I.I.S. “Benvenuto Cellini”

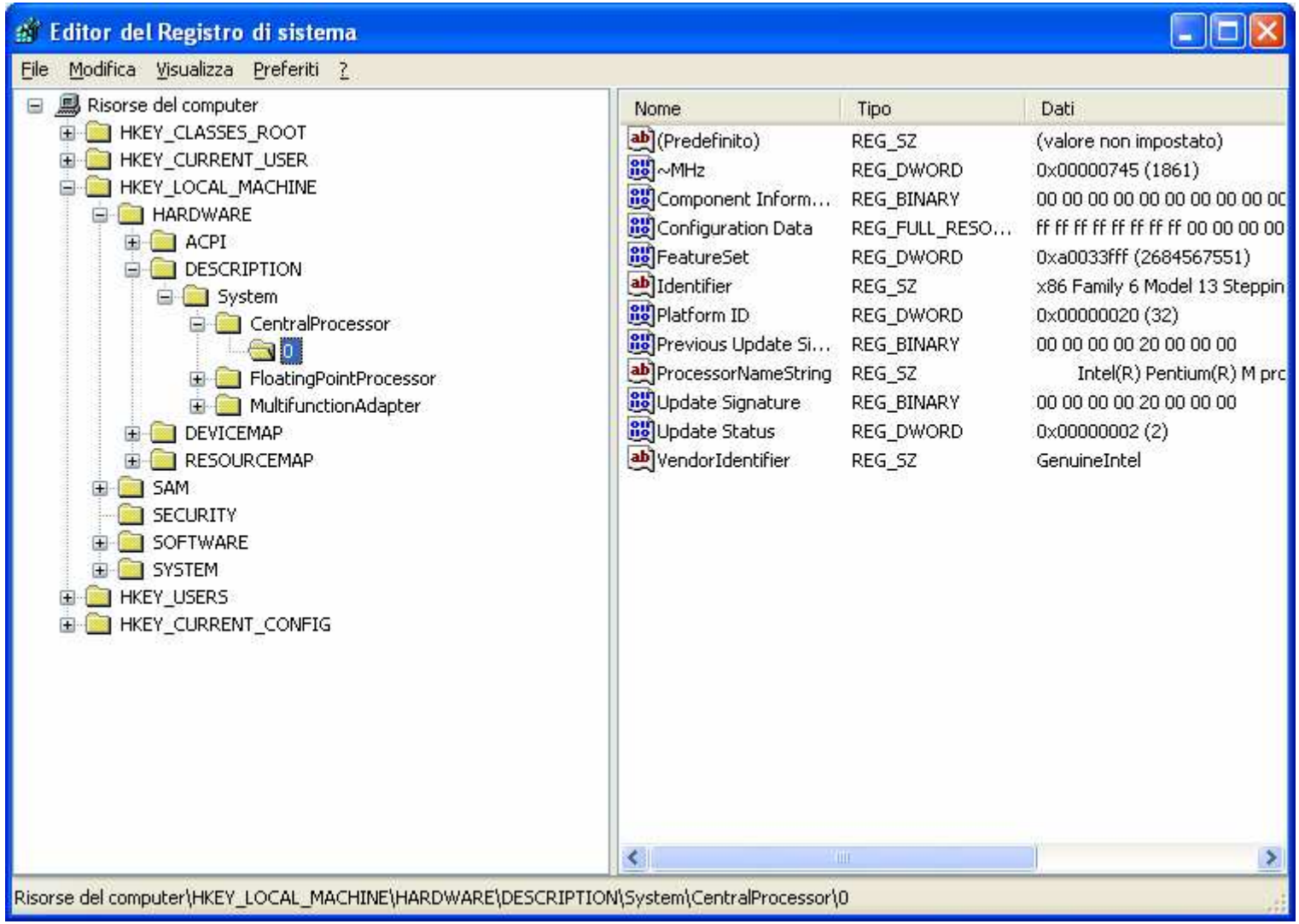
Corso di formazione tecnica

Il Registro di Sistema

Prof. Alessandro Pinto

v.2009

Cosa è il registro di sistema?



Cosa è il registro di sistema?

Il registro di sistema è un *database* dove sono archiviate le informazioni di configurazione del computer relative a:

- Hardware e driver di periferica
- Applicazioni installate
- impostazione dei protocolli e dei dispositivi di rete
- Utenti

Buona parte delle informazioni memorizzate nel registro corrispondono ad impostazioni configurabili tramite l'interfaccia utente di Windows (Pannello di Controllo, Gestione Computer, Strumenti di Amministrazione).

Si consiglia di utilizzare l'interfaccia utente di Windows anziché eseguire le modifiche direttamente mediante l'editor del Registro di sistema.
In alcuni casi la modifica manuale del Registro di sistema costituisce tuttavia il metodo migliore per risolvere un eventuale malfunzionamento.

L'errata modifica del Registro di sistema tramite l'editor o un altro metodo può causare seri problemi, che potrebbero richiedere la reinstallazione del sistema operativo. La modifica del Registro di sistema è a rischio e pericolo dell'utente.

Un po’ di storia…

DOS

Le impostazioni di sistema sono conservate nei file CONFIG.SYS e AUTOEXEC.BAT

Le singole applicazioni possono inoltre fare riferimento a file di configurazione specifici che accompagnano i file eseguibili (tipicamente .CFG o .INI). Non c’è uno standard specifico.

Windows 3.1

Per la prima volta si parla di registro di sistema: si tratta di un singolo file, REG.DAT, il cui compito principale è immagazzinare le informazioni relative agli oggetti OLE

Gli altri dati di configurazione sono memorizzati in file di testo con estensione .INI.

Di particolare rilievo:

SYSTEM.INI
contiene la configurazione del sistema in relazione al hardware impiegato

WIN.INI
contiene le personalizzazioni del sistema secondo le necessità dell’utente
(font dei caratteri, lingua, sfondo del desktop, screensaver, tipi di file associati…)

Formato dei file .INI

L'elemento base è il ***parametro***. Ogni parametro è costituito da una coppia nome/valore separate dal simbolo '=': **nomechiave=valore**

I parametri possono essere raggruppati in ***sezioni***. La dichiarazione di inizio sezione consiste nel nome della sezione racchiuso tra parentesi quadre (es: [drivers]).

Non è prevista una dichiarazione di fine sezione.

Le sezioni non sono nidificate: il file è un semplice elenco di parametri.

Esempio

```
[drivers]
wave=mmdrv.dll
timer=timer.drv

[mci]
[driver32]
[386enh]
woafont=app850.FON
EGA80WOA.FON=EGA80850.FON
EGA40WOA.FON=EGA40850.FON
CGA80WOA.FON=CGA80850.FON
CGA40WOA.FON=CGA40850.FON
```

La dimensione massima valida di un file REG.DAT o .INI è di **64KB**. In alcuni casi, tuttavia si problemi verificano quando questi file sono maggiori di **32 KB**. (http://support.microsoft.com/kb/78346)

Windows 95 e NT

Le informazioni conservate nel REG.DAT e nei file *.INI vengono unificate nel Registro di Sistema (Windows Registry)

Vantaggi:

• Centralizzazione delle informazioni

• Migliore organizzazione grazie alla gerarchia

• Possibilità di gestire strutture più complesse di dati

• Minor vincoli sulle dimensioni

N.B. che nella cartella di installazione di windows si continuano a trovare alcuni file .ini: sono mantenuti per compatibilità con vecchie applicazioni che possono richiederlo

.

Chi usa il registro?

Installazione

L’installazione di una applicazione, o l’esecuzione del setup di Windows, aggiunge dati di configurazione al Registro di sistema.

Rilevazione modifiche hardware

Ogni volta che il p.c. viene avviato, vengono aggiornate le informazioni relative all’hardware della macchina. (Es. l’enumerazione delle periferiche)

Kernel

Legge il registro nella fase di avvio determinando quali driver caricare (e in che ordine)

Driver di periferica

Leggono e scrivono nel registro i parametri di configurazione (es. risorse impiegate, IRQ, DMA). Il funzionamento è analogo alla voce “DEVICE=“ nel config.sys

Strumenti di amministrazione

Le impostazioni da Pannello di Controllo e da Strumenti di Amministrazione agiscono sui dati memorizzati nel Registro di sistema

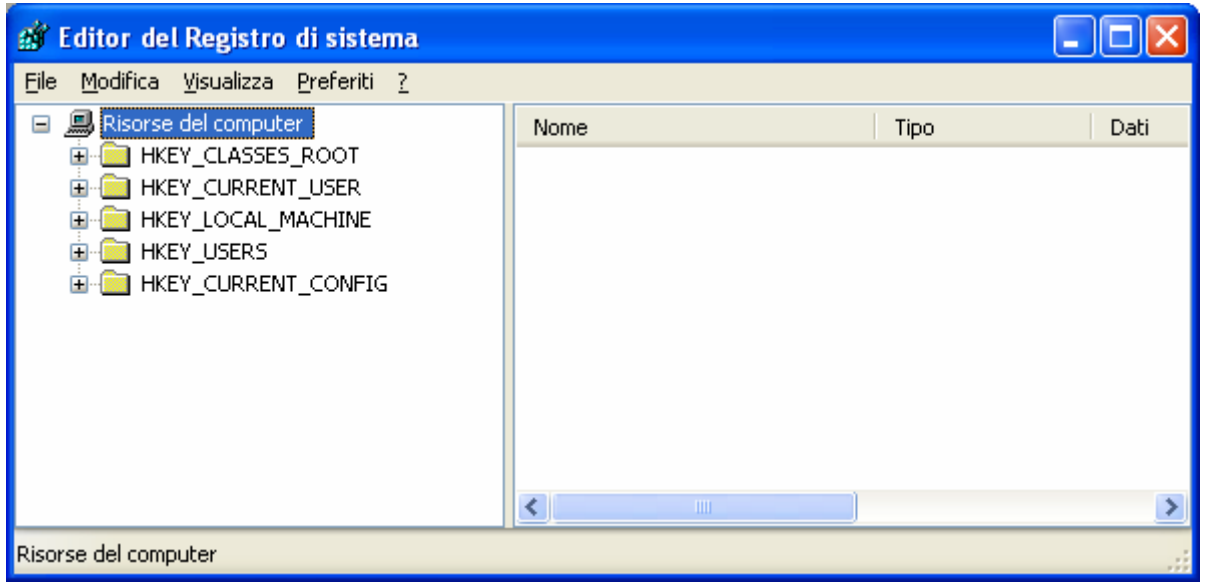
Strumenti per operare sul Registro di Sistema

Lo strumento principale per gestire il Registro di Sistema è il Microsoft Registry Editor REGEDIT.EXE

In ambiente NT esiste un secondo strumento, REGEDT32.EXE..
Questo supporta certe caratteristiche specifiche del registro di NT (es. le impostazioni dei permessi sulle chiavi) che non sono supportate da REGEDIT.EXE.
In NT/2k è pertanto sconsigliato l'uso di regedit per manipolare il registro, o per lo meno, va limitato alla sola consultazione senza non impiegarlo per eseguire modifiche.

La versione di REGEDIT inclusa in WinXP invece supporta pienamente le funzioni del registro e può essere avviata dalla riga di comando digitando sia regedit che regedt32.

Architettura del registro



Il registro è organizzato gerarchicamente con una struttura ad albero (analogia con il file system)

Ogni “cartella” visualizzata nell’editor (regedit.exe o regedt32.exe) è detta *chiave* e può contenere sia altre chiavi (sottochiavi) sia *valori*

Un valore rappresenta l’elemento di livello più basso lungo uno specifico ramo dell’albero (Corrisponde al *parametro* del file .ini)

Una chiave contiene sempre almeno un valore con il nome *default (predefinito)*

In analogia al filesystem, una qualsiasi chiave (o valore) può essere identificata dal percorso (es. HKEY_CURRENT_USER\RemoteAccess\Addresses.)

Top level keys

Il registro è diviso in cinque sezioni principali (sottoalberi) che costituiscono le *root keys* o top *level keys*.

Il nome di queste chiavi inizia con il prefisso H(handle)KEY, seguito dal nome dell'area specifica:

- **HKEY_CLASSES_ROOT (HKCR)**
- **HKEY_CURRENT_USER (HKCU)**
- **HKEY_LOCAL_MACHINE (HKLM)**
- **HKEY_USERS (HKU)**
- **HKEY_CURRENT_CONFIG (HKCC)**

Albero e alias

Tra le cinque sezioni elencate, in realtà tre sono *alias* di altre parti dell'albero.

HKEY_CLASSES_ROOT = HKLM\Software\Classes & HKCU\Software\Classes
HKEY_CURRENT_USER = HKEY_USERS\<Valore SID>
HKEY_CURRENT_CONFIG = HKLM\System\CurrentControlSet\HardwareProfile\Current

Solo due sottoalberi (HKLM e HKU) sono "reali" ovvero si appoggiano su file fisici

Un alias è una vista diversa della medesima informazione. (Non è una copia!)

Una modifica su un valore di un alias si riflette immediatamente sul dato originale (e viceversa).

Gli alias esistono solo mentre windows è in esecuzione.

(HKEY_CURRENT_USER esiste se l'utente ha fatto accesso al sistema)

I file del registro

Sebbene il registro sia visto come una entità unica, la maggior parte di esso si trova distribuita su più di un file fisico.

Windows 9x:

-SYSTEM.DAT informazioni relative alla macchina

-USER.DAT informazioni relative all'utente

Di norma sono contenuti nella cartella Windows

Windows NT/2k/XP

Il registro si trova in una serie di file binari, che prendono il nome di *hive* ("alveare"), localizzati nelle cartelle:

1) **%SystemRoot%\System32\config**

2) **%SystemDrive%\Documents and Settings\<nomeutente>**

3) **%SystemDrive%\Documents and Settings\<nomeutente>\Impostazioni locali\Dati applicazioni\Microsoft\Windows**

N.B. il nome delle cartelle dipende dalla localizzazione del S.O.

Ramo dell'albero	Nome file hive	Salvataggio operazioni	Cartella
HKLM\SAM	SAM	SAM.LOG	1
HKLM\SECURITY	SECURITY	SECURITY.LOG	1
HKLM\SOFTWARE	software	software.LOG	1
HKLM\SYSTEM	SYSTEM	SYSTEM.LOG	1
HKU\.DEFAULT	default	default.LOG	1
HKU\<SID>	NTUSER.DAT	NtUser.dat.log	2
HKU\<SID>_Classes	UsrClass.dat	UsrClass.dat.LOG	3

I file .LOG sono file temporanei nel quale vengono registrate le variazioni del registro.

Le modifiche del registro sono scritte prima nel file .log, successivamente nel hive reale.

Quando l'operazione è terminata il file log è resettato.

Se avviene un crash di sistema durante la scrittura di un hive, le modifiche conservate nel log vengono applicate al boot successivo.

N.B. quando il sistema operativo è in esecuzione questi file sono mantenuti aperti e bloccati dal sistema operativo stesso. Non è pertanto possibile operarvi direttamente (ad esempio per fare un backup)

→ Appositi strumenti di backup, oppure,

→ Disco di avvio in ambiente XP (Es. BartPE)

Nel caso il sistema operativo non sia in grado di caricare uno o più dei file hive, abbiamo un errore critico che impedisce l'avvio della macchina.

Impossibile avviare Windows XP. Il seguente file manca o è danneggiato: \WINDOWS\SYSTEM32\CONFIG\SYSTEM

Impossibile avviare Windows XP. Il seguente file manca o è danneggiato: \WINDOWS\SYSTEM32\CONFIG\SOFTWARE

Stop: c0000218 {Errore nel file del Registro di sistema} Il Registro di sistema non ha potuto caricare il file hive: \SystemRoot\System32\Config\SOFTWARE oppure il suo registro o la sua copia.

Errore di sistema: Lsass.exe Durante l'aggiornamento di una password, il verificarsi di questo stato indica che il valore fornito per la password corrente non è esatto.

E' possibile, come ultima risorsa, fare riferimento alle copie di salvataggio del registro che vengono archiviate in:

-%SystemRoot%\repair

-%SystemDrive%\System Volume Information_restore{GUID}\RP*x*\Snapshot

Per le modalità di ripristino tramite queste copie di salvataggio, si rimanda alla nota tecnica Microsoft specifica: **http://support.microsoft.com/kb/307545**

La funzione dei cinque rami principali

HKEY_LOCAL_MACHINE

E’ specifico della macchina (come implica il nome).
Contiene le informazioni sull’hardware attualmente installato nella macchina e sui programmi e sistemi in esecuzione quando non legati ad un utente specifico.

HKLM\Hardware

Viene creato al primo avvio e contiene le informazioni dinamiche relative alla configurazione hardware del sistema (Es. tipo di processore, Hardware Abstraction Layer caricato, interrupt in uso dalle periferiche, enumerazione dei dispositivi…)

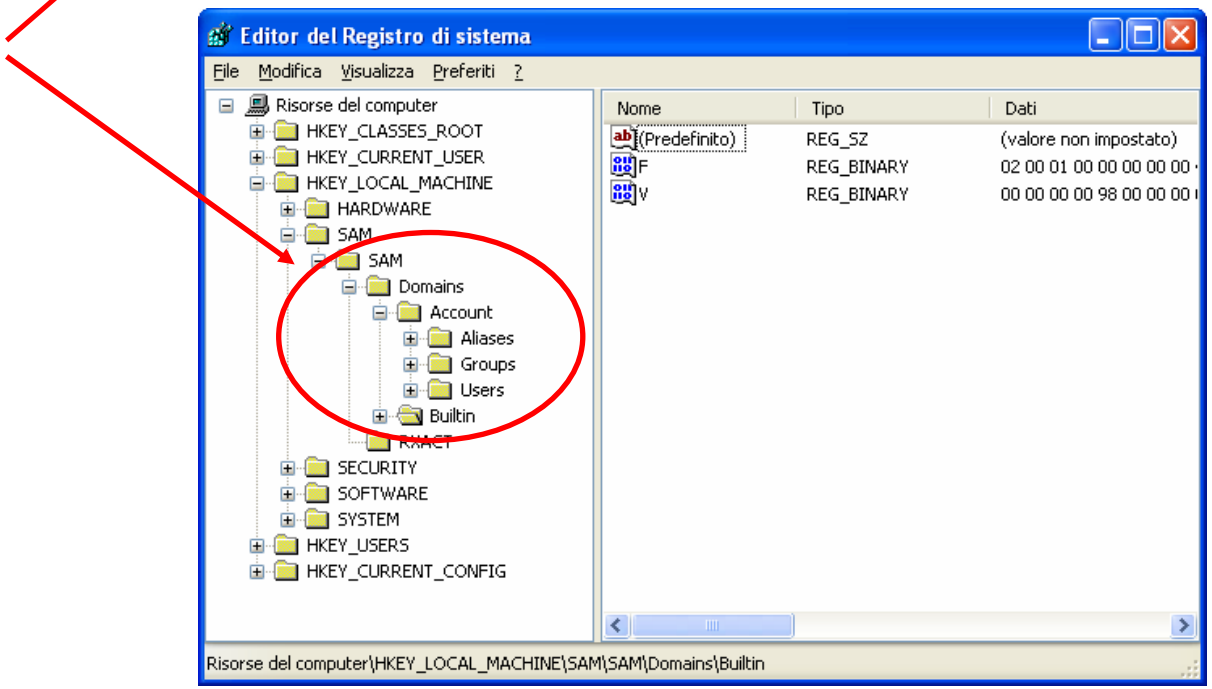
In linea di massima sono da considerarsi valori volatili: una eventuale modifica viene resettata al successivo riavvio.

HKLM\SAM e HKLM\Security

Nelle macchine non connesse ad un dominio contengono le informazioni relative alla gestione degli accessi.

Normalmente, anche con privilegi di amministratore, non è possibile visualizzare il contenuto di queste chiavi. L’accesso è consentito solo all’utente **system**

Editor di registro eseguito come Amministratore



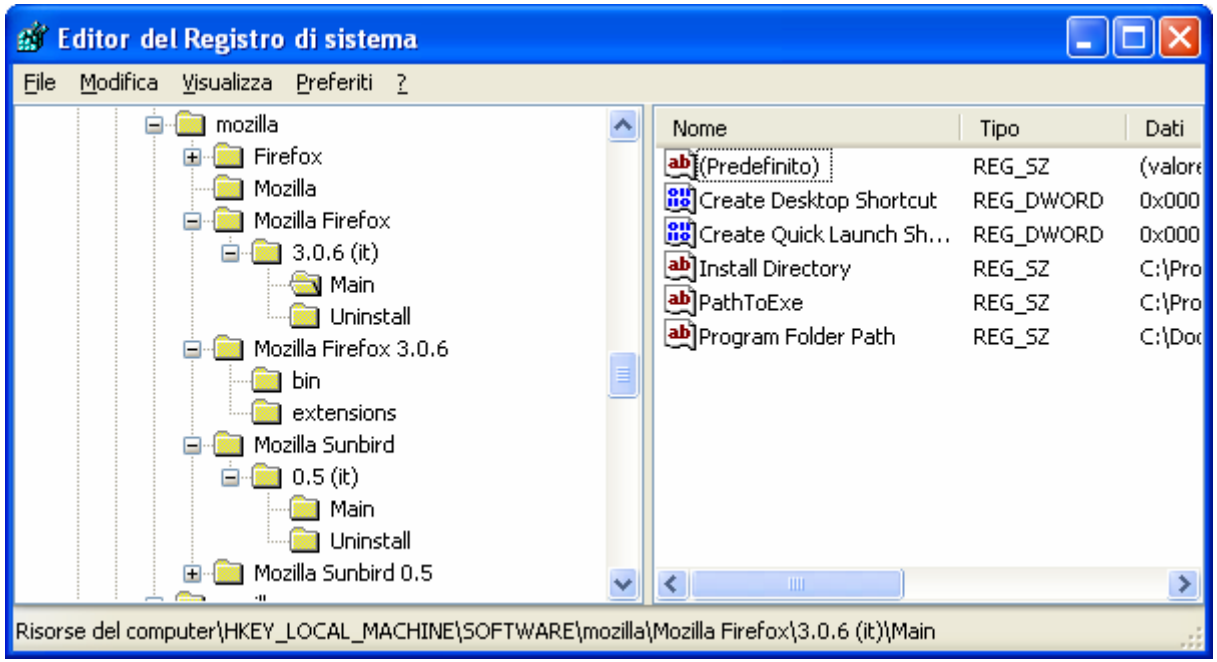
Editor di registro eseguito come System

(psexec –i –s regedit)

HKLM\Software

In questa chiave tutte le applicazioni Microsoft e la maggior parte delle applicazioni di terze parti, scrivono le loro informazioni di configurazione (percorsi, opzioni, personalizzazioni…).

In linea di principio ogni produttore di applicazioni dovrebbe creare una chiave (tipicamente con il nome dell'azienda) e all'interno di questa le sottochiavi e valori relativi alle proprie applicazioni. (Es. HKML\Software\mozilla\mozilla firefox\3.0.6(it)…..)



Inoltre contiene la chiave Classes che è sorgente per l'alias HKEY_CLASSES_ROOT

HKLM\System

E’ la porzione di registro che conserva la configurazione del sistema operativo stesso.

In particolare, in HKLM\System\CurrentControlSet\Services, che troviamo la definizione dei *servizi* e *dispositivi* NT:

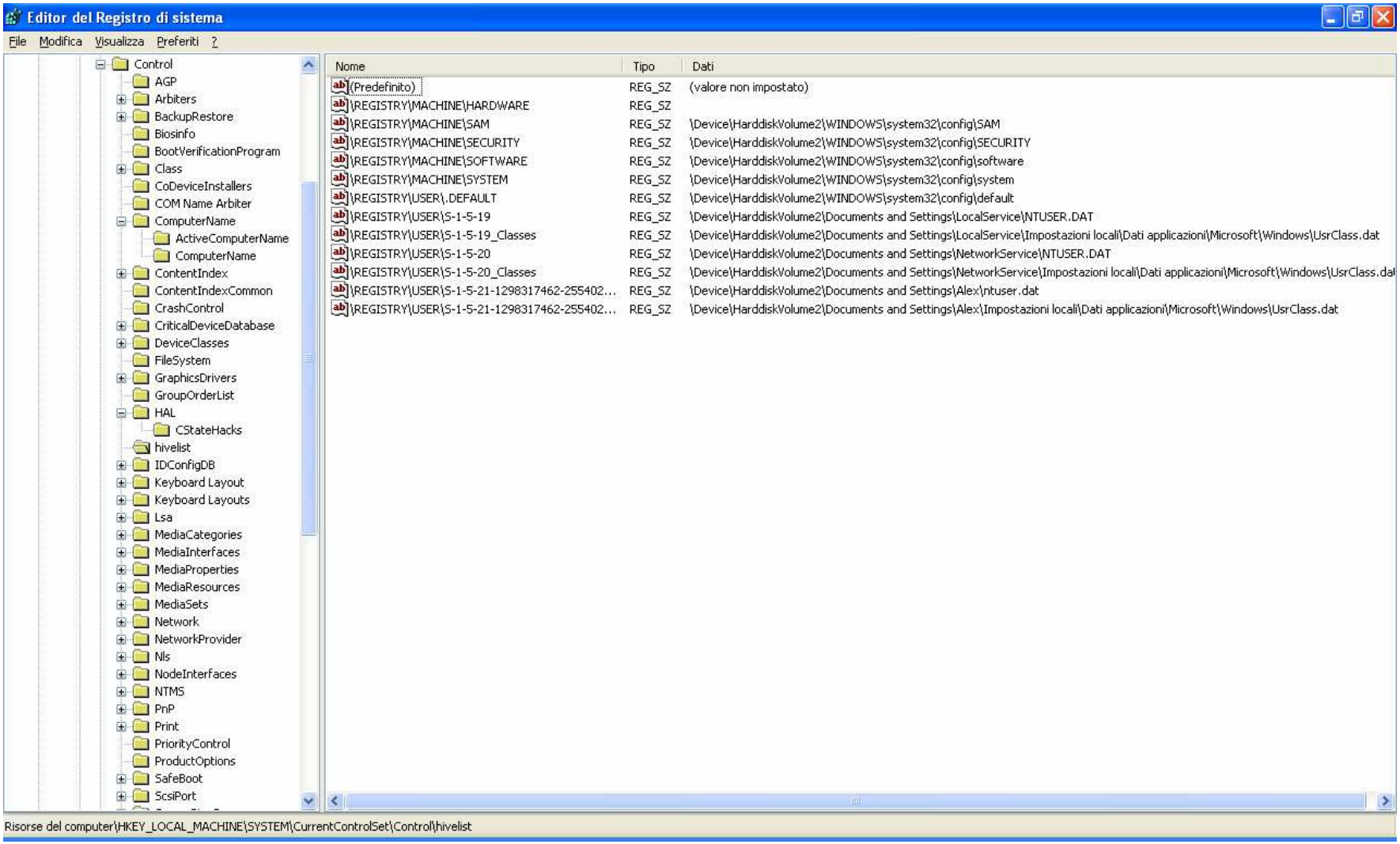
Altre sottochiavi di sistema particolarmente significative:

HKLM\System\CurrentControlSet\Control (configurazione del S.O., vedi esempio la hivelist)

HKLM\System\CurrentControlSet\Control\CriticalDeviceDatabase (elenco dei driver dei dispositivi indispensabili per l’avvio del S.O. Es il controller del disco)

HKLM\System\CurrentControlSet\Enum (elenco dei dispositivi PnP trovati al boot)

Entrando nel safe menù premendo F8 al boot, è possibile di avviare la macchina con l’ultima configurazione valida. Questo significa l’impiego di un CurrentControlSet diverso tra quelli disponibili nel registro. (Vedi anche HKLM\System\Select)


Editor del Registro di sistema
File Modifica Visualizza Preferiti ?
Control
AGP
Arbiters
BackupRestore
Biosinfo
BootVerificationProgram
Class
CoDeviceInstallers
COM Name Arbiter
ComputerName
ActiveComputerName
ComputerName
ContentIndex
ContentIndexCommon
CrashControl
CriticalDeviceDatabase
DeviceClasses
FileSystem
GraphicsDrivers
GroupOrderList
HAL
CStateHacks
hivelist
IDConfigDB
Keyboard Layout
Keyboard Layouts
Lsa
MediaCategories
MediaInterfaces
MediaProperties
MediaResources
MediaSets
Network
NetworkProvider
Nls
NodeInterfaces
NTMS
PnP
Print
PriorityControl
ProductOptions
SafeBoot
ScsiPort
Nome Tipo Dati
(Predefinito) REG_SZ (valore non impostato)
\REGISTRY\MACHINE\HARDWARE REG_SZ
\REGISTRY\MACHINE\SAM REG_SZ \Device\HarddiskVolume2\WINDOWS\system32\config\SAM
\REGISTRY\MACHINE\SECURITY REG_SZ \Device\HarddiskVolume2\WINDOWS\system32\config\SECURITY
\REGISTRY\MACHINE\SOFTWARE REG_SZ \Device\HarddiskVolume2\WINDOWS\system32\config\software
\REGISTRY\MACHINE\SYSTEM REG_SZ \Device\HarddiskVolume2\WINDOWS\system32\config\system
\REGISTRY\USER\.DEFAULT REG_SZ \Device\HarddiskVolume2\WINDOWS\system32\config\default
\REGISTRY\USER\S-1-5-19 REG_SZ \Device\HarddiskVolume2\Documents and Settings\LocalService\NTUSER.DAT
\REGISTRY\USER\S-1-5-19_Classes REG_SZ \Device\HarddiskVolume2\Documents and Settings\LocalService\Impostazioni locali\Dati applicazioni\Microsoft\Windows\UsrClass.dat
\REGISTRY\USER\S-1-5-20 REG_SZ \Device\HarddiskVolume2\Documents and Settings\NetworkService\NTUSER.DAT
\REGISTRY\USER\S-1-5-20_Classes REG_SZ \Device\HarddiskVolume2\Documents and Settings\NetworkService\Impostazioni locali\Dati applicazioni\Microsoft\Windows\UsrClass.dat
\REGISTRY\USER\S-1-5-21-1298317462-255402... REG_SZ \Device\HarddiskVolume2\Documents and Settings\Alex\ntuser.dat
\REGISTRY\USER\S-1-5-21-1298317462-255402... REG_SZ \Device\HarddiskVolume2\Documents and Settings\Alex\Impostazioni locali\Dati applicazioni\Microsoft\Windows\UsrClass.dat
Risorse del computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist

HKEY_USERS

Il numero di sottochiavi contenuto dipende da quanti utenti stanno facendo accesso sulla macchina.

HKU\.Default

La prima sottochiave sicuramente presente è .Default

Viene impiegata come profilo per l'account LocalSystem quando fa accesso come servizio

N.B.che tale chiave non è da intendere invece, in Win2k/XP, relativa al Default User, cioè all'utente per il quale ancora non è stato creato un profilo (non avendo mai fatto accesso alla macchina) come al contrario potrebbe far pensare.
Il profilo del Default User è infatti localizzato in **C:\Document and settings\Default User** come un qualsiasi altro profilo utente.

.Default è inoltre impiegata dal S.O. per impostare l'aspetto del desktop prima che l'utente abbia fatto accesso al sistema. (N.B. che in questo caso per lo sfondo deve essere usato un file .bmp)

HKU\<SID>

Le altre sottochiavi presenti sono relative al profilo utente degli utenti **correnti** sul sistema, sia come accesso interattivo (console) sia come servizio in esecuzione.

Ogni profilo è caricato sotto HKU nella sottochiave corrispondente al SID (Security Identifier) dell'utente.

HKEY_CURRENT_USER

Rappresenta la porzione di registro del profilo utente per l'utente correntemente connesso alla console della macchina. E' in realtà un collegamento a HKU\<SID> per l'utente corrente.

HKEY_CLASSES_ROOT

E' un diretto discendente del REG.DAT di Win3.1

Contiene principalmente le associazioni dei tipi di file e le registrazioni delle classi degli oggetti OLE e COM.

E' ottenuto come merging di due distinti sottoalberi: HKLM\Software\Classes e HKCU\Software\Classes. Questo permette di avere in un unico sottoalbero sia le classi registrate per la macchina che quelle relative all'utente.

Nel merging le chiavi dell'utente sono caricate per prime, successivamente quelle relative alla macchina evitando duplicazioni e conflitti.

N.B. l'installazione di applicazioni non previste nativamente per l'ambiente multiutente win2k/XP può presentare proprio problemi in questa sezione del registro, registrando le classi solo per l'utente che ha eseguito l'installazione che in tal caso non vengono viste dagli altri utenti.

– Il primo gruppo di sottochiavi in HKCR è rappresentato da tutte le estensioni dei tipi di file che sono registrati nel sistema. (Es. se c'è Word installato, troveremo la sottochiave .doc). Per ogni estensione c'è come minimo il riferimento alla definizione di classe associata con il documento.

– Le definizione di classe costituiscono il secondo gruppo di sottochiavi in HKCR. Queste contengono:

- il nome descrittivo del tipo di file come appare in Explorer
- Il puntatore all'icona di default
- Le informazioni necessarie per permettere alle applicazioni di usare il documento come oggetto OLE (se previsto)
- Come maneggiare il documento all'interno della shell di Windows (doppio click del tasto sinistro e/o menù contestuale con il tasto destro)

HKEY_CLASSES_ROOT è aggiornato automaticamente quando un'applicazione è installata o disinstallata, a volte tuttavia può essere necessario intervenire manualmente (ad esempio per ripristinare l'associazione di un tipo di file erroneamente sostituita da una nuova applicazione).

Sebbene questo sia possibile operando sul registro, è preferibile (e più semplice) agire tramite il pannello "Tipi di File" nel menù Opzioni Cartella di Explorer.

Permessi e privilegi di accesso

Come il file system NTFS, ogni chiave di registro e sottochiave ha una Access Control List (ACL) associata.

Ciascuna ACL comprendo un certo numero di voci dette Access Control Entries (ACE)

Una ACE definisce l'utente o il gruppo al quale è consentito l'accesso alla risorsa e quale tipo di accesso (Read, Full Control e Special Access)

N.B. che le ACL del registro NON DIPENDONO dal file system in uso quindi sono attive anche se il S.O. è installato su FAT32

I permessi sono assegnati solo alle chiavi di registro, non si estendono ai valori

Poiché l'accesso a certe chiavi del registro costituisce un operazione privilegiata (es. accedere a SAM, Security, machine policy, user policy), di norma all'utente è impedita la modifica (e in certi casi anche la lettura) delle chiavi più critiche.

N.B. in una tipica installazione domestica questo non viene avvertito poiché l'utente viene automaticamente inserito nel gruppo Administrators.