system will restart. Then go back into Recovery Console and try to `cd "\System Volume Information"` and continue this guide from there. If you had to perform this step in order to get into System Volume Information, then remember to grab a copy of the SYSTEM hive when you get to the bottom of this guide (`copy _REGISTRY_MACHINE_SYSTEM \windows\system32\config\SYSTEM`)

Hopefully, you will see a folder with a large name of the form: **_restore{MANY-NUMBERS-AND-LETTERS-HERE}**. If there is more than one **_restore{}** folder, you may need to return to this step to choose a different one later in this procedure. You will need to type out all of the numbers and letters, exactly as they appear, in the following command:

1. `cd _restore{YOUR-NUMBERS-AND-LETTERS-HERE}`
2. `dir`

NOTE: the characters around the numbers/letters are curly braces (**Shift+[** and **Shift+]**).

If your System Restore points are intact, you will see one or more folders with the name **RPx**, where **x** is a number representing a restore point ID. Choose the second-to-last restore point ID, because in most cases, the very last restore point folder usually contains a copy of the corrupted registry hive we are trying to replace.

If this entire procedure does not solve your registry corruption issue, start this procedure again and choose a different **RPx** or **_restore{}** folder. If you know what date your registry issue(s) started, you can choose an appropriate **RPx** folder based on the date listed next to each folder.

If your second-to-last restore point folder is **RP126**, type:

1. `cd RP126`
2. `cd snapshot`
3. `dir`

After you type **dir**, you will see a list of filenames similar to those listed above (such as "_REGISTRY_MACHINE_SYSTEM", and so forth). If this folder is empty or the hive you want to copy is missing, go back two directories, get a new directory listing, and choose a new **RPx** folder:

1. `cd ..`
2. `cd ..`
3. `dir`

Continue this process until you have located a folder which contains the copies of the registry. If you get lost, you can start at the beginning of this procedure by typing:

1. `cd "\System Volume Information"`

If all is well and you have found the restore point you wish to use, now you will be able to copy the appropriate hive. Here are a few examples of what hives to copy and why:

If you have recently installed new hardware or a hardware driver and now your system is unbootable or unstable, disconnect the hardware from your system and replace the SYSTEM hive by typing the following command:

1. `copy _REGISTRY_MACHINE_SYSTEM \windows\system32\config\SYSTEM`

(You will also need to copy this hive if you had to rename your current SYSTEM hive in order to get into the System Volume Information folder at the beginning of this guide.)

If your system was working fine but one or more user accounts are no longer listed at the Welcome Screen, copy the SECURITY and SAM hives:

1. `copy _REGISTRY_MACHINE_SAM \windows\system32\config\SAM`
2. `copy _REGISTRY_MACHINE_SECURITY \windows\system32\config\SECURITY`

If you installed a new program and want all of its changes removed from your registry, copy the SOFTWARE hive:

1. `copy _REGISTRY_MACHINE_SOFTWARE \windows\system32\config\SOFTWARE`

NOTE: Replacing any of your registry hives will revert your system to the time and date that the System Restore point was created. Additionally, the amount of System Restore points listed when using the actual System Restore wizard inside of Windows will not match what you find here. Fortunately, you have access to many more copies of the registry than the System Restore interface allows you to see.

To exit Recovery Console once you are done copying one or more hives, type **exit**. Your system will restart. Be sure to remove any CD-ROMs and floppy disks before your computer has a chance to attempt to boot from them. If Windows is still not working properly, follow the procedure again, but choose an **RPx** folder with a lower number than the one you just used. Repeat this process until your system is working again. If you are unable to get your system to work again and you have run out of restore point IDs, it is time to backup your data and reinstall Windows.

Accessing System Volume Information within Windows

Windows XP Home

In Windows XP Home, you cannot disable "simple file sharing", and thus, can't view the **Security** tab which allows you to modify NTFS permissions on files and folders. To work around this limitation:

1. Boot into Safe Mode by tapping the F8 key during bootup, just before the Windows XP splash screen appears, and choose **Safe Mode**.
2. Once logged in under Safe Mode, open **My Computer**, click on **Tools**, **Folder Options**, then the **View** tab. Uncheck both **Show hidden files and folders** and **Hide protected operating system files** if these items are checked.
3. Double click on the drive that is being monitored by System Restore (by default this is your system drive, which is usually **C:**), right click on the **System Volume Information** folder, and choose **Sharing and Security**. Select the **Security** tab.
4. Under **Groups or user names** you may notice that the only entry is SYSTEM. To give yourself permission to view the contents of this folder, click **Add** and type in your user name in the **Enter the object names to select** text area.
5. Reboot as normal. You will now have access to System Volume Information.

Windows XP Professional

The steps to access the System Volume Information folder are similar to those in Windows XP Home, however you do not have to boot into Safe Mode at all.

1. Open **My Computer**, click on **Tools**, **Folder Options**, then the **View** tab. Uncheck both **Show hidden files and folders** and **Hide protected operating system files** if they are checked. Also uncheck **Use simple file sharing** if it is checked, because simple file sharing prevents access to the Security tab.
2. Right click on the System Volume Information folder, choose **Sharing and security**, and then select the **Security** tab when the dialog appears.
3. Under **Groups or user names** you may notice that the only entry is SYSTEM. To give yourself permission to view the contents of this folder, click **Add** and type in your user name in the **Enter the object names to select** text area. You will now have access to System Volume Information.

Alternative method

Right-click on the Desktop, and choose New > Shortcut. Enter the location: "X:\System Volume Information_restore{YOUR-NUMBERS-AND-LETTERS-HERE}" (without quotation marks) where X: is the drive letter containing the SVI you want to examine, and "{YOUR-NUMBERS-AND-LETTERS-HERE}" is the

CLSID of the repository you want to examine. Obviously, you'd have to already know where yours is.

See also

- MSKB 309531 (http://support.microsoft.com/?kbid=309531) - Gaining access to the System Volume Information folder
- MSKB 307545 (http://support.microsoft.com/?kbid=307545) - Recovering from registry corruption (this is a destructive method)

Retrieved from "http://wiki.lunarsoft.net/index.php?title=System_Volume_Information&oldid=1151"
Category: Templates