▶ Nel cuore di Windows

Un Registro per tenere il sistema sotto controllo

Il Registro è un componente chiave, che nasconde in sé molte informazioni critiche per il funzionamento del sistema e delle applicazioni. Prima o poi può capitare anche all'utente qualsiasi di metterci le mani per risolvere un problema o per personalizzare il comportamento di Windows

Molti utenti non hanno mai sentito parlare del *Registry* (o *Registro di sistema*) di Windows. Altri hanno qualche idea più o meno precisa sulla sua funzione e sui contenuti. Sono comunque in pochi a metterci le mani, perché è un compito delicato, riservato in primo luogo a Windows e alle applicazioni. Ma a volte il Registro è l'ultima risorsa per rimediare a una situazione o per modificare un comportamento, visto che è lo strumento centrale per personalizzare Windows. Può accadere ad esempio che cambiate scheda grafica o ne aggiornate il driver, ma che Windows recalcitri trovando nel Registro tracce di precedenti installazioni che lo confondono; conviene allora fare pulizia aggiornando manualmente il Registro. Oppure non gradite il fatto che all'avvio Windows modifichi la disposizione delle icone sul desktop: in questo articolo vi spieghiamo come fargli cambiare abitudini.

Come è nato e si è evoluto il Registro di sistema

Il Registro è un deposito centralizzato di informazioni su tutti gli aspetti del computer: l'hardware, il sistema operativo, il software applicativo e gli utenti. Di solito viene aggiornato da Windows e dalle applicazioni, ma anche l'utente può farlo – con le dovute cautele – utilizzando l'utility *Regedit.exe* di Windows o uno degli altri editor di Registro che si trovano in commercio.

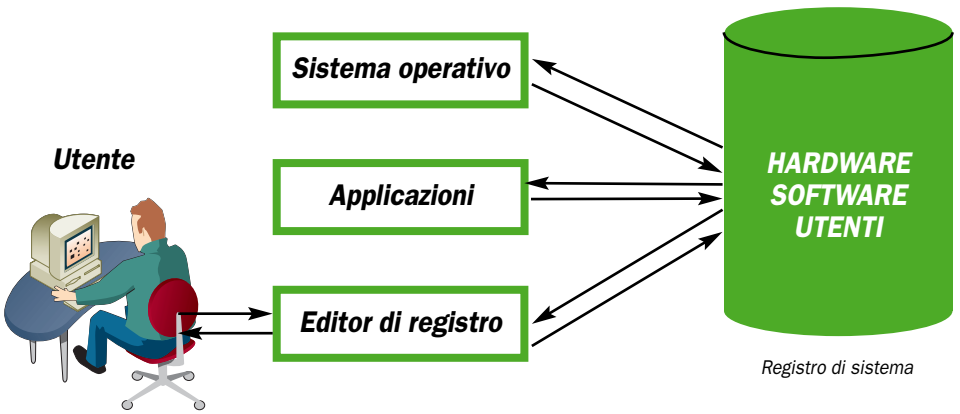
Dato che il Registro contiene praticamente tutte le informazioni sulla configurazione del sistema, è qui che si può intervenire per modificare aspetti dell'interfaccia e comportamenti di default e in generale personalizzare l'uso di Windows secondo le necessità e i gusti degli utenti.

Ai tempi del DOS e di Windows 1.0 i file di configurazione erano *Config.sys* e *Autoexec.bat*. Con Windows 2.0 fecero la loro comparsa *Win.ini* e *System.ini*, dedicati alla configurazione di Windows e del sistema. A quel tempo anche le applicazioni cominciarono a usare i file *.ini*.

Windows 3.0 introdusse nuovi file *.ini* di sistema, come ad esempio *Progman.ini*, *Winfile.ini* e *Control.ini*. La prima forma di Registro apparve in Windows 3.1; era costituita da un unico file *Reg.dat* usato principalmente come catalogo degli oggetti *OLE* (*Object Linking and Embedding*). La maggior parte degli altri dati di configurazione era ancora contenuta nei file *.ini*, sempre più difficili da gestire sia perché numerosi sia per la loro struttura di lunghi file in formato testo. L'attuale Registro ha le sue radici in Windows 95, quando il problema fu risolto introducendo una struttura gerarchica, più adatta a contenere e catalogare una grande massa di dati. Sebbene non sia privo di difetti (struttura complessa, impostazioni oscure, difficoltà di ricerca), il moderno Registro ha portato diversi vantaggi: è costituito da file protetti (essendo file di sistema), nascosti e *di sola lettura*, perciò non modificabili o cancellabili accidentalmente; può essere usato in rete per consultare e aggiornare le configurazioni dei PC e dispone di un editor (Regedit, parte di Windows) che ne presenta una visione gerarchica e ne permette la consultazione e la modifica, anche se non offre spiegazioni sui contenuti.

Sebbene il Registro sia generalmente considerato una singola entità, il suo contenuto è memorizzato fisicamente in più file. In Windows 9x vengono usati *System.dat* e *User.dat*, contenuti solitamente nella directory di Windows e dedicati a informazioni che riguardano rispettivamente il sistema e l'utente. In Windows NT, 2000 e XP il Registro è distribuito su più file, che Microsoft chiama hive per analogia con la struttura a celle degli alveari (in inglese beehive). Gli *hive* sono contenuti per lo più nel ramo *System32\Config* della directory di Windows e sono riconoscibili dai nomi *Default*, *Sam*, *Security* e *System* più i rispettivi file *.log*; gli *hive* di ogni profilo

A COSA SERVE



Il registro di sistema è un deposito centralizzato delle informazioni su tutti gli aspetti del computer: l'hardware, il sistema operativo, il software applicativo e gli utenti. Normalmente viene aggiornato da Windows e dalle applicazioni, ma anche l'utente - con le dovute precauzioni - può modificarlo con un apposito editor.

utente (*Ntuser.dat* e il suo *.log*) sono contenuti nelle corrispondenti sottodirectory di Windows, solitamente *\Documents and Settings\nomeutente*.

Visione gerarchica, ma con ripetizioni

Comunque siano distribuiti fisicamente i dati del Registro, l'apposito editor Regedit ne fornisce una visione gerarchica. Per lanciare l'editor basta digitare *Regedit.exe* al prompt di *Start/Esegui*. La finestra che si apre mostra, nel pannello di sinistra, un albero che ha come radice Risorse del computer e cinque o sei sottoalberi a seconda della versione di Windows (il Registro di Windows 9x ha un sottoalbero in più). I nomi di questi sottoalberi sono detti *chiavi predefinite* perché rappresentano le suddivisioni standard del Registro; i loro nomi iniziano con HKEY: H come handle (maniglia) perché sono i punti di riferimento della struttura e KEY perché sono chiavi di identificazione.

Gli elementi di ogni sottoalbero subito sotto le chiavi predefinite si chiamano *chiavi*. Ogni chiave può avere sotto di sé delle *sottochiavi* e queste, a loro volta, possono includere ulteriori livelli di sottochiavi. Ci sono però delle sovrapposizioni. Il primo sottoalbero, HKEY_CLASSES_ROOT, è nello stesso tempo una chiave predefinita e una sottochiave di HKEY_LOCAL_MACHINE; infatti ne replica una sezione per maggiore comodità di accesso. HKEY_CLASSES_ROOT contiene centinaia tra chiavi e sottochiavi: in parte assomigliano a estensioni di file, altre sono simili a nomi di applicazioni. Le informazioni in HKEY_CLASSES_ROOT permettono ad esempio di eseguire il programma appropriato quando si apre un file in Windows Explorer (*Esplora Risorse*).

Gli altri sottoalberi del Registro

Il secondo sottoalbero è HKEY_CURRENT_USER; come dice il nome, contiene informazioni riguardanti l'utente collegato in modo interattivo (cioè tramite login locale, non via connessione remota). Anche questa chiave predefinita è un *alias*, perché replica, in modo più esplicito e accessibile, informazioni già presenti in uno dei rami del sottoalbero HKEY_USERS. Per esempio la sottochiave HKEY_CURRENT_USER\RemoteAccess\Addresses contiene le informazioni sulle connessioni di rete di tipo telefonico che sono state installate. Così come i file su disco vengono identificati dal loro *path*, iniziando dalla *directory radice*, anche gli elementi del Registro sono identificati dalla successione delle chiavi e sottochiavi, separate da barre rovesciate, partendo da una delle chiavi predefinite. La barra di stato sul fondo della finestra di Regedit mostra il percorso completo della chiave corrente.

La terza chiave predefinita è HKEY_LOCAL_MACHINE, che contiene le informazioni sulla configurazione del computer, valide per tutti gli utenti. Come si nota dagli esempi, a ogni chiave sono associate una o più impostazioni; nel pannello di destra di Regedit si vedono i nomi e i valori delle impostazioni associate alla chiave corrente. Selezionando ad esempio HKEY_LOCAL_MACHNE\Config\0001\Display\Fonts il pannello delle impostazioni elenca nomi e valori delle font di sistema. L'icona di fianco ai nomi indica che si tratta di valori stringa; un altro tipo di dato comune nel Registro è quello binario, come si può vedere nell'esempio riguardante il sottoalbero HKEY_USERS. Questa chiave predefinita, la quarta, dà accesso alle informazioni contenute nel profilo di default e nei profili degli utenti catalogati. Dei sottoalberi visti finora, solo due, HKEY_LOCAL_MACHINE e HKEY_USERS, rappresentano la totalità delle informazioni su configurazione e utenti, mentre gli altri due sono degli alias per una parte delle stesse informazioni. Un alias non è una copia ma un'altra vista, più comoda da usare, sugli stessi dati. Quando si aggiornano i dati di un alias vengono modificati i dati originali e viceversa.

Il quinto sottoalbero del Registro, HKEY_CURRENT_CONFIG, contiene le informazioni sul profilo hardware del computer al suo avvio; serve ad esempio per configurare le impostazioni dei device driver e la risoluzione del monitor. Anche in questo caso le informazioni si basano sui contenuti di HKEY_LOCAL_MACHINE; uno degli esempi mostra che in Windows 98 HKEY_CURRENT_CONFIG è l'alias di uno dei rami Config (i profili hardware) di HKEY_LOCAL_MACHINE.

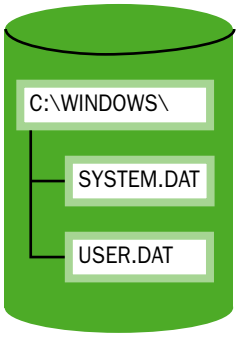
Presente soltanto in Windows 9x, il sottoalbero HKEY_DYN_DATA è una copia residente in memoria di alcune informazioni del Registro da tenere rapidamente accessibili; queste riguardano la configurazione hardware, ad uso del Plug and Play Configuration Manager, e le statistiche di prestazioni dei componenti di rete.

Accesso anche in rete

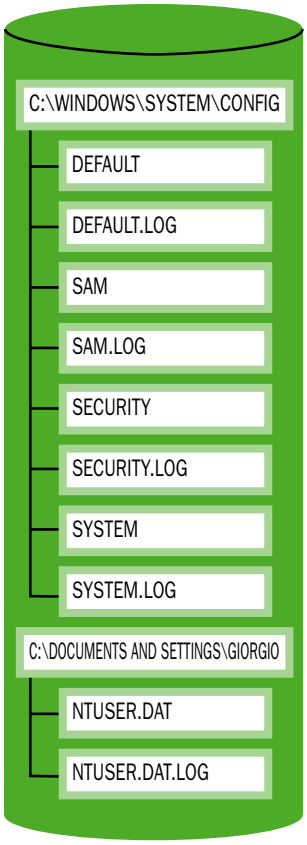
Regedit permette di accedere non soltanto al Registro del computer locale, ma anche ad altri PC sulla rete. L'operazione è diretta, a meno che la macchina locale o remota usi Windows 9x; in tal caso occorre installare i servizi di *Remote Registry* e *Remote Administration* con le opportune impostazioni di sicurezza. Altrimenti basta selezionare *Connetti a Registro di configurazione di rete* nel menu principale di Regedit e specificare il nome di un computer per modificarne il Registro come avviene sul PC locale. Regedit può essere usato per importare ed esportare tutto o parte del Registro oppure per modificarne i contenuti, aggiungendo nuove chiavi e impostazioni, modificando le impostazioni delle chiavi esistenti o eliminando chiavi e impostazioni. Prima di vedere un esempio di personalizzazione del sistema tramite l'editor di Registro, diamo un'occhiata al formato delle informazioni. Gli esempi mostrano che la finestra di Regedit è divisa in due pannelli: quello di sinistra mostra le chiavi e quello di destra mostra i valori delle impostazioni. Per ogni chiave c'è almeno un'impostazione di *Default* o *Predefinita*, a cui non è assegnato un valore. In Windows 9x sono previsti tre tipi di dato, tuttora i più comuni: *numeri bi-* ▷

COME È STRUTTURATO

Sebbene il registro appaia come un'unica struttura gerarchica, fisicamente consiste di file separati: due in Windows 9x e almeno 10 in Windows NT/2K/XP.



I file del Registro in Windows 9X



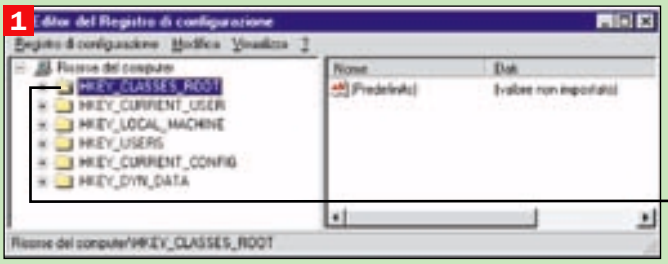
I file del Registro in Windows NT, 2000, XP

▷ *nari*, *numeri binari DWorld* (valori su parola doppia, ovvero 4 byte anziché 2) e *stringhe*. In Windows 2000 e XP i tipi di dato più comuni sono *Reg_Binary* (binario con visualizzazione decimale), *Reg_Dword* (binario su 4 byte), *Reg_Expand_Sz* (stringa di lunghezza variabile), *Reg_Multi_Sz* (stringa multipla), *Reg_Sz* (stringa di lunghezza fissa) e *Reg_Full_Resource_Descriptor* (serie di array nidificati per contenere una lista di risorse). Ma può capitarvi di incontrarne altri, perché il descrittore del tipo di dato è un numero binario di 4 byte, che consente miliardi di valori diversi (la prima metà riservata al sistema, la seconda ai programmi applicativi).

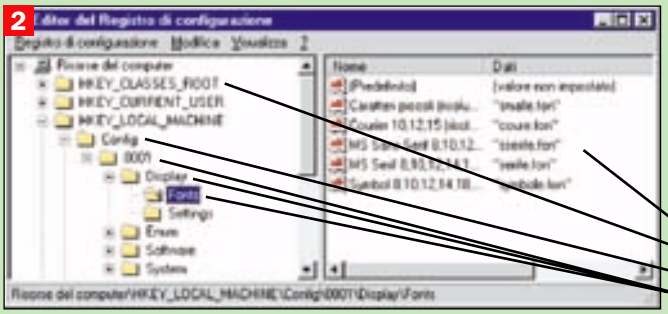
Dopo questa lunga introduzione, siamo pronti per la prima modifica del Registro. È un esempio molto semplice, ma se preferite cautelarvi da possibili errori potete fare prima una copia di backup del Registro tramite la funzione *Esporta* del menu principale di Regedit. La funzione di esportazione produce un file di testo con tutti i dati del Registro, che potete ripristinare con la funzione *Importa*.

Prendendo Windows 98 come terreno di prova, aggiungeremo un'impostazione a una chiave di Registro già esistente; lo scopo di questo intervento è quello di evitare che Windows modifichi la posizione delle icone sul desktop quando viene riavviato. Dopo avere attivato Regedit (tramite *Start\Esegui*), percorriamo il sottoalbero HKEY_CURRENT_USER, scendendo di livello fino a posizionarci sulla chiave HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer. Se è assente un'impostazione *NoSaveSettings*, la aggiungiamo selezionando *Modifica, Nuovo, Valore binario*. Nella finestrella Nuovo valore digitiamo *NoSaveSettings,* quindi selezioniamo *Modifica* e di nuovo *Modifica* nel sottomenu; nella finestra di input digitiamo otto volte 0 (zero) per indicare in esadecimale che i due byte del nuovo valore devono essere a zero. Ora usciamo dal Registro e spostiamo qualche icona del desktop: al successivo riavvio ritroveremo il desktop come l'abbiamo lasciato. ■

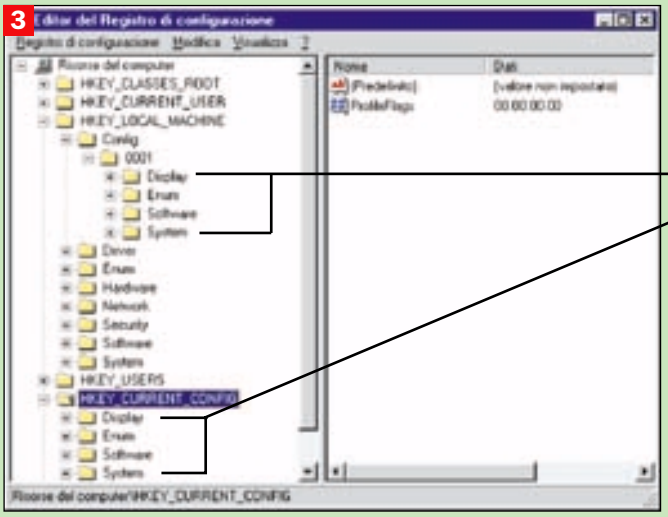
Giorgio Gobbi



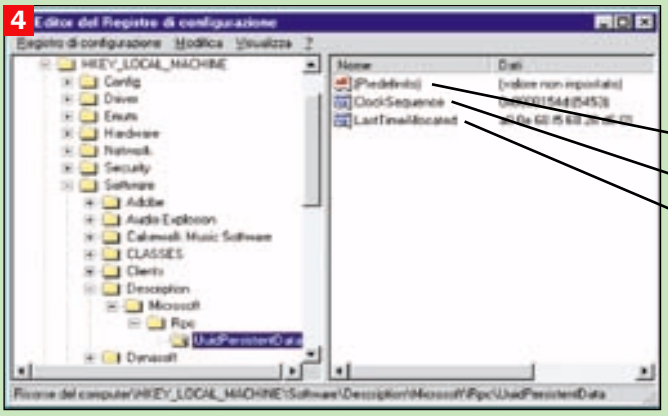
1 Regedit.exe è l'editor del registro di sistema fornito con Windows. Questa è la finestra come appare in Windows 98



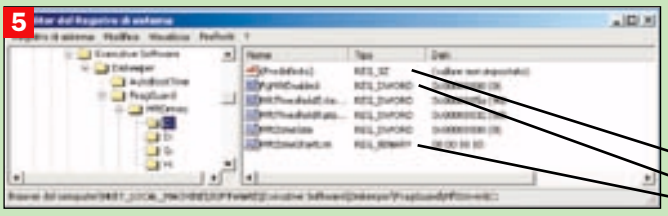
2 Gli elementi del Registro sono identificati da chiavi predefinite (HKEY...), chiavi e sottochiavi. Ogni chiave o sottochiave ha una o più impostazioni caratterizzate da un nome del tipo di dato e dal valore.



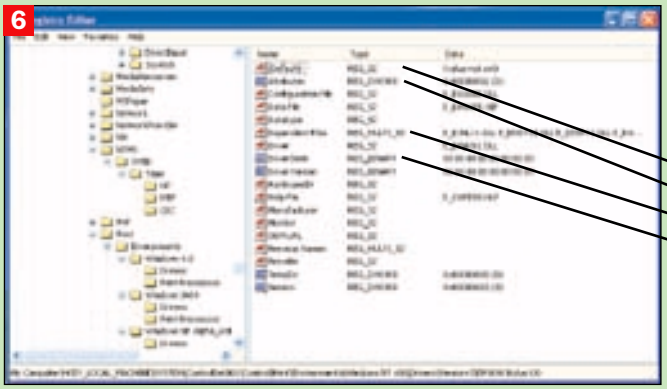
3 Alcuni rami della struttura visualizzata da Regedit sono alias di altri rami, allo scopo di facilitarne l'accesso.



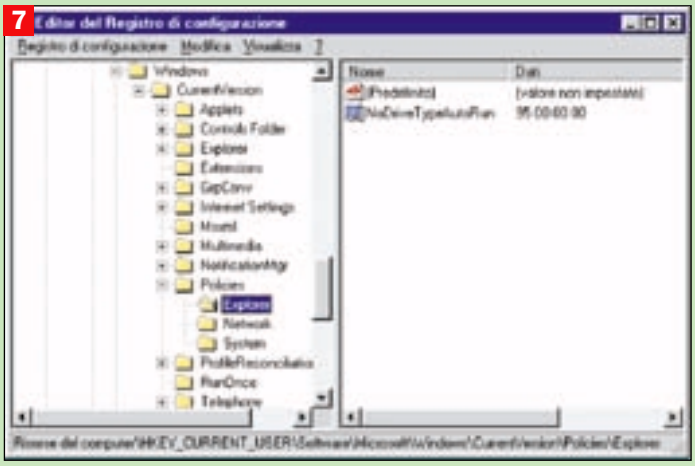
4 In Windows 9x le impostazioni del registro sono di tipo binario, binario DWORD (32 bit) o stringa



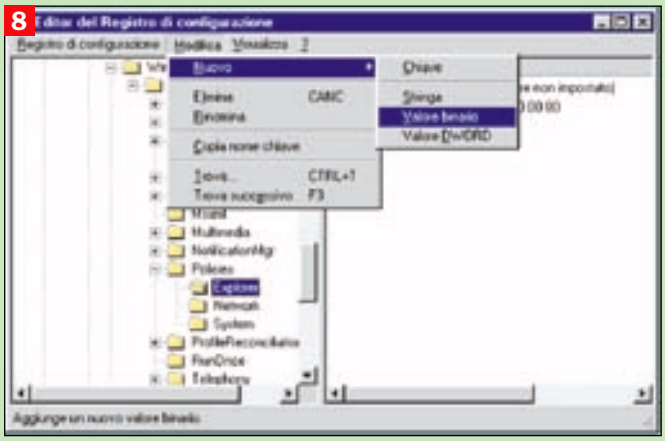
5 In Windows 2000 e XP vengono mostrati i tipi di dato di uso comune: REG_BINARY, REG_DWORD, REG_EXPAND_SZ, REG _MULTI_SZ, REG_FULL_RESOURCE_DESCRIPTOR (altri tipi possono essere definiti). L'esempio si riferisce a Windows 2000.



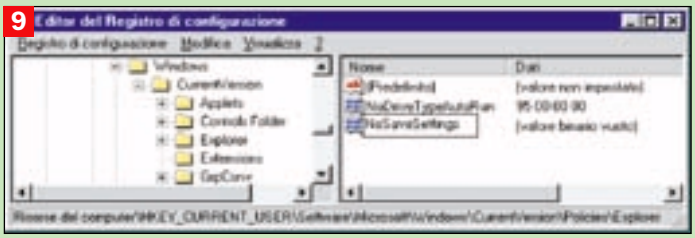
6 Un esempio in Windows XP dove vengono usati vari tipi di dato utilizzati per le impostazioni del Registro.



7 Primo passo dell'esempio. Ci posizioniamo nella sottochiave di Registro di cui vogliamo modificare le impostazioni.

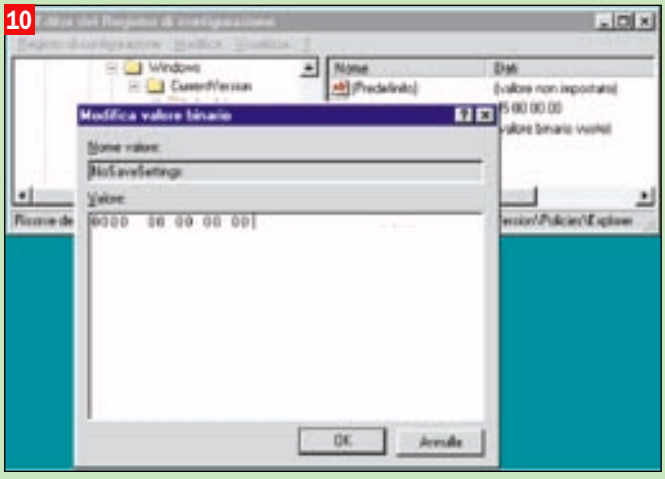


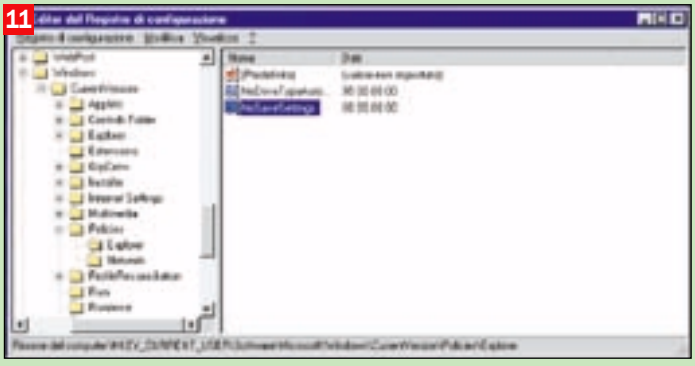
8 Secondo passo: per aggiungere un'impostazione di tipo binario, selezioniamo *Modifica*, *Nuovo*, *Valore binario*.



9 Terzo passo: digitiamo il nome della nuova impostazione, *NoSaveSettings*.

10 Quarto passo: assegnamo valore zero alla nuova impostazione selezionando *Modifica*, ancora *Modifica* e digitando otto zeri.





11 Quinto passo: *NoSaveSettings* è stata inserita con valore zero. Basta uscire da Regedit, ora Windows non altera la disposizione delle icone sul desktop al riavvio.

▶ Windows

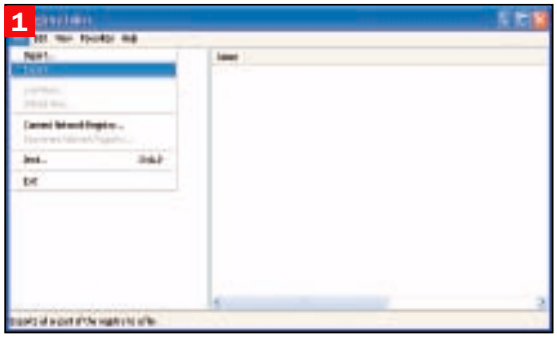
Il backup del Registro di sistema

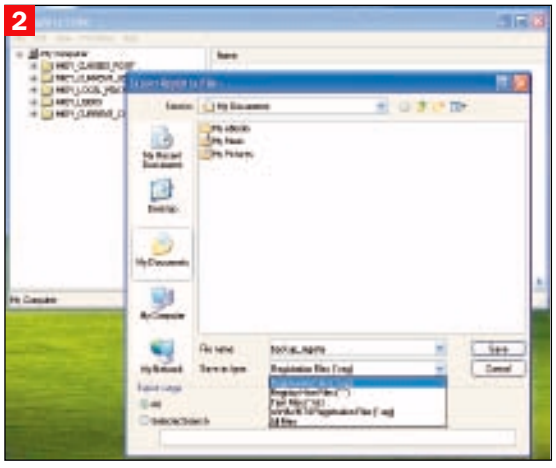
Prima di modificare il Registry di Windows è bene farne una copia di backup, utile anche per rimediare agli eventuali danni prodotti da qualche nuova installazione

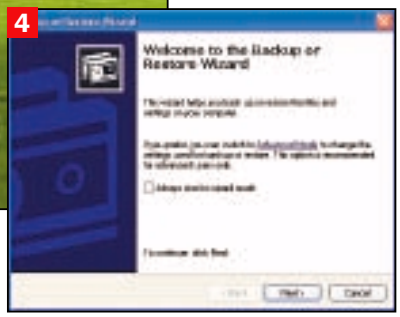
di Giorgio Gobbi

Parlando del Registro, il consiglio abituale è di lasciarlo modificare a Windows, alle applicazioni e alle apposite utility che personalizzano la configurazione del sistema senza fare danni. Una di queste è Xteq Setup, che trovate all'interno del nostro CD ROM. Esaurite le raccomandazioni di rito, se avete deciso di avventurarvi nella giungla del Registro, il suggerimento successivo è di essere cauti, non tentare nulla che non si sia ben capito e salvare una copia di backup di tutto o parte del Registro (quella che si modifica). D'altra parte se si modifica incautamente la descrizione della scheda grafica e del suo driver, Windows può anche rifiutarsi di ripartire, quindi il backup è necessario ma non sufficiente. Se volete la garanzia di poter ripristinare il sistema con tutte le applicazioni, i dati e le personalizzazioni, il modo più rapido ed economico è salvare periodicamente dischi o partizioni con Drive Image o un programma analogo; risparmierete ore interminabili di installazione e riconfigurazione e non perderete nessun dato e impostazione. Se non volete salvare ogni volta l'intera installazione, potreste decidere di fare un backup più ridotto e selettivo, ma tenete presente che in caso di ripristino di uno stato precedente è possibile perdere la coerenza tra ciò che viene ripristinato (anteriore) e ciò che è stato installato dopo la data del backup. Riducendo ulteriormente la prospettiva, se il sistema funziona bene e state per aggiungere una periferica, un driver o un'applicazione su cui avete qualche dubbio, potete salvare il Registro o le parti interessate così da poter tornare subito alla situazione precedente (Windows XP offre la

Due modi per copiare il Registro







3 L'applicazione Backup di Windows (se non l'avete installata la trovate sul CD di Windows XP) permette, tra l'altro, di salvare il Registro

4 La prima volta Backup viene avviato con il Wizard, ma potete decidere di entrare direttamente nel programma

1 Il modo più semplice per creare una copia di backup del Registro di sistema è attraverso la funzione *Export* di Regedit

2 La funzione *Export* permette di salvare il Registro, intero o in parte, in diversi formati. Si può salvare ad esempio un ramo, un sottoramo o una sola chiave con le sue impostazioni

funzione di Device Driver Rollback per tornare al driver precedente).

A volte un'applicazione è dotata di un file *.Reg*, un'estensione associata a Regedit (l'editor di Registro); un doppio clic su uno di questi file (cosa da non fare) eseguirebbe l'immediata modifica del Registro secondo le istruzioni contenute nel file. Se aprite un file .Reg con un editor potete vedere quali sono le aree del Registro interessate dalla nuova installazione, così potete decidere di fare un backup solo di queste parti. Questo però richiede qualche conoscenza in più; prima è bene imparare come fare una copia di backup dell'intero Registro o degli *hive*, i rami (o sottoalberi) di cui è costituito. Sebbene per ogni versione di Windows siano esistite diverse utility di backup, lo strumento comune a tutte le release è Regedit, che permette l'importazione ed esportazione dell'intero Registro o di una sezione (ramo o chiave più sottochiavi). Nell'esempio in Windows XP, selezionando *Export* dal menu *File* di Regedit, si può scegliere se copiare tutto il Registro (*All*) o il ramo o sottoramo correntemente selezionato nel pannello di sinistra (*Selected branch*).

Oltre a immettere la directory e il nome del file di backup, si deve scegliere tra cinque opzioni: *file di Registro* (*.Reg*, quindi in formato testo compatto), *file di hive* (binario), *file di testo* (esteso), file *.Reg* compatibile con Windows 9x e NT oppure Tutti i file, vale a dire salvataggio dell'intero Registro in formato *.Reg*. Un esempio di Registro di Windows XP con poche applicazioni installate occupa circa 40 MB in formato *.Reg* e circa il doppio in formato *.txt*.

L'importazione di tutto o parte di un backup avviene tramite la funzione *Import* di Regedit. Data la pericolosità dell'estensione *.Reg* (un doppio clic aggiorna il Registro con il contenuto del file, senza chiedere conferma) può essere utile modificare l'estensione da *.Reg* in qualcosa di più innocuo.

Un caso in cui basta esportare una sola chiave di Registro (il che include le eventuali sottochiavi) è quello in cui avete deciso di modificare quella particolare chiave con Regedit. Ammesso che la modifica non sia catastrofica (cioè impedisca il riavvio di Windows), potrete ripristinare la situazione precedente reimportando il file *.Reg* salvato.

Segnaliamo un altro sistema per creare un backup del Registro in Windows XP, cioè tramite Windows Backup, che fa parte di XP Pro ma non viene installato di default. Backup è presente anche sul CD di XP Home; va prelevato da *\Valueadd\Msft\Ntbackup*. Il file di backup però è molto più ingombrante, perché viene salvato non solo il Registro ma l'intero stato del sistema (file di boot, file Active Directory, certificati), per un totale di alcune centinaia di MB.

Dato però che Windows Backup è un'utility comoda e versatile, che include uno scheduler per pianificare i backup giorno per giorno, può essere utile installarli, non foss'altro che per eseguire i tradizionali backup dei vostri dati. Inoltre Backup è utile perché funziona eseguendo *copie ombra* (*volume shadow copy*) dei dati, includendo i file aperti e fotografando la situazione nel momento del backup, senza interrompere il lavoro degli utenti e senza saltare i file in uso.

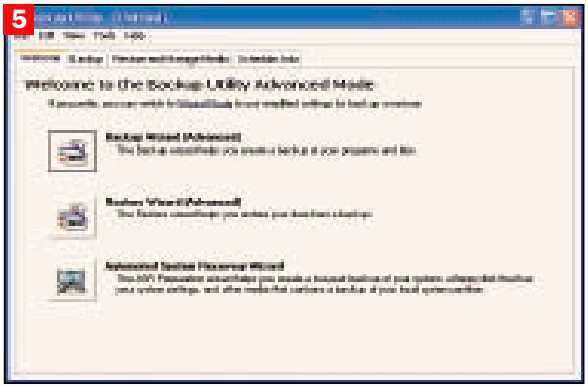
Come si vede nelle illustrazioni, una volta installato, Backup viene eseguito da *Programmi*, *Accessori*, *Strumenti di sistema*.

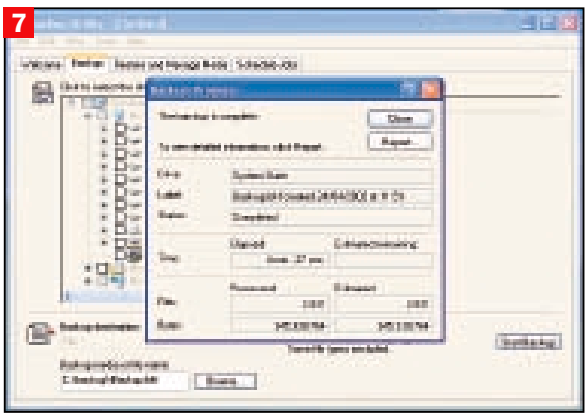
La prima volta propone di usare i Wizard per la scelta delle operazioni, ma potete deselezionare questa opzione ed entrare direttamente nello schermo di Backup dopo aver selezionato la linguetta Backup nella finestra introduttiva.

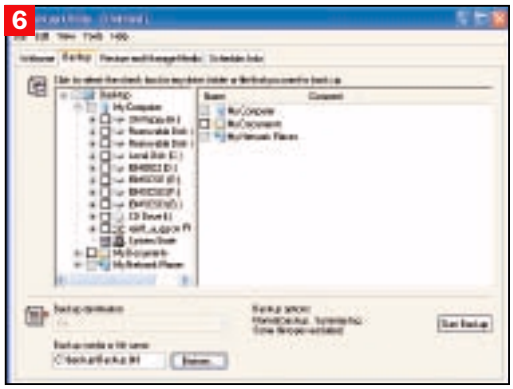
Qui potete selezionare, disco per disco, il sottoalbero da salvare (o tutto il disco) e la destinazione, con l'aggiunta della voce Stato del sistema, l'unica che ci interessa se vogliamo copiare solo il Registro (e inevitabilmente i file di sistema). Come si vede nell'esempio, in quattro minuti e mezzo sono stati salvati 345 MB.

La stessa utility provvede al ripristino. ■

5 Per scegliere direttamente le parti da includere nel backup si seleziona la linguetta *Backup*

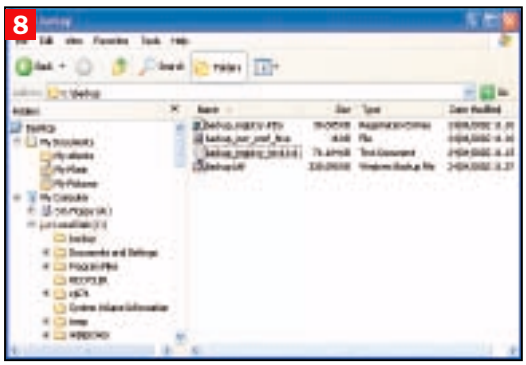






6 La sezione *Backup* vi permette di selezionare i dischi e directory da salvare e anche i file che costituiscono lo *Stato* del sistema, di cui fa parte il Registro

7 Alla fine del backup dello *Stato* del sistema, questo report indica che sono stati salvati oltre 2.000 file per un totale di 345 MB

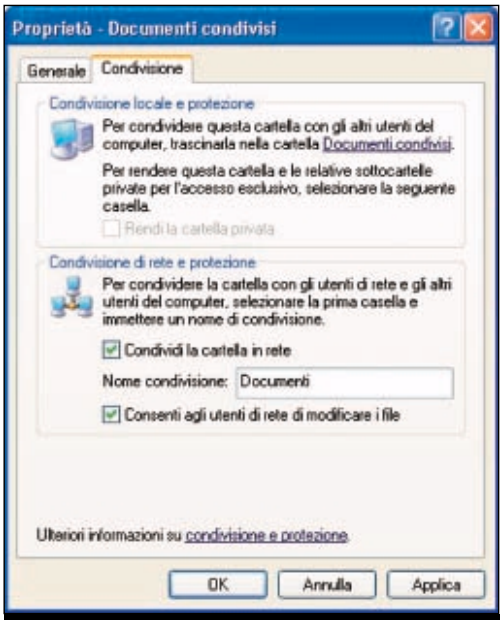


8 A seconda del formato scelto, il backup del Registro occupa qualche decina o qualche centinaio di megabyte; il formato più compatto per un backup completo è il *.Reg*, ma attenzione: facendo doppio clic su un file *.Reg* si modificano all'istante le parti di Registro che vi sono contenute

▶ Configurazione del sistema operativo

Windows XP, registro e dintorni

Continua la serie di articoli sul registro di Windows. Prendiamo in esame le funzioni principali del sistema di Microsoft con due esempi che riguardano le cartelle Documenti e Documenti condivisi



La cartella Documenti condivisi consente pieno accesso a tutti gli utenti; per motivi di sicurezza può essere opportuno toglierla da Risorse del computer

Sempre di più il funzionamento di Windows ruota intorno al registro di sistema (o registry). Un doppio clic sul nome di un file, l'apertura di un'applicazione, il logo di un utente, qualsiasi modifica all'hardware e software installato determinano accessi al registro. Durante il normale lavoro potreste contare migliaia di accessi al registro di sistema (non nel giro di settimane, ma di minuti).

In Windows XP il registro ha subito un'evoluzione per migliorarne la flessibilità e l'efficienza; ora non ha più limitazioni di ingombro e le informazioni che hanno legami logici, come le impostazoni di una certa chiave, tendono a essere registrate nella stessa area del disco, anziché sparpagliate a caso.

Molte delle modifiche alla configurazione di XP sono possibili tramite le funzioni di Windows, per quanto nascoste possano essere; in certi casi però è ancora necessario l'editing diretto del registro. Vale la regola di modificare il registro solo nei casi strettamente necessari e di fare un backup del registro o delle parti interessate prima di ogni modifica. A questo scopo si possono usare le funzioni di import/export dell'editor Regedit, l'applicazione Backup di Windows XP (copiando lo *Stato del sistema*), i comandi *Copy* e *Xcopy* facendo il boot da un altro sistema operativo o altri modi ancora. L'ideale è utilizzare due installazioni di Windows (in due partizioni diverse) sullo stesso computer, in modo che una possa sempre accedere ai file dell'altra. Il contenuto dei file del registro, salvato quando Windows non è avviato, è presumibilmente più integro e coerente; inoltre può essere ripristinato anche se Windows non parte.

In questo modo, per creare una copia di backup del registro, basta avviare la seconda installazione di Windows (per esempio su D:) ed eseguire il comando *xcopy C:\Windows\System32 \Config*.* E:\Backup_registro*.*/s* (supponendo di voler copiare l'intera struttura del registro da *C:* alla cartella *Backup_registro* su *E:*). Xcopy viene eseguito aprendo una finestra a riga di comando (tipo MS DOS) tramite *Start*, *Programmi*, *Accessori*, *Prompt dei comandi* (oppure *Start*, *Esegui*, *cmd*). Mentre Windows è in funzione non si possono copiare i file del registro con copy o xcopy; si possono salvare con *Regedit* e *Backup*, ma queste copie sono ripristinabili con i rispettivi programmi solo se Windows è avviabile.

Le impostazioni di Windows

Prima di proporre possibili modifiche al registro, ne riassumiamo brevemente la struttura, ricordando che si tratta di un database gerarchico suddiviso in cinque *root key*, o *chiavi predefinite*, chiamate HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_CURRENT_CONFIG, che abbreviamo con HKCR, HKCU, HKLM, HKU e HKCC. Di questi cinque sottoalberi, i più importanti sono HKLM e HKU, perché sono gli unici che sono effettivamente registrati su disco. Le altre root key sono collegate a sottochiavi di HKLM o HKU. Come si può intuire, HKU contiene impostazioni specifiche per ogni utente e HKLM contiene impostazioni che riguardano la configurazione del sistema (come hardware, software e sicurezza).

HKCU contiene le impostazioni relative all'utente della console (l'utente che sta usando la tastiera) ed è un link alla sottochiave SID (security identifier) di HKU che identifica appunto l'utente corrente. Tra le tante sottochiavi di HKCU, quella più ramificata e ricca di informazioni è *Software*, che contiene le impostazioni delle applicazioni con le personalizzazioni specifiche per l'utente corrente.

La struttura di questa sottochiave è standardizzata, in modo da raccogliere le impostazioni di tutte le applicazioni dei vari produttori di software nella forma *HKCU\Software\produttore\programma\versione\ecc*. Le impostazioni relative a Windows iniziano per esempio con *HKCU\Software\Microsoft\Windows\CurrentVersion*.

Le cartelle dell'utente

Windows XP assegna a ogni utente una serie di cartelle speciali, che nella versione italiana si chiamano *Dati applicazioni*, *Impostazioni locali*, *Cookies*, *Documenti*, *Menu Avvio* e via dicendo. Questi nomi di cartella sono presenti nel registro come valori di altrettante impostazioni (*AppData*, *LocalSettings*, *Cookies*, *Start Menu* ecc.) della chiave HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders. La parte %USERPROFILE% del percorso che vedete in Regedit è una variabile di ambiente di sistema che rappresenta il percorso del profilo dell'utente corrente, solitamente partendo dalla radice della partizione di Windows. In altre parole, i percorsi delle cartelle che Windows riserva ai dati personali dell'utente rientrano in una

delle decine di chiavi di registro che definiscono la configurazione di Explorer.

In particolare la cartella *Documenti* (contenente a sua volta *Immagini* e *Musica*) compare in prima fila quando aprite *Risorse del computer*. Questo però non significa che le cartelle personali debbano rimanere necessariamente in quella posizione. Ci sono buoni motivi per spostare almeno una parte delle cartelle elencate in *User Shell Folders*; per esempio potreste volere Documenti, Immagini e Preferiti in un'altra partizione o in un drive di rete (magari protetto da RAID) per tenerli al sicuro indipendentemente da una particolare installazione di Windows; così potete anche utilizzare la stessa cartella di documenti personali da tutte le macchine della rete. Per modificare il percorso di una di queste cartelle basta selezionare la relativa impostazione in Regedit e quindi eseguire *Modifica* con clic destro (non dimenticate di fare un backup del registro prima di modificarlo). Al successivo riavvio le nuove impostazioni entreranno in vigore.

HKEY_USERS e HKEY_CURRENT_USER

Il legame tra HKCU e HKU ha il significato di un alias: le modifiche apportate a HKCU si applicano anche al corrispondente utente in HKU e verranno salvate al *logoff*. Nelle illustrazioni vedete che HKCU è collegato a un utente in HKU identificato da un SID che inizia per S-1-5-21.

Gli altri SID sono identificatori predefiniti: *.DEFAULT* contiene le impostazioni utente usate da Windows XP prima del logon di un utente; S-1-5-18, S-1-5-19 e S-1-5-20 sono i SID rispettivamente degli account *LocalSystem*, *LocalService* e *NetworkService*, utilizzati da programmi o servizi di Windows XP e possono essere ignorati. Altri eventuali utenti avranno anch'essi un SID che inizia con S-1-5-21. Nel SID la prima cifra è il numero di versione (per ora 1), mentre la seconda e la terza cifra rappresentano livelli di autorità (Authority e Subauthority); 5-21 è una coppia di valori non unica usata per identificare utenti specifici.

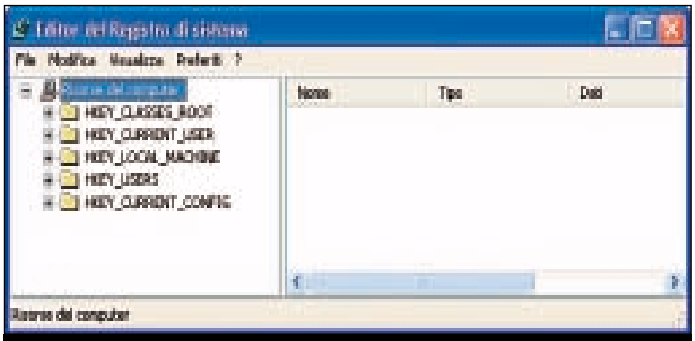
Togliere Documenti condivisi da Risorse del computer

La finestra *Risorse del computer* di Windows XP, nella sezione *File archiviati sul computer* (la prima dall'alto), mostra sia la cartella *Documenti* dell'utente corrente sia la cartella *Documenti condivisi*, utile ad esempio per condividere file tra i membri di una famiglia o di un piccolo gruppo di lavoro.

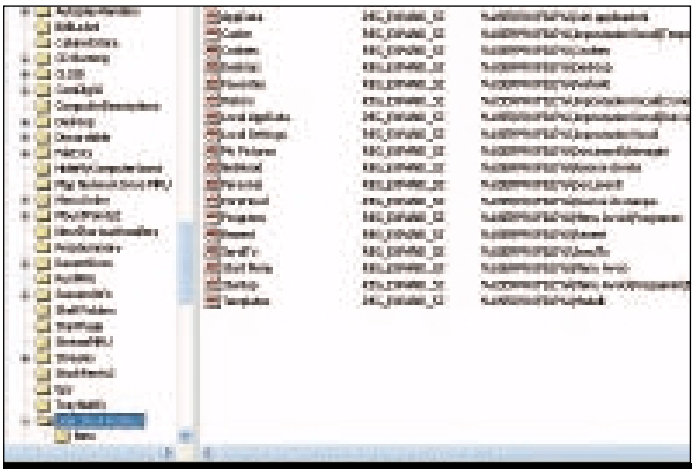
Ci sono tuttavia alcuni esperti che, per motivi di sicurezza, raccomandano di rimuovere tutte le condivisioni non indispensabili, specialmente quando i computer appartengono a un gruppo di lavoro che include PC con Windows 9x/Me, per sua natura privo di gestione degli utenti e della sicurezza. In questi casi un'infezione da worm di un PC della rete si propagherebbe facilmente agli altri computer; infatti, per default, le proprietà di condivisione della cartella *Documenti condivisi* consentono agli altri utenti accesso completo ai file che vi sono contenuti. Per rimuovere la cartella Documenti condivisi e relative sottocartelle da *Risorse del computer* basta eseguire Regedit, aprire la chiave HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MyComputer\NameSpace\DelegateFolders e cancellare la chiave *{59031a47-3f72-44a7-89c5-5595fe6b30ee}*. Prima, però, eseguite un backup del registro o create un punto di ripristino con l'utility *Ripristino configurazione di sistema* in *Start*, *Programmi*, *Accessori*, *Utilità di sistema*. ■

Giorgio Gobbi

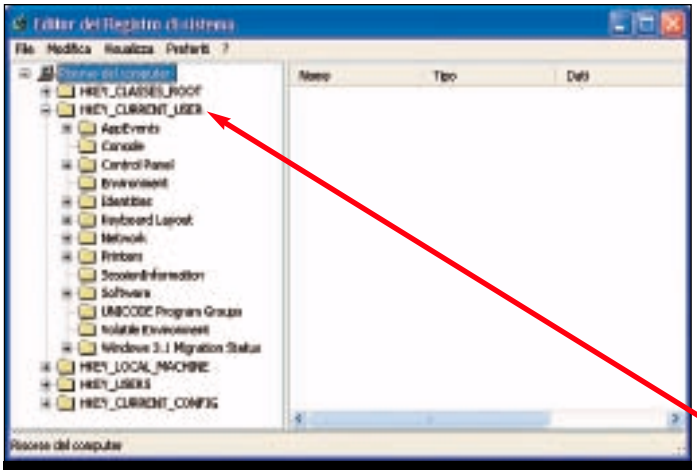
(Nel CD Guida trovate le precedenti puntate sul Registry di Windows)



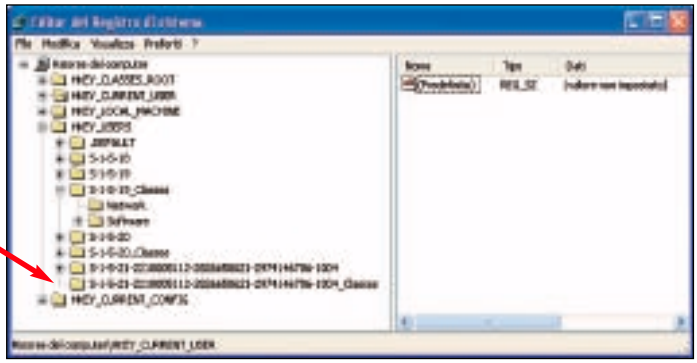
La struttura del registro di sistema di Windows XP



I percorsi delle cartelle personali degli utenti (come Documenti) sono definiti nelle impostazioni della chiave User Shell Folders del ramo HKEY_CURRENT_USER del registro; si possono modificare con Regedit per esempio per avere un'unica cartella Documenti accessibile da tutti i PC della rete



La chiave HKEY_CURRENT_USER (impostazioni relative all'utente corrente) è alias di una sottochiave di HKEY_USERS (impostazioni di tutti gli utenti)



▶ Tuning

Configurare al meglio il registro di **Windows XP**

In questa puntata vediamo come personalizzare l'apertura di Windows XP e il processo di logon in base ai propri gusti o necessità; per farlo usiamo le funzioni del sistema operativo andando a modificare il registro di sistema

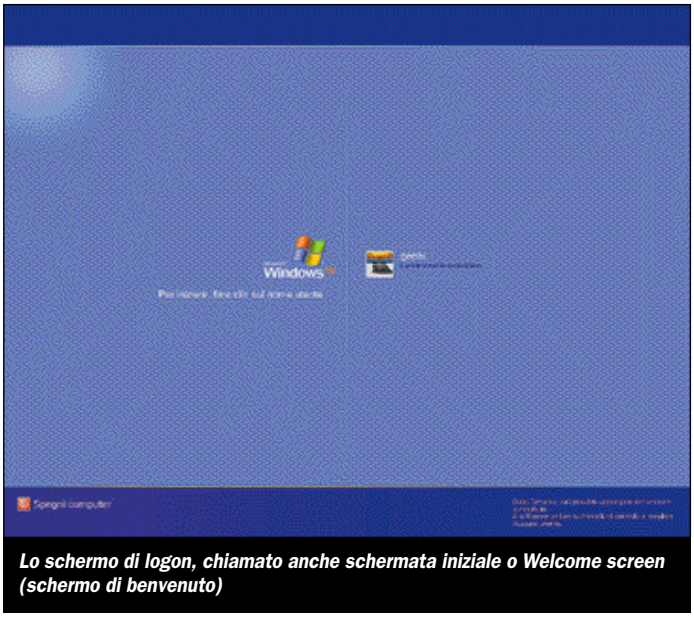
Con un pizzico di editing del registro di sistema e con l'uso delle utility di Windows XP non è difficile modificare l'interfaccia di apertura di Windows e le modalità di accesso (il cosiddetto *logon*, chiamato anche indifferentemente *login*).

In queste pagine vedremo come intervenire per modificare lo schermo di apertura di XP, come si crea un messaggio iniziale (da mostrare all'apertura di Windows), come si sceglie l'interfaccia di logon, come si abilita o disabilita il *Cambio rapido dell'utente*, come si può rendere automatico il logon, come si può mostrare o nascondere i nomi degli utenti al logon.

Lo schermo di benvenuto

Sebbene non ci sia più la scritta di benvenuto, lo schermo iniziale di Windows è normalmente quello che in inglese di chiama *Welcome screen*, su fondo azzurro con i nomi degli utenti. A parte le installazioni aziendali, che possono essere state personalizzate, se avete installato la vostra copia di Windows e avete definito uno o più utenti per il vostro sistema, i loro nomi saranno visibili sullo schermo di benvenuto. L'accesso a Windows (*Windows logon*) avviene facendo clic su uno degli utenti e inserendo la password (se è stata definita).

L'icona assegnata da XP a ogni utente può essere modificata tramite *Start, Pannello di controllo, Account utente, Modifica account, selezione dell'utente, Cambia immagine*. Se nessuna delle icone proposte vi soddisfa o se volete inserire il vostro ritratto, basta scegliere *Cerca altre immagini* o *Ottieni immagine da fotocamera o da scanner*.



Lo schermo di logon, chiamato anche schermata iniziale o Welcome screen (schermo di benvenuto)

Logon automatico

Se il vostro PC non è in rete, non è portatile e in generale si trova in un ambiente protetto e privo di minacce alla sicurezza, potreste voler attivare il logon automatico, senza dover specificare utente e password a ogni logon.

È importante notare che questa funzione comporta un rischio alla sicurezza: chiunque possa mettere le mani sul vostro computer potrà accedere a tutti i contenuti, incluse le eventuali risorse di rete condivise. Questa è quindi un'opzione da usare per compiti specifici (per esempio test che riavviano il computer più volte) o in ambiente sicuro.

Ecco come si può attivare l'accesso automatico a Windows: si apre l'editor di registro (*Start, Esegui, Regedit*), ci si posiziona sulla chiave HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon e si trova la voce *DefaultUsername*. Il suo valore deve essere il nome dell'utente che dovrà avere accesso automatico a Windows. Subito sopra, dovrebbe esserci la voce *DefaultPassword*; se non c'è la si crea con *Modifica, Nuovo, Valore stringa* (tipo di dato REG_SZ) e assegnando alla nuova voce il nome *DefaultPassword*.

Ora si modifica il valore di *DefaultPassword* (clic destro, *Modifica*) assegnando come password di default la password dell'utente scelto per l'autologon. L'ultima modifica da fare al registro è la creazione della voce *AutoAdminLogon* (*Modifica, Nuovo, Valore stringa*) e l'assegnazione del valore 1 alla nuova stringa. A questo punto si esce da Regedit, si chiude la sessione di Windows e si riavvia; l'utente di default avrà accesso automatico a Windows.

Nel momento in cui altre persone avessero accesso al PC o il computer venisse connesso a Internet o altra rete, ricordatevi di ripristinare le impostazion di registro, cancellando la voce *AutoAdminLogon* e il valore della voce *DefaultPassword*. Il valore di *DefaultUsername* resta il nome dell'u-

articoli sul CD n. 69

Le puntate precedenti

1 - **Un registro per tenere il sistema sotto controllo**, PC Open, aprile 2002

2 - **Il backup del registro di sistema**, PC Open, giugno 2002

3 - **Windows XP, registro e dintorni**, PC Open, dicembre 2002

tente di default, anche se il logon torna a essere manuale.

Un nuovo schermo di apertura

Lo schermo di benvenuto è una piacevole evoluzione della finestra di logon di Windows NT e 2000, ma non è detto che sia gradito a tutti gli utenti. Un utente finale potrebbe preferire uno sfondo artistico sia per lo schermo di benvenuto (logon) sia per il desktop, mentre un'azienda potrebbe personalizzare i propri computer inserendo il proprio logo nello schermo di apertura.

È facile modificare lo sfondo del desktop: basta fare un clic destro sul desktop, *Proprietà, Desktop* e selezionare un file grafico dalla cartella di Windows o da altra cartella tramite *Sfoglia*.

Per sostituire lo schermo di benvenuto con un'immagine creata dall'utente, il percorso inizia disabilitando lo schermo di benvenuto tramite *Pannello di controllo, Account utente*, *Cambia modalità di accesso e disconnessione* e quindi disattivando *Usa la schermata iniziale*. Può accadere che entrando in questa finestra compaia un messaggio relativo al *Cambio rapido utente*; basta cliccare *Annulla* e continuare.

Ora che abbiamo eliminato il Welcome screen (schermata iniziale), basta impostare nel registro di sistema il nome e percorso del file con l'immagine che vogliamo visualizzare all'apertura di Windows, che farà anche da sfondo alla finestra di logon.

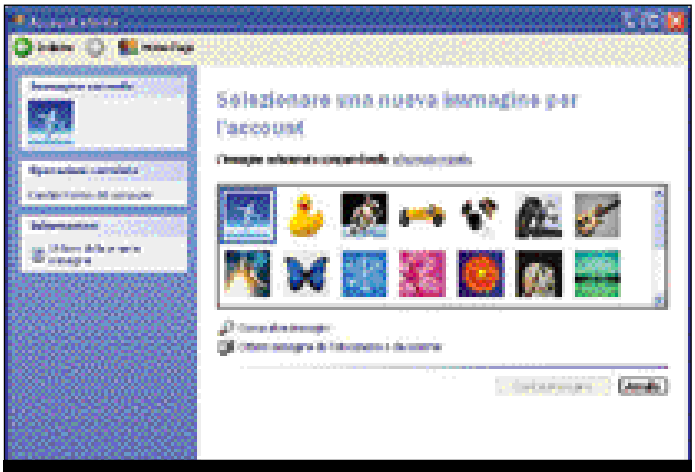
Si esegue Regedit (Start, Esegui), ci si posiziona sulla chiave HKEY_USERS\.DEFAULT\Control Panel\Desktop e sulla voce *Wallpaper*. Con clic destro e *Modifica* si inserisce il percorso completo del file di sfondo (per esempio in formato .bmp). Al prossimo riavvio, sullo schermo apparirà la vostra foto, opera d'arte o altra immagine preferita (o il logo aziendale), che potrà anche coincidere con l'immagine scelta come sfondo per il desktop.

Cambio rapido di utente

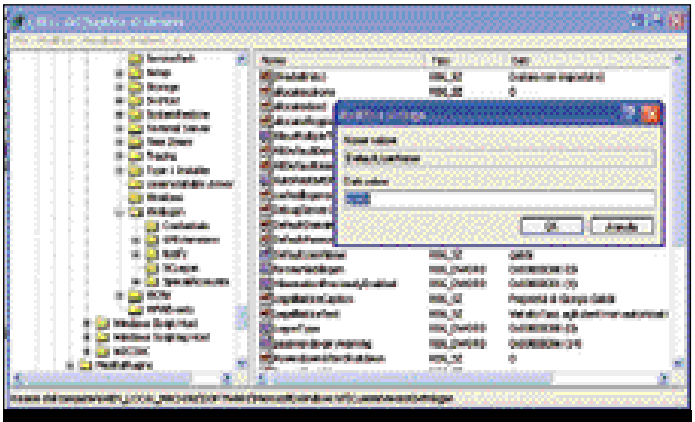
Windows XP permette la multiutenza dei programmi in background: sebbene un solo utente utilizzi la tastiera e il mouse, più utenti possono avere sessioni aperte (con logon effettuato) e avere programmi in esecuzione, per esempio la riproduzione di un film su DVD con la seconda uscita video (se l'avete) inviata al televisore o a un secondo monitor.

Abbiamo visto che in *Pannello di controllo, Account utente, Cambia modalità di accesso e disconnessione,* si può attivare o disattivare il *Cambio rapido utente*, che è selezionabile se è attivata l'opzione *Usa la schermata iniziale*. Una volta attivato il cambio rapido utente, per passare da un utente all'altro basta premere il tasto *Windows* (tra *Ctrl* e *Alt* sulle tastiere dei desktop) insieme al tasto *L*. Immediatamente si torna allo schermo di logon dove si può aprire un'altra sessione con nome di utente diverso o portare in primo piano una sessione già aperta in background. In pratica non occorre il *logoff*: l'utente resta *logged on* e le sue applicazioni restano aperte.

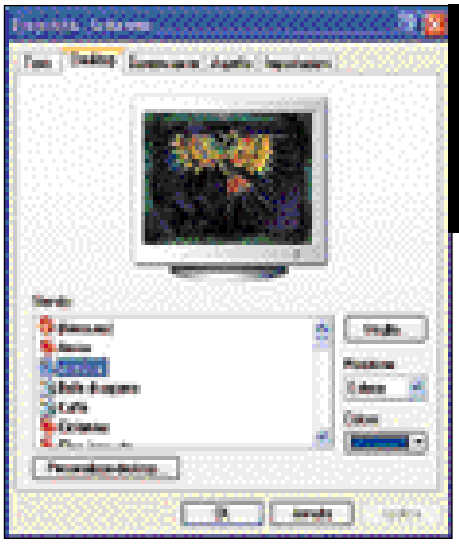
Inutile dire che per sfruttare questa funzionalità dovrete avere memoria in abbondanza, specialmente se i programmi aperti eseguono del lavoro anche in background.



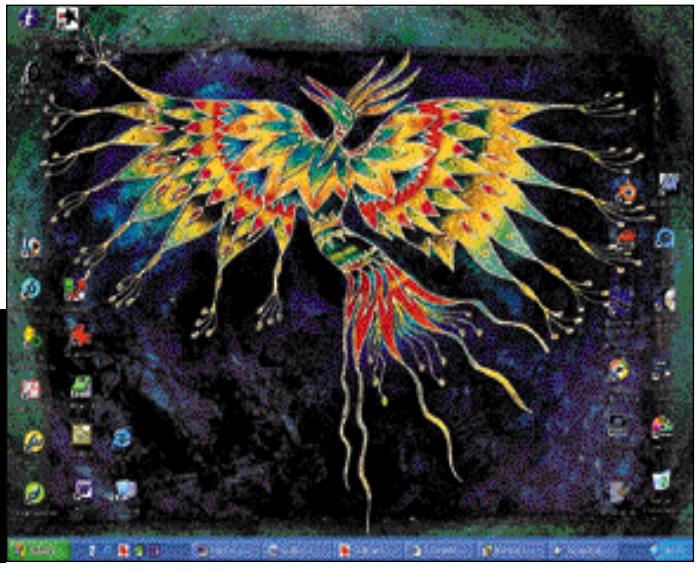
Windows XP permette di sostituire l'icona associata all'utente con un'altra immagine, sia scelta tra quelle proposte da XP sia fornita dall'utente



Per impostare il logon automatico all'avvio di Windows basta editare alcune voci della chiave di registro Winlogon; questa è un'operazione sconsigliata, per motivi di sicurezza, se il PC è in rete o è accessibile ad altre persone



Windows permette di sostituire lo sfondo del desktop in Proprietà - Schermo, ma non offre una funzione per sostituire lo schermo di avvio



Se lo si desidera, è possibile modificare lo schermo di avvio di Windows; nell'esempio ci proponiamo di utilizzare lo sfondo del desktop anche per l'avvio di XP

Quando il PC resta inutilizzato ed è in funzione uno screen saver, per default il sistema torna allo schermo di logon alla ripresa dell'attività (input di mouse o tastiera). Se preferite barattare questa misura di sicurezza con l'immediatezza d'uso, basta disattivare l'opzione *Al ripristino torna alla schermata iniziale* in *Proprietà schermo, Screen saver* (dopo clic destro sullo sfondo del desktop).

Se volete attivare l'opzione *Utilizza cambio rapido utente* ma non potete farlo perché è visualizzata in grigio (quello che succede disattivando la schermata iniziale), c'è un rimedio.

Aprite la finestra *Strumenti, Opzioni cartella* in Explorer (Risorse del computer) e disattivate la casella *Abilita file non in linea*, così verrà resa nuovamente disponibile l'opzione *Utilizza cambio rapido utente*.

Mostrare e nascondere gli utenti

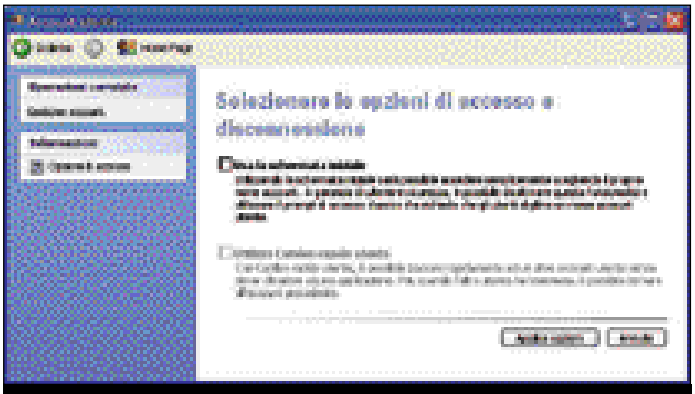
Nel Welcome screen, o schermata iniziale, sono elencati uno o più utenti; basta fare clic su uno di essi per fare il logon. Il punto chiave è che questo elenco di utenti non è necessariamente completo. Consideriamo per esempio l'utente Administrator di Windows XP Professional; sappiamo che esiste, ma per default non viene visualizzato. Per fare il login come Administrator potete premere due volte *Ctrl-Alt-Del* nella finestra di logon e inserire nome utente e password nella finestra che appare. Windows XP Home Edition non permette il logon come Administrator, anche se questo utente esiste e per default ha password vuota. Se doveste ricorrere alla *Recovery Console* (la console di ripristino di emergenza) in XP Home dovrete specificare la password di Administrator (se non vi piace vuota potete cambiarla tramite *Pannello di controllo, Account utente, Modifica account*).

Oltre ad Administrator, potete avere altri account nascosti, non solo quelli speciali usati da Windows ma anche account corrispondenti a utenti in carne e ossa definiti da voi.

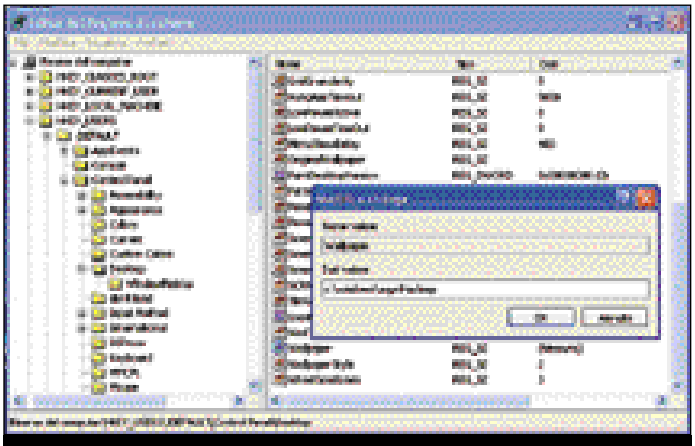
In generale potete personalizzare lo schermo di logon aggiungendo o togliendo utenti a piacere. Per farlo, aprite Regedit e vi posizionate sulla chiave HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList.

Qui aggiungete una nuova voce (*Modifica, Nuovo, Valore DWORD*) e le assegnate come nome l'account che vi interessa mostrare o nascondere.

Per nascondere l'account assegnate alla voce corrispondente valore 0; per renderlo visibile assegnate valore 1. E per quanto riguarda Administrator? Per renderlo sempre visibile nello schermo di logon ba-



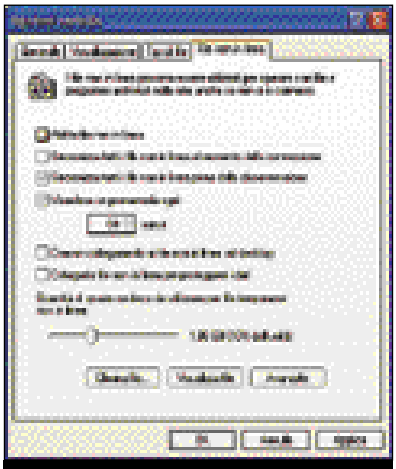
Per modificare lo schermo di avvio è necessario per prima cosa disattivare lo schermo di logon *(schermata iniziale o* Welcome screen*)*



Dopo aver disattivato la schermata iniziale, si apre Regedit e si assegna alla voce Wallpaper *il nome e il percorso del file con la nuova immagine di apertura, che nell'esempio è la stessa usata per il desktop*

Il risultato delle due operazioni precedenti è l'apertura di Windows XP con l'immagine di nostra scelta; dopo qualche istante appare la finestra di logon che chiede nome e password dell'utente

Se non avete problemi di sicurezza (per esempio utenti non autorizzati a usare il vostro PC), potete disattivare, in Proprietà - Schermo*, il ritorno allo schermo di logon ogni volta che uscite dallo screen saver per riprendere il lavoro*



Disattivando l'opzione **Abilita file non in linea** *in* **Opzioni Cartella** *di* **Risorse del computer** *viene mantenuta la possibilità di attivare il cambio rapido di utente anche senza attivare l'uso della schermata iniziale di* **logon**

sta aggiungere Administrator alle voci della chiave *UserList* e assegnarle valore 1.

Nascondere l'ultimo utente

Per motivi di riservatezza o di sicurezza, spesso si desidera nascondere il nome dell'utente che per ultimo ha eseguito un logon.

Windows, per facilitare l'utente abituale, ripropone come default il nome dell'ultimo utente che ha avuto accesso al sistema.

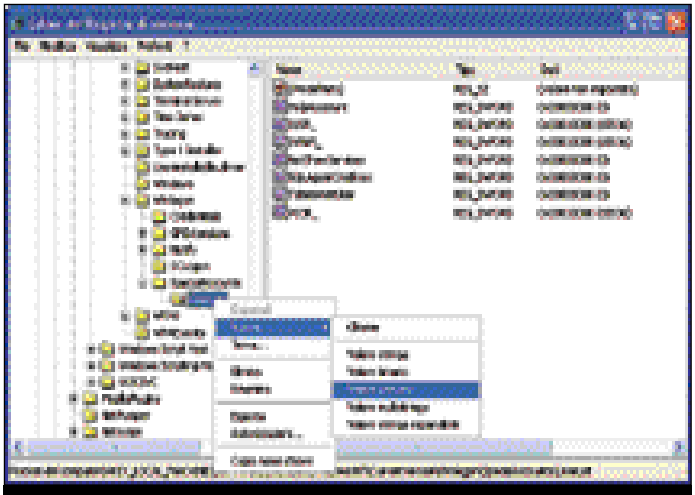
Per impedire che questo avvenga, si ricorre all'editing del registro. Aperto Regedit, ci si posiziona sulla chiave HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system, si aggiunge una nuova voce con *Modifica, Nuovo, Valore DWORD* e le si assegna il nome *DontDisplayLastUserName*. Quindi, con clic destro e *Modifica*, si assegna a questa voce il valore 1. Se in seguito vorrete disabilitare questa opzione e tornare al comportamento di default, basterà assegnare valore 0 a *DontDisplayLastUserName*.

Un messaggio iniziale

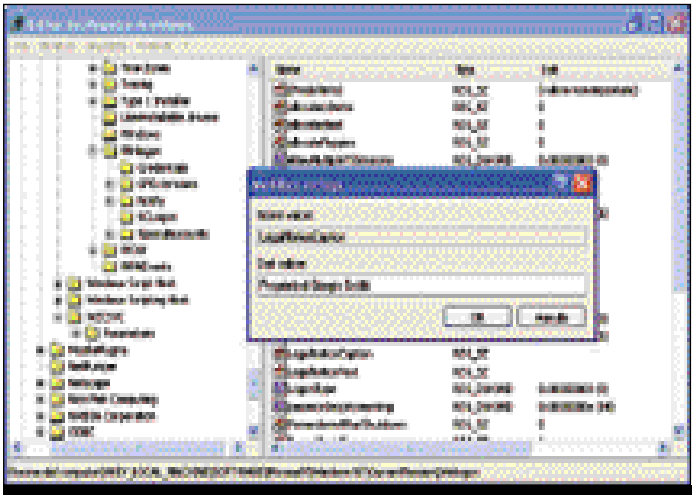
Talvolta è utile impostare un messaggio iniziale che sarà visualizzato come prima cosa all'avvio di Windows. In XP potete definire il titolo della finestra e il testo contenuto all'interno. Per esempio, il legittimo utente di un PC potrebbe avvisare eventuali ospiti indesiderati di stare alla larga, perché non sono autorizzati all'accesso ma vengono registrati e rischiano gravi sanzioni (può essere uno scherzo o una cosa seria, decidete voi).

Un modo facile per farlo è l'editing di due voci di registro sotto la chiave HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon. Alla voce *LegalNoticeCaption* dovrete assegnare come valore (con clic destro e Modifica) il titolo che volete dare alla finestra del messaggio; assegnerete quindi come valore della voce *LegalNoticeText* il testo che sarà visualizzato dentro la finestra. ■

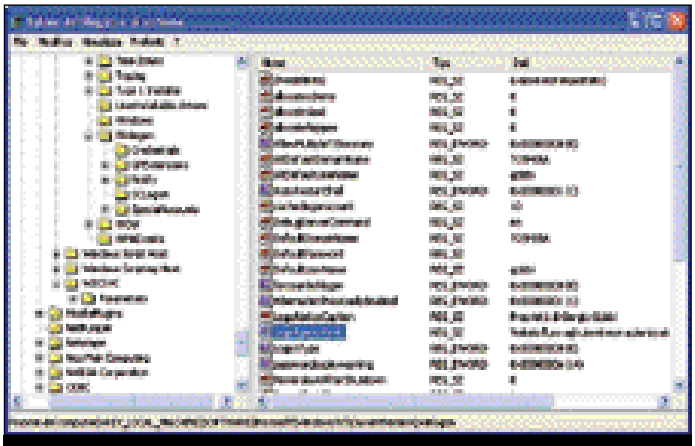
Giorgio Gobbi



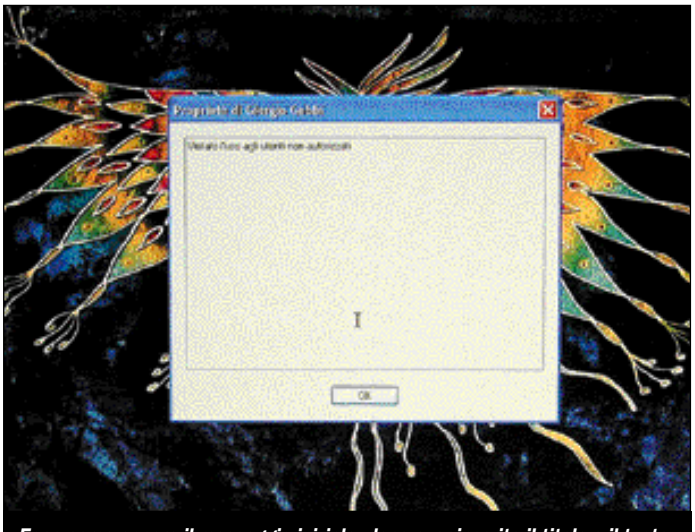
Inserendo una nuove voce sotto la chiave UserList del registro, possiamo determinare se un utente sarà visibile o nascosto nella lista proposta dalla schermata iniziale di logon; per esempio, si può rendere visibile l'utente Administrator in XP Professional



Tramite l'editing di due voci di registro, si può introdurre un messaggio iniziale che verrà mostrato all'utente all'avvio di Windows XP



LegalNoticeCaption (il titolo) e LegalNoticeText (il testo) sono le due voci della chiave Winlogon che permettono di mostrare un messaggio iniziale all'utente di Windows XP



Ecco come appare il messaggio iniziale, dopo aver inserito il titolo e il testo nel registro di sistema

▶ Le novità dell'ultima versione

DirectX 9: un salto nel colore con un miliardo di sfumature

Molte delle schede grafiche 3D appena uscite sfoggiano il supporto alle librerie di Microsoft come segno di distinzione. Ma non tutti sanno che cosa sono e come funzionano. Vediamolo insieme

DirectX è uno strato software che fa da ponte tra il programma che sta girando sul sistema operativo Windows e l'hardware. I programmi invece di accedere direttamente alla periferica hardware (per esempio la scheda audio, video o joystick) richiamano delle funzioni standard di DirectX. Quest'ultimo traduce, con l'ausilio dei driver sviluppati dal produttore, le istruzioni in comandi compresi dalle periferiche.

Per capire meglio questo concetto facciamo un passo indietro: ai tempi del DOS e di Windows 3.x i software accedevano direttamente alle funzioni hardware dei componenti. I programmatori dovevano quindi includere nel software i driver necessari per gestire i vari tipi di periferiche esistenti. Da un lato il sistema ha i suoi vantaggi perché consente di spremere al massimo le funzionalità della periferica, allo stesso tempo però obbliga il programmatore a inserire una miriade di driver per supportare il maggior numero di periferiche possibili. Se un utente possedeva un hardware per il quale non era incluso il driver doveva rinunciare a eseguire il programma.

A partire da Windows 95 Microsoft ha introdotto un nuovo metodo di gestione delle periferiche hardware, il DirectX appunto, che rende le applicazioni software non più legate a un hardware specifico.

In DirectX esistono due "traduttori": *HAL* (*Hardware Abstraction Layer*) e *HEL* (*Hardware Emulation Layer*). All'avvio del PC DirectX interroga le periferiche alla ricerca delle capacità supportate, le capacità riscontrate sono quindi memorizzate in una tavola che verrà interpellata durante l'esecuzione del programma. Se il programma richiede un'operazione che l'hardware può eseguire, per esempio il Transform e Lightning, è HAL ad occuparsi della gestione. Viceversa è la parte HEL che se ne incarica eseguendo l'operazione in emulazione software. HEL ha alcune limitazioni e la principale è che non è in grado di eseguire in emulazione tutte le capacità hardware. Pertanto un'immagine finale ottenuta da un'emulazione software sarà diversa dalla stessa immagine elaborata in hardware.

I diversi moduli che compongono DirectX

DirectX è composto da vari moduli. *DirectDraw* e *Direct3D*, dalla versione 7 sono accorpati in un modulo unico chiamato *DirectX Graphics*, si occupano di tutto quanto riguarda la visualizzazione e l'accelerazione hardware dell'immagine.

DirectInput è la parte designata al controllo delle periferiche, joystick e simili, usati nei giochi. *DirectX Audio* è il componente che gestisce la riproduzione della parte audio mentre *DirectPlay* è l'interfaccia software che fornisce le funzionalità necessarie per i giochi multiplayer. *DirectShow* infine permette di riprodurre e modificare in tempo reale i file audio e video.

In ogni rilascio di DirectX Microsoft aggiunge nuove funzionalità. Per esempio nella 9 è incluso l'*Hardware Displacement Mapping*, il supporto per una visualizzazione del colore a 10 bit che permette di riprodurre circa un miliardo di sfumature, l'applicazione di 16 texture in una singola passata e altro. L'Hardware Displacement Mapping è una tecnica che migliora la riproduzione delle superfici. Su una superficie piana è applicata una mappa di livelli di grigio e il programma modifica la superficie in base ai livelli di grigio.

Facciamo un esempio, immaginiamo di disegnare un cerchio e di applicarvi sopra un altro cerchio di colore grigio, con la parte centrale più chiara che vira in tonalità più scure verso l'esterno. Il risultato finale dell'elaborazione sarà un cono, se le sfumature dal centro verso l'esterno sono costanti, oppure il rilievo di una montagna. Il principio è

Prima di avviare la diagnostica di DirectX è consigliabile chiudere tutti i programmi in esecuzione dal Task Manager di Windows e disabilitare gli antivirus e firewall

simile a quello usato nelle mappe geografiche dove l'altezza delle montagne è rappresentata con vari livelli di marrone. La visualizzazione a 10 bit è un grosso passo in avanti nella resa cromatica delle immagini. Con la tecnologia a 8 bit, che corrisponde a 16 milioni di colori visualizzabili, era possibile riprodurre fino a 256 sfumature per ogni singolo colore (rosso, verde e blu). A 10 bit il numero di colori supera il miliardo e le sfumature disponibili per ogni singolo colore salgono a 1.024. La possibilità di applicare sino a 16 texture in una sola passata consente di creare superfici elaborate aumentandone il realismo.

Come è intuibile non basta installare il DirectX 9 per beneficiare di tutte queste migliorie grafiche, servono una scheda video che abbia la capacità di eseguirle e dei driver appositamente scritti.

Trucchi d'installazione della nuova versione

Nello sviluppo di DirectX Microsoft ha mantenuto la compatibilità totale con le versioni precedenti, tuttavia possono insorgere problemi di funzionamento con alcune delle periferiche installate. Ecco alcuni consigli e informazioni per evitarli e risolverli.

I sistemi operativi Microsoft che supportano DirectX 9 sono: Windows 98, 98SE, Millennium, 2000 e XP. Windows 95 supporta fino alla versione 8.0a mentre NT4 è fermo alla versione 3.0a contenuta nel Service Pack 6.

Una volta installato non è possibile rimuovere DirectX in quanto parte integrante del sistema.

I metodi di rimozione che si trovano in Internet non sono affidabili al 100 per cento e possono compromettere la stabilità o il funzionamento completo del sistema. Gli utilizzatori di Windows XP e Millennium possono creare un punto di ripristino con l'utility *Ripristino configurazione di sistema* accessibile in *Start, Tutti i programmi, Accessori, Utilità di sistema*. Con gli altri sistemi è consigliato un backup.

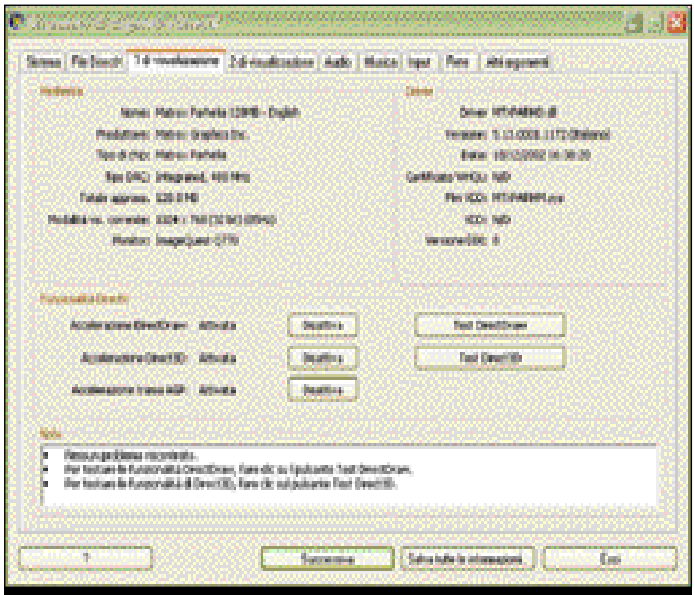
Ma prima di installare DirectX aggiornate tutti i driver delle periferiche. Le ultime versioni di driver generalmente non possiedono la certificazione *WHQL* (*Windows Hardware Quality Lab*), una serie di test che ne verificano la compatibilità col sistema operativo, e in qualche caso potrebbero avere dei problemi di funzionamento. Per scoprire se il malfunzionamento dipende dal driver ci sono vari metodi. Il primo è sostituire il driver con una versione certificata, il secondo di utilizzare il driver incorporato in Windows (se disponibile) e infine di provare con un'altra versione.

I programmi eseguiti in background potrebbero utilizzare delle risorse di sistema richieste dall'applicazione o dal gioco. Per evitare interferenze in Windows 9x premete contemporaneamente i tasti *Ctrl, Alt e Canc* (o *Del*) e chiudete tutti i programmi in esecuzione ad eccezione di *Explorer* e *Systray (*in Windows XP chiudete tutto quanto è visibile*)*. Se al riavvio dopo l'installazione di DirectX ci sono dei problemi col video, righe verticali o funzionamento solo in modalità provvisoria, è necessario installare nuovamente i driver video. Prima però è consigliabile installare i driver inclusi in Windows per una normale scheda video VGA.

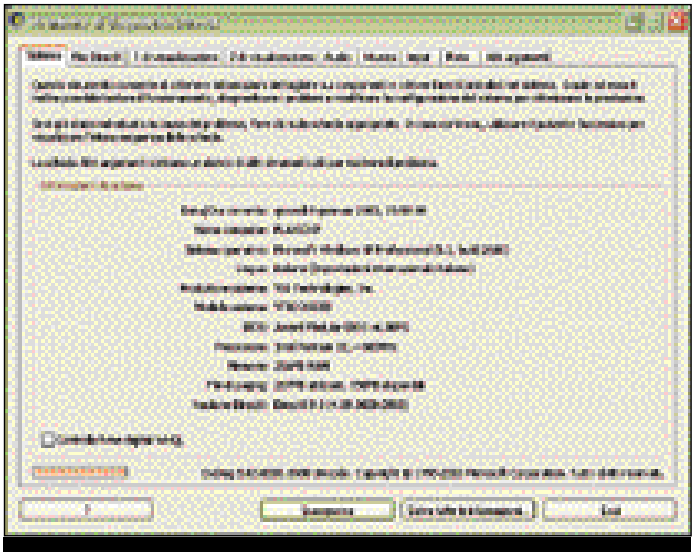
Se l'audio non funziona correttamente provate ad abbassare gradualmente l'impostazione di accelerazione hardware che si trova nelle *Proprietà audio avanzate*. In Windows XP è raggiungibile da *Start, Pannello di controllo, Suoni e periferiche audio, Audio, Avanzate, Prestazioni*.

In DirectX è incluso Dxdiag.exe, un potente strumento di diagnostica che permette di verificare le capacità di accelerazione hardware delle periferiche presenti e il loro stato, la versione installata, se ci sono dei problemi con i file di DirectX e altro. Dxdiag è avviabile da *Start, Esegui* e digitando Dxdiag.exe nella casella. ■

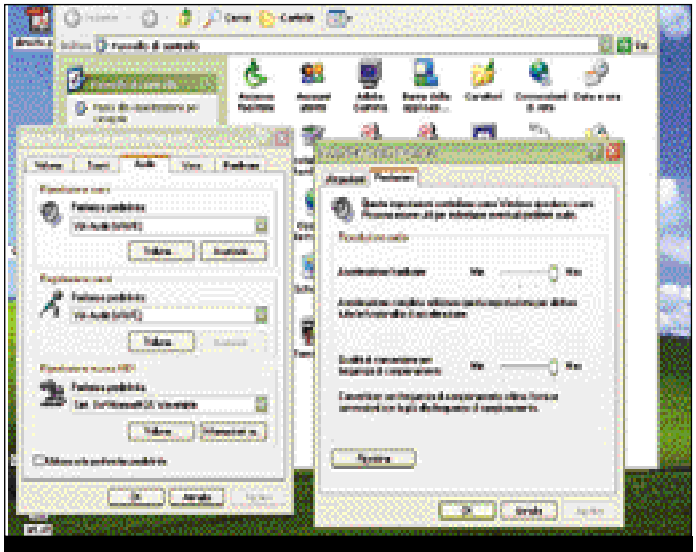
Flavio Nucci



Nella diagnostica di DirectX è visibile lo stato delle funzionalità relative alla periferica, in questo caso la scheda grafica, ed è possibile eseguire alcuni test



La schermata iniziale dello strumento di diagnostica di DirectX con le informazioni di sistema



Nelle proprietà audio avanzate si trova la regolazione per l'accelerazione hardware della riproduzione audio

▶ Conoscere il sistema operativo

Ripristinare i file del registro

Anche se Windows non si avvia, non tutto è perduto. Ecco spiegata nel dettaglio la procedura per riprendere una configurazione di sistema salvata precedentemente

di Giorgio Gobbi

articoli sul CD n. 70

Le puntate precedenti

1 - Un registro per tenere il sistema sotto controllo, PC Open, aprile 2002

2 - Il backup del registro di sistema, PC Open, giugno 2002

3 - Windows XP, registro e dintorni, PC Open, dicembre 2002

4 - Configurare al meglio il registro di Windows Xp, PC Open, marzo 2003

Prendiamo lo spunto da un episodio accaduto per parlare dei file del registro di sistema e di come ripristinarli persino se Windows non è avviabile.

Rispetto alle versioni precedenti, e in particolare a Windows 2000, da cui deriva, Windows XP ha introdotto nuove funzioni per facilitare la manutenzione del sistema. Un esempio significativo è l'utility *Ripristino configurazione di sistema*, che permette di ripristinare uno stato precedente del sistema quando si verifica un problema grave per l'integrità e il funzionamento di Windows. Per *stato del sistema* si intende un insieme di dati chiave che descrivono l'installazione (hardware, sistema operativo, utenti e applicazioni) e che sono contenuti nel registro e in altri file di sistema (la lista dei file è contenuta in Windows\System32\Restore\Filelist.xml).

Il caso di una workstation

La nostra storia inizia con una workstation biprocessore basata su dischi SCSI in RAID 0. Dopo un paio d'anni di onorato servizio senza problemi con Windows 2000, è stato deciso di passare a Windows XP e di sostituire i due dischi SCSI con un singolo drive di capacità superiore, anche perché il controller RAID installato non supportava Windows XP. Sostituiti i dischi e il controller SCSI, è stato installato XP e il sistema ha funzionato regolarmente per un po' di giorni. I problemi sono iniziati il mattino in cui il sistema non si è più avviato, avvisando che il file SYSTEM era corrotto. Prima di raccontare che cosa è accaduto, vediamo che cos'è il file SYSTEM.

I file del registro

Nelle puntate precedenti (gli articoli sono disponibili in formato PDF nel BCD Guida) abbiamo visto che la struttura logica del registro di sistema è una gerarchia di sottoalberi che si chiamano HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS e HKEY_CURRENT_CONFIG.

Le chiavi HKLM e HKU (usiamo le abbreviazioni) sono le due strutture principali; le altre tre non sono altro che link, per comodità di accesso, ad alcune sottochiavi di HKLM e HKU. HKU contiene i profili degli utenti e HKLM contiene tutto il resto: informazioni su hardware, sistema operativo, applicazioni e utilizzo del sistema.

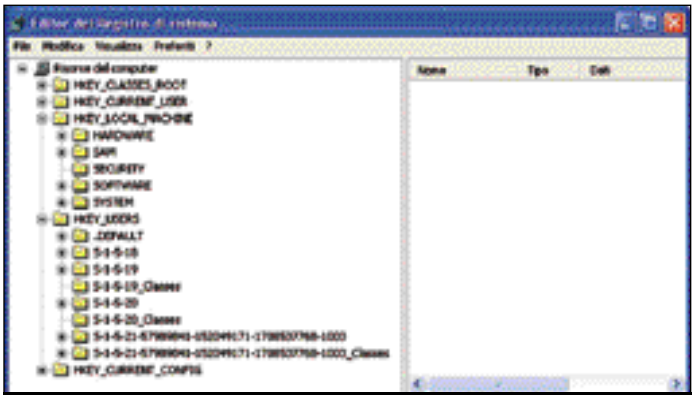
Fisicamente, la struttura logica è contenuta in una serie di file residenti per la maggior parte in WINDOWS\system32\config.

Vediamo quelli principali: il file SYSTEM conserva i contenuti della sottochiave HKEY_LOCAL_MACHINE\SYSTEM; il file SOFTWARE supporta la chiave HKEY_LOCAL_MACHINE\SOFTWARE; il file SAM (Security Accounts Manager) supporta la chiave HKEY_LOCAL_MACHINE\SAM; SECURITY supporta HKEY_LOCAL_MACHINE\SECURITY. Passando alle descrizioni degli utenti, DEFAULT supporta HKEY_USERS\.DEFAULT; le chiavi di tipo HKU\SID (i SID sono i Security Identifiers: codici che identificano gli utenti, sia persone sia account di sistema) sono supportate dai file NTUSER.DAT e NTUSER.DAT.LOG ubicati in ciascuno dei profili utente, sotto Documents and Settings; le chiavi HKU\SID\Classes sono supportate dai file UsrClass.dat e UsrClass.dat.LOG anch'essi ubicati in ciascun profilo utente sotto Impostazioni locali\Dati applicazioni\Microsoft\Windows. In WINDOWS\system32\config ci sono altri file ausiliari: quelli .sav contengono lo stato del registro dopo la fase in modo testo del setup di Windows, ripristinabili in caso di problemi durante la fase in modo grafico; i file .log contengono le variazioni ai file del registro, poi registrate su disco in modo sicuro; i tre file .evt contengono la registrazione degli eventi (suddivisi in *Applicazione*, *Protezione* e *Sistema*) visualizzati dall'utility Visualizzatore Eventi.

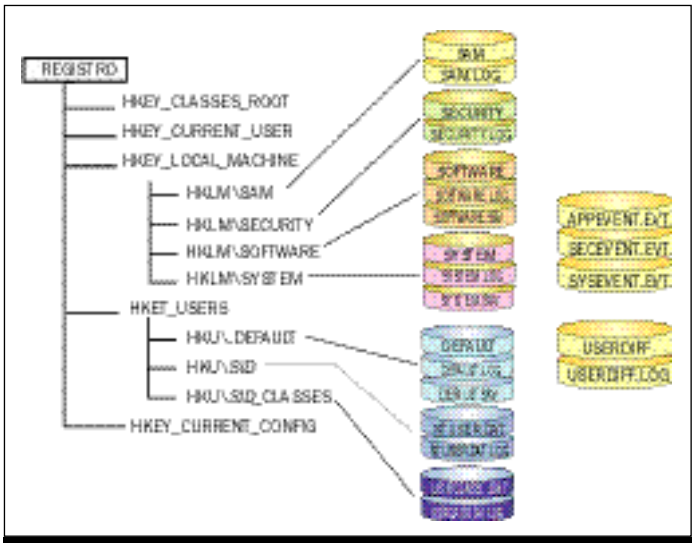
SYSTEM è il più importante dei file di registro e viene utilizzato fin dalle prime fasi del processo di avvio di Windows. Nella chiave HKLM\SYSTEM ci sono tra l'altro le informazioni per inizializzare il registro, inclusa la posizione delle altre chiavi di registro. Quindi, se SYSTEM manca o è corrotto, il processo di avvio di Windows si arresta con un messaggio di errore.

La workstation si blocca

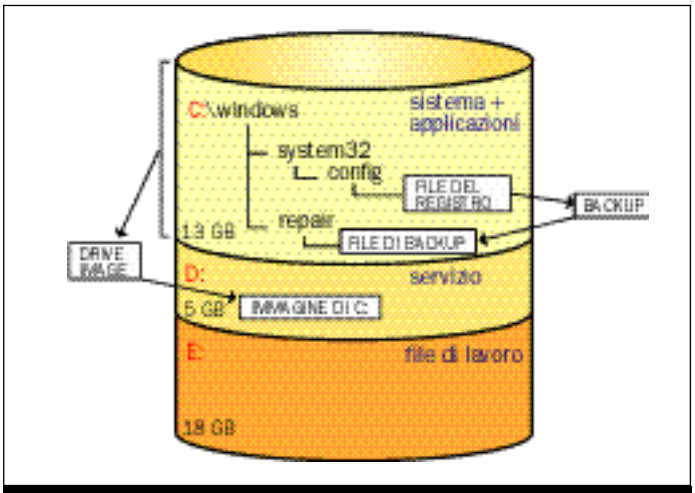
La prima volta che Windows XP ha mostrato questo messaggio di errore, il proprietario della workstation ha reinstallato Windows e qualche applicazione, giusto per tastare il terreno. *Chkdsk* non aveva riscontrato difetti sul disco (appena acquistato) e la disavventura sembrava imputabile a qualche problema software, vista anche la complessità dell'installazione. Un paio di giorni dopo però l'evento si ripete e questa volta il file corrotto è SOFTWARE, il più grosso dei fi-



I cinque* "hive" *o* sottoalberi *in cui è suddiviso il registro; HKEY_LOCAL_MACHINE e HKEY_USERS contengono tutti i dati, gli altri rami sono degli alias per comodità di accesso



La corrispondenza tra le sezioni (hive) del registro e i rispettivi file fisici



Nell'esempio citato nell'articolo, l'hard disk della workstation è stato suddiviso in tre partizioni; l'utility Backup salva giornalmente i file del registro, mentre Drive Image salva periodicamente un'immagine della partizione C:

le di registro. A questo punto l'utente chiede soccorso con due obiettivi: 1) risolvere il problema e 2) non dover reinstallare Windows XP, Service Pack 1, vari Windows Update, una schiera di applicazioni e tutte le personalizzazioni (senza contare il ripristino dei backup della posta e dei dati) se il problema dovesse ripetersi.

Per far fronte a errori che possono impedire il funzionamento di Windows, come la corruzione del registro, è stata adottata una strategia a più livelli, in modo da proteggere l'installazione qualunque cosa accada. Premettiamo che erano in funzione firewall e antivirus e che gli errori non erano imputabili ad attacchi provenienti dall'esterno.

Strategia di difesa

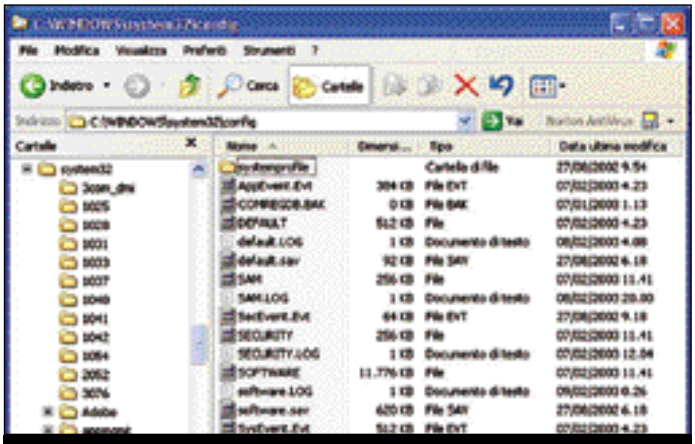
Le misure di salvaguardia messe in campo sono state:

1) tenere libera una partizione da 5 GB per salvare periodicamente un'immagine completa dell'installazione (Windows più applicazioni)

2) installare **Drive Image 2002** (utility per creare l'immagine delle partizioni) e creare i due floppy di emergenza per l'esecuzione in DOS

3) impostare l'esecuzione automatica quotidiana del backup dello stato del sistema, che include i file di registro. Questo si aggiunge a operazioni standard come la periodica verifica del disco con Chkdsk e la frequente deframmentazione dei dischi.

La partizione libera era già stata creata sul disco prevedendo la necessità di un'area di servizio per scambi di dati o per un'installazione parallela di Windows, che in certe situazioni permette di riparare l'installazione principale e di recuperare i dati dal disco. In assenza di una partizione libera si può utilizzare una partizione di lavoro con qualche gigabyte libero. Se il disco ha una sola partizione, che è la situazione più sfavorevole per poter fare manutenzione, si può utilizzare un secondo disco o creare una nuova partizione con **PartitionMagic** o un'utility equivalente. Naturalmente non si può creare il file immagine di una partizione nella stessa partizione da copiare. Drive Image 2002, in ogni caso, è in grado di restringere la partizione da salvare e di creare una partizione di backup, senza dover ricorrere a PartitionMagic.



La directory WINDOWS\system32\config contiene la maggior parte dei file del registro (tutti i dati tranne le informazioni relative agli utenti)

Drive Image 2002 funziona in Windows, ma non può creare un'immagine della partizione di sistema o di avvio con Windows in funzione; per copiare l'immagine della partizione dove è installato Windows, Drive Image programma un boot in DOS. Se per qualche motivo questo riavvio in DOS non dovesse funzionare, si utilizzano i due floppy di emergenza creati durante l'installazione di Drive Image. Con i due dischetti si possono fare le operazioni di copia e ripristino di immagini, anche su dischi SCSI. Nel caso i file immagine fossero in rete, Drive Image è in grado di produrre una coppia di dischetti per il salvataggio e ripristino in rete, ma il loro utilizzo non è alla portata di tutti gli utenti.

Con Drive Image viene installato anche **Image Explorer**, un'utility che permette di vedere i contenuti di un file immagine, verificarne l'integrità ed estrarre singoli file dall'immagine (inclusi i file del registro).

Nella nostra strategia difensiva, dopo aver installato Windows e poche applicazioni fondamentali, salviamo un'immagine della partizione di sistema (o anche di più partizioni) con Drive Image; dopo di che, qualsiasi cosa accada, saremo in grado di ripristinare l'intera installazione in meno di un'ora. Se la situazione è grave (Windows instabile ed errori in agguato), converrà fare diversi backup della partizione man mano che si installano le applicazioni, così da mettere al sicuro il lavoro fatto mentre si cerca di risolvere il problema.

Backup

Dopo aver creato la prima immagine dell'installazione, provvediamo a proteggere i file di registro. Dato che non possiamo copiarli con Windows aperto, scegliamo uno dei tanti modi per farne la copia. Il più semplice per l'utente è utilizzare l'utility **Backup di Windows** in modalità avanzata. Backup è una delle utility di sistema (si trova tramite il menu *Accessori*); per copiare i file di sistema occorre disattivare la modalità guidata, rientrare in modalità avanzata, scegliere *Backup guidato* e *Backup dello stato del sistema*. Sullo schermo finale della procedura, il bottone delle opzioni avanzate permette di specificare la sostituzione del backup precedente (altrimenti riempiamo il disco con tanti backup da 300 MB ciascuno) e ▷

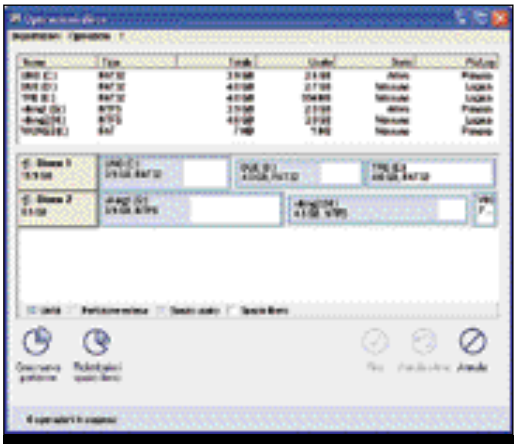
di programmare destinazione, data e periodicità del backup (consigliamo giornaliero, visto che richiede solo pochi minuti).

Il file generato dall'utility Backup con il nome che abbiamo specificato non è il vero obiettivo di questa operazione, perché il suo ripristino richiede l'uso della stessa utility, utilizzabile solo se Windows funziona. In realtà eseguiamo Backup per un suo sottoprodotto: la copia fisica dei principali file di registro nella directory *WINDOWS\repair*.

A questo punto, se si rovina un file del registro, lo sostituiamo con questa copia di backup, dopo di che Windows riparte e possiamo decidere di eseguire *Ripristino configurazione* di sistema per avere una configurazione integra e coerente. Con tutta probabilità possiamo utilizzare l'ultimo punto di ripristino per riportare Windows a una situazione recente e funzionante; in caso di problemi il ripristino è reversibile e si può scegliere un punto di ripristino precedente. Nel 12% di partizione riservato per default ai punti di ripristino possono starci anche due mesi di copie dei file di sistema (su partizioni NTFS i file di ripristino sono compressi).

Drive Image 2002 è il programma più potente e facile da usare per creare l'immagine delle partizioni

Se il disco contiene una sola partizione, Drive Image 2002 crea lo spazio per il file immagine



Drive Image include alcune funzioni di PartitionMagic per la gestione delle partizioni

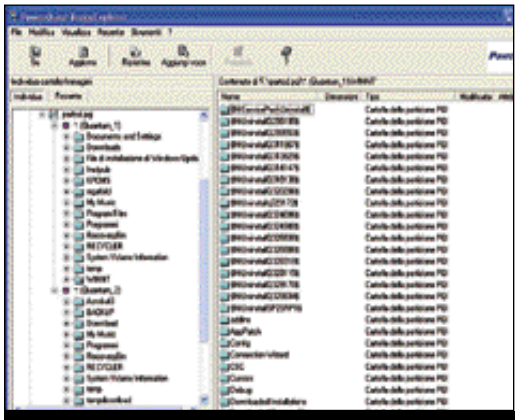


Image Explorer, fornito insieme a Drive Image 2002, permette di esplorare le immagini delle partizioni e di estrarne i file componenti

Sostituire i file di registro

Per completare il discorso manca un punto chiave: come sostituire il file di registro corrotto con la copia fatta in *WINDOWS\repair*. Se sul computer è disponibile una seconda installazione di Windows, basta un drag and drop per trasferire il file in pochi istanti. In caso contrario utilizziamo la *Console di ripristino di emergenza*, un ambiente con interfaccia in modo testo (tipo DOS) e una serie di comandi non molto diversi da quelli che si usano nella finestra prompt di Windows. Ci procuriamo il CD di installazione di Windows XP, lo inseriamo nel drive e riavviamo il computer come se volessimo reinstallare Windows; dopo qualche minuto di copia dei file di base, compare un menu che propone di installare Windows o di premere *R* per riparare un'installazione esistente.

Scegliamo la seconda strada; dopo aver premuto R viene chiesto a quale installazione si desidera accedere (inserire il numero, 1 se ce n'è una sola) e la password dell'utente Administrator, dopo di che la Console si mette in attesa dei comandi. I comandi che dobbiamo usare, simili a quelli del DOS, si limitano a Cd per cambiare directory, Ren per cambiare nome al file di registro corrotto in Windows\system32\config e Copy per copiare il file di backup dalla directory WINDOWS\repair a quella WINDOWS\system32\config. Con Dir potete elencare i contenuti di una directory. Per vedere la sintassi di un comando basta digitare il nome del comando seguito da /? (per esempio copy /?).

Il prompt mostra la lettera della partizione e il nome della directory di Windows, nel caso più semplice C:\WINDOWS. Supponendo di sostituire il file SYSTEM di registro, la sequenza dei comandi sarebbe:

```
Cd system32\config
Ren SYSTEM SYSTEM.KO
Copy \WINDOWS\repair\SYSTEM
Exit
```

Quando si digita Exit la Console di ripristino si chiude e il sistema viene riavviato. Se il file di registro corrotto era l'unico problema, Windows si avvierà regolarmente e come tocco finale si potrà eseguire il Ripristino configurazione di sistema. Quello che vale per un file vale per tutti i file di registro; se lo si desidera si possono rinominare i vecchi DEFAULT, SAM, SECURITY, SOFTWARE e SYSTEM e sostituirli con gli omonimi file salvati da Backup in WINDOWS\repair; questo è superfluo se eseguite il ripristino della configurazione (che sostituisce il registro), ma è una buona idea se preferite riparare il registro ed evitare il ripristino. In ogni caso è utile eseguire un'utility di controllo e correzione dell'integrità del registro, come WinDoctor delle Norton Utilities.

La copia della partizione in un file immagine può richiedere anche un'ora, mentre per il backup dello stato del sistema bastano quattro minuti. Quindi la prima può essere eseguita di tanto in tanto, in un orario in cui la macchina può restare fuori servizio. Il backup quotidiano dei file di registro invece è automatico e non impedisce l'uso del sistema, anche se forse è meglio non agitare troppo le acque mentre vengono copiati, in tempo reale, i contenuti del registro.

La workstation funziona

Che ne è stato della workstation? Dopo averla attrezzata come descritto sopra e aver completato l'installazione delle applicazioni, è tornata in uso a pieno ritmo e, dopo un paio di giorni, si è ripetuto l'errore sul file SYSTEM, come sempre tra uno spegnimento e una riaccensione del computer. Abbiamo sostituito il file come descritto sopra ed eseguito Ripristina *configurazione di sistema* utilizzando l'ultimo punto di ripristino e Windows ha funzionato regolarmente.

Per cercare una soluzione alla corruzione del registro abbiamo disabilitato la cache in scrittura sul disco SCSI nella

sezione *Criteri* della finestra *Proprietà del disco*. In questo modo Windows esegue fisicamente ogni scrittura su disco prima di passare all'istruzione successiva; le prestazioni potrebbero essere leggermente inferiori, ma con un disco molto veloce dotato di 8 MB di cache interna non lo si nota, mentre si ottiene invece un funzionamento più affidabile. Di fatto, a distanza di parecchi giorni, non si è più verificata la corruzione del registro.

Salvagente

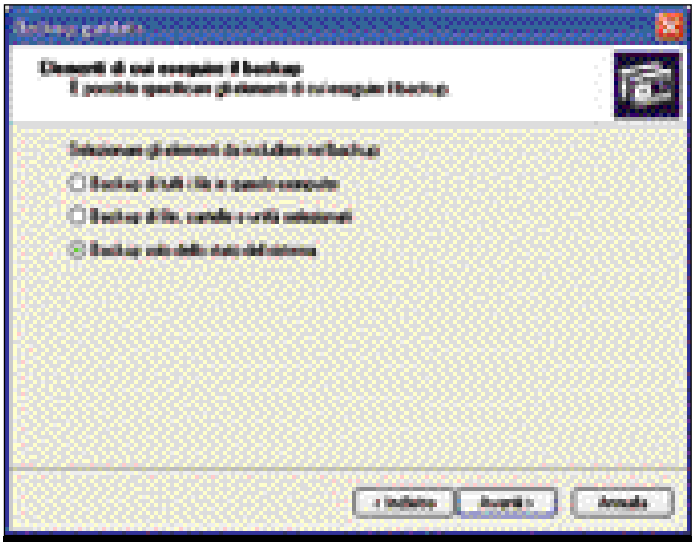
Supponiamo che abbiate letto questo articolo e che, prima di decidere se metterlo in pratica o no, un mattino Windows XP vi dia il benvenuto con un messaggio del tipo: "Windows non ha potuto essere avviato perché il seguente file è assente o corrotto: \WINDOWS\system32\config\SYSTEM".

Il nome del file nel messaggio potrebbe essere SOFTWARE e anziché questo messaggio potrebbe uscire un errore Stop c0000218 (Registry File Failure), ma il significato è lo stesso: il registro è stato corrotto.

Microsoft ha scritto che un danno al registro spesso accade quando i programmi che accedono al registro non rimuovono completamente le voci temporanee che vi creano, una situazione che si verifica anche quando un programma viene fatto abortire (chiudendone il processo) o incappa in un errore che lo blocca. Il rimedio segnalato da Microsoft, applicare il Service Pack 1, ha dimostrato di non risolvere il problema, per lo meno nel nostro caso.

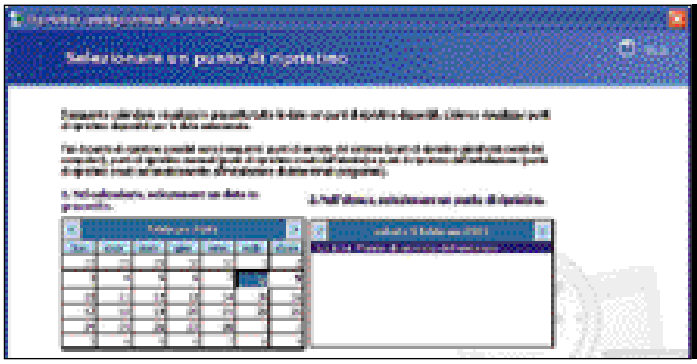
Ebbene, se in futuro trovate il registro corrotto e non ne avete tenuto i backup periodici, è ancora possibile recuperare il sistema (purché la funzione Ripristino configurazione di sistema non sia stata disattivata), solo che la procedura è piuttosto laboriosa ed è troppo lunga per essere qui riportata. La trovate nell'articolo 307545 della Knowledge Base Microsoft, "How to Recover from a Corrupted Registry that Prevents Windows XP from Starting", http://support.microsoft.com/default.aspx?scid=kb;en-us;307545.

Inutile dire che è di gran lunga più facile programmare il backup automatico dello stato del sistema. ■

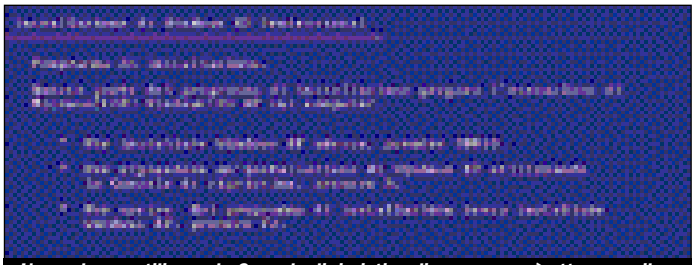


L'utility Backup permette di salvare lo stato del sistema (comprendente i file del registro)

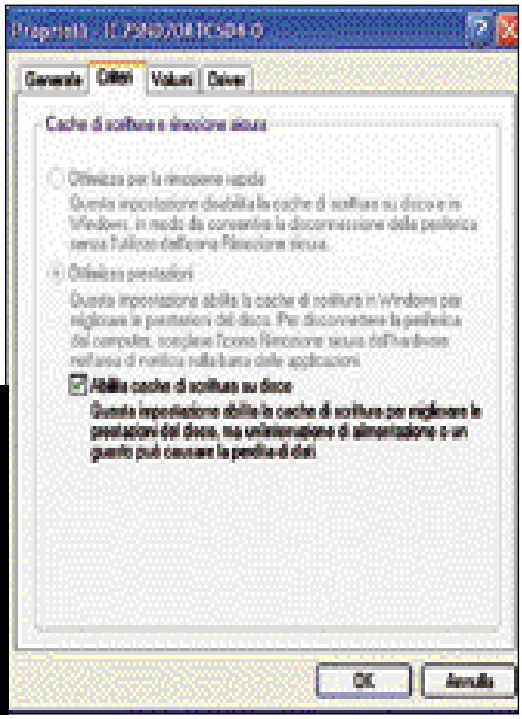
Il backup dello stato del sistema occupa 370 MB e richiede meno di quattro minuti



L'utility Ripristino configurazione di sistema permette di scegliere quale punto di ripristino utilizzare tra quelli disponibili



Un modo per utilizzare la Console di ripristino di emergenza è attraverso il CD di installazione di Windows, rispondendo R quando appare questo schermo



La sezione Criteri delle Proprietà del disco permette di disabilitare la cache in scrittura dell'hard disk se si ha motivo di credere che riduca l'affidabilità del sistema

▶ Dentro Windows

Registro di sistema: la chiave HKEY_LOCAL_MACHINE

È fra le Key principali del registry e descrive ogni particolare delle configurazioni hardware e software del computer. Vediamone le caratteristiche in dettaglio

di Giorgio Gobbi

articoli sul CD n. 71

Dei cinque "hive" (alveari) o root key (chiavi principali o radice) che formano la struttura gerarchica del registro di sistema (qui ci riferiamo al registro di Windows XP), due sono quelli principali: HKEY_LOCAL_MACHINE e HKEY_USERS. Gli altri tre (HKEY_CLASSES_ROOT, HKEY_CURRENT_USER e HKEY_CURRENT_CONFIG) sono alias di altrettante sottochiavi dei primi due, utilizzate per comodità di accesso, viste le dimensioni e la complessità della struttura.

Mentre HKEY_USERS contiene le informazioni riguardanti tutti gli utenti locali per cui è definito un account e un profilo, HKEY_LOCAL_MACHINE contiene una grande massa di informazioni sulla composizione hardware e software del sistema (indipendentemente dagli utenti), più due sezioni di informazioni sulla sicurezza (legate agli utenti).

La chiave HKEY_LOCAL_MACHINE contiene cinque sottochiavi: HARDWARE (creata ogni volta che viene avviato il sistema, contiene la descrizione dei dispositivi installati e informazioni relative ai device driver e alle risorse associate); SAM (*Security Account Manager*, informazioni su utenti e gruppi e sottosistemi di sicurezza, non visibili e non modificabili dagli editor di registro come Regedit); SECURITY (criteri locali di sicurezza, anch'essi non visibili e non modificabili da editor); SOFTWARE (informazioni su tutti i programmi installati e relative impostazioni) e SYSTEM (informazioni che controllano l'avvio di Windows, la sequenza di caricamento dei driver e dei servizi di sistema e altre informazioni sul comportamento del sistema operativo). Vediamo queste cinque sezioni una per una.

HARDWARE

La chiave HKEY_LOCAL_MACHINE\HARDWARE contiene la descrizione dell'hardware rilevato durante l'avvio di Windows; tutte queste informazioni vengono perdute quando si chiude il sistema. Sui computer dotati di un BIOS ACPI (*Advanced Configuration and Power Interface*) compatibile, Windows XP offre il supporto integrato per la gestione del Plug and Play e dell'alimentazione dei sottosistemi hardware (risparmio energetico).

Durante l'avvio, il sistema operativo verifica la presenza del BIOS ACPI e in caso affermativo l'ACPI è abilitato; in caso negativo viene disabilitato l'ACPI e abilitato il vecchio e meno affidabile APM (*Advanced Power Management*). In presenza di supporto ACPI viene caricato il corrispondente HAL (*Hardware Abstraction Layer*), che determina il caricamento del driver ACPI, interfaccia tra il sistema operativo e il BIOS.

Se il sistema è dotato di BIOS ACPI compatibile con Windows XP, la prima sottochiave di HKEY_LOCAL_MACHINE\HARDWARE è ACPI; in caso contrario (per esempio sui PC con ACPI compatibile solo con Windows 98), questa chiave è assente. Le informazioni nella chiave ACPI sono binarie e quindi praticamente incomprensibili per gli utenti.

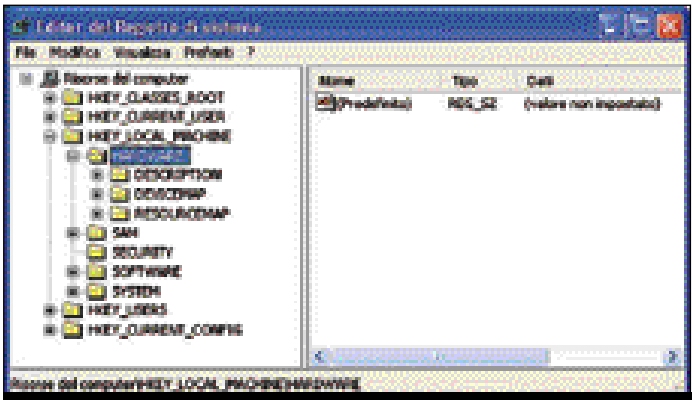
La seconda sottochiave di HKEY_LOCAL_MACHINE\HARDWARE è DESCRIPTION, che contiene dati raccolti da Ntdetect.com e da Ntoskrnl.exe durante l'avvio di Windows. Queste informazioni includono identificatore del computer, tipi di bus, tastiera, mouse, porte seriali e parallele, drive, controller, adattatore video, coprocessore aritmetico e altro.

La terza sottochiave di HARDWARE è DEVICEMAP, le cui sottochiavi contengono informazioni sui device driver richiesti da ogni dispositivo. Queste informazioni spesso fanno riferimento a voci contenute nella chiave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet.

La quarta sottochiave di HARDWARE è RESOURCEMAP, che contiene informazioni sulle risorse di sistema allocate a ciascun dispositivo (incluse porte, indirizzi DMA e IRQ). Dato che queste informazioni sono codificate in modo compatto, sono pressoché indecifrabili; per consultarle e modificarle l'utente può usare l'utility *Gestione Periferiche* (Start, clic destro su *Risorse del computer*, *Gestione*, *Gestione Periferiche*).

SAM e SECURITY

Le informazioni contenute in queste due sottochiavi, relative a utenti, gruppi, diritti di accesso, criteri (policy) relativi



Il sottoalbero HARDWARE contiene la descrizione dell'hardware rilevato durante l'avvio di Windows; queste informazioni vengono perdute alla chiusura di Windows

Le puntate precedenti

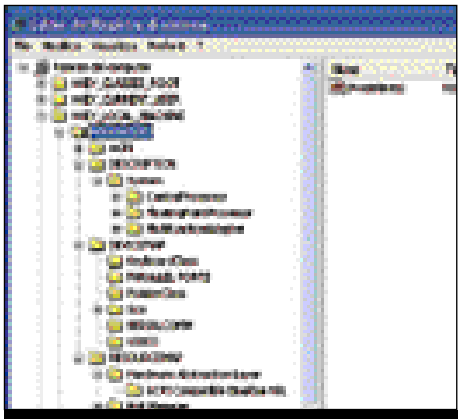
1 - **Un registro per tenere il sistema sotto controllo**, PC Open, aprile 2002

2 - **Il backup del registro di sistema**, PC Open, giugno 2002

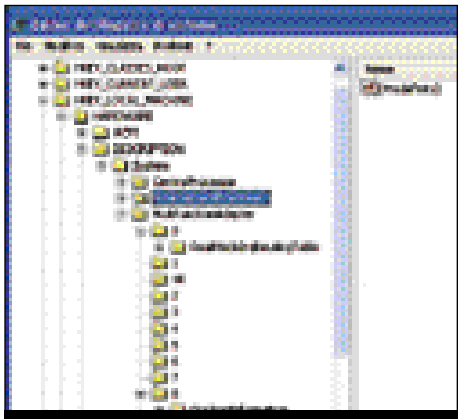
3 - **Windows XP, registro e dintorni**, PC Open, dicembre 2002

4 - **Configurare al meglio il registro di Windows XP**, PC Open, marzo 2003

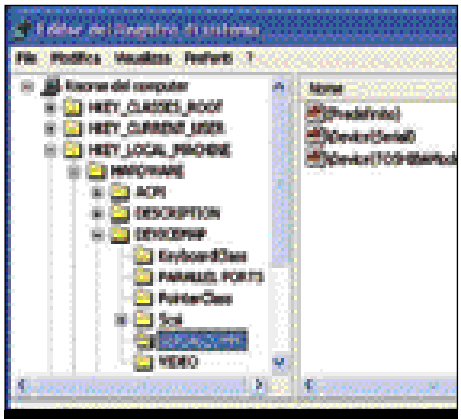
5 - **Ripristinare i file del registro**, PC Open, aprile 2003



Le sottochiavi di HARDWARE contengono le informazioni sui sottosistemi della scheda madre e sulle periferiche collegate



La sottochiave DESCRIPTION contiene i dati raccolti da Ntdetect.com e da Ntoskrnl.exe durante l'avvio del sistema



La sottochiave DEVICEMAP contiene informazioni sui device driver richiesti dai dispositivi hardware

all'uso delle password, appartenenza a gruppi e altro, non sono né visibili né modificabili da Regedit. Per consultare e modificare queste informazioni gli utenti del gruppo Administrators utilizzano le utility di Windows, come Utenti e gruppi locali in Gestione computer e Criteri di protezione locali in Strumenti di amministrazione, che hanno un'interfaccia amichevole e facilmente comprensibile.

SOFTWARE

La sottochiave HKEY_LOCAL_MACHINE\SOFTWARE contiene un gigantesco database con le informazioni sulle applicazioni installate sul computer e relative impostazioni di configurazione. Come per la chiave HARDWARE, si tratta di informazioni valide per tutti gli utenti del PC. Tra le sottochiavi di SOFTWARE, si notano, mescolate insieme, le chiavi standard che fanno parte della struttura del registro e le chiavi delle applicazioni, che hanno i nomi dei rispettivi produttori. Segnaliamo in particolare le sottochiavi Classes, Clients, Microsoft, ODBC, Policies, Program Groups, Secure e Voice. Non basterebbe un intero libro per descrivere in dettaglio questa sezione del registro, perciò cominceremo con l'introdurre l'argomento, riservandoci qualche approfondimento nelle prossime puntate di questa rubrica.

Classes

La sottochiave Classes contiene le stesse voci presentate come alias nella root key HKEY_CLASSES_ROOT. Le sottochiavi sono due tipi; quelle di tipo estensione-file associano le applicazioni installate sul computer con i tipi dei file, identificati dalle rispettive estensioni. Queste associazioni sono visibili e modificabili tramite *Opzioni cartella* nel menu *Strumenti* di *Esplora risorse*.

Le sottochiavi di tipo definizione-classe contengono informazioni associate a oggetti COM. COM (*Component Object Model*) è un'architettura Microsoft per costruire applicazioni basate su componenti software; ogni oggetto COM ha un'identità unica e mostra le proprie interfacce in modo da essere accessibile da altri componenti e applicazioni. Il modello COM supera l'iniziale versione di OLE (*Object Linking and Embedding*) e il relativo meccanismo DDE (*Dynamic Data Exchange*) di comunicazione tra processi, fornendo meccanismi più flessibili, indipendenti dal linguaggio e già abilitati alla comunicazione tra processi. I dati contenuti nella seconda parte di Classes specificano quindi informazioni che hanno a che fare con la struttura dei programmi, le loro interfacce e i legami con altri moduli. Queste informazioni sono create da programmi appositi con supporto COM e di solito non sono modificate via editor.

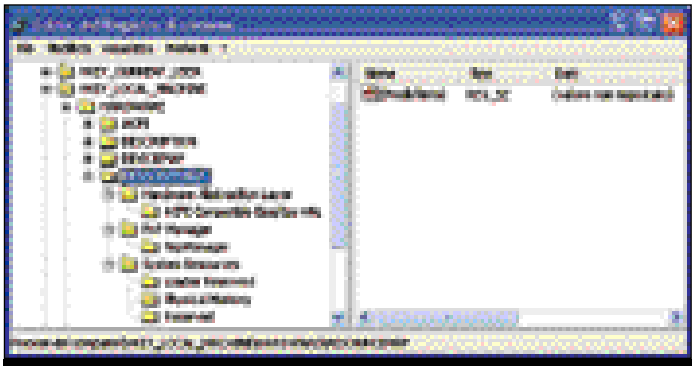
Clients

HKEY_LOCAL_MACHINE\SOFTWARE\Clients contiene informazioni su relazioni client-server e in particolare le informazioni utilizzate da Windows per servizi di posta elettronica e associati. Vi si trovano diverse sottochiavi utilizzate da Outlook e da Outlook Express, come Calendar, Contacts, Mail e News, più ulteriori sottochiavi utilizzate da altre applicazioni Microsoft come Office, Internet Explorer, Messenger e Media Player.

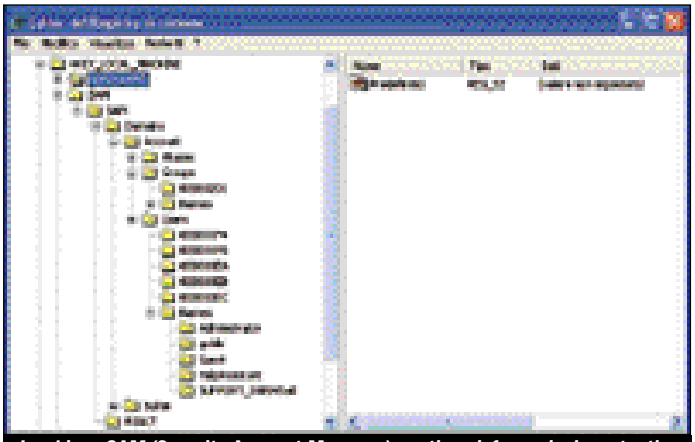
Microsoft

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft è l'elemento più voluminoso della chiave SOFTWARE, visto il numero dei componenti descritti. Una delle sue sottochiavi di maggiore importanza è HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion, che contiene informazioni sul tipo di installazione e sul software che supporta i servizi di sistema.

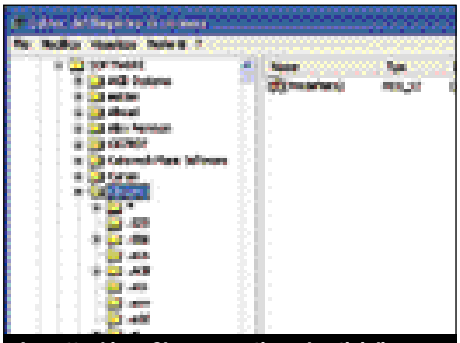
Tre sottochiavi di Microsoft\Windows NT\CurrentVersion particolarmente utili per i ▷



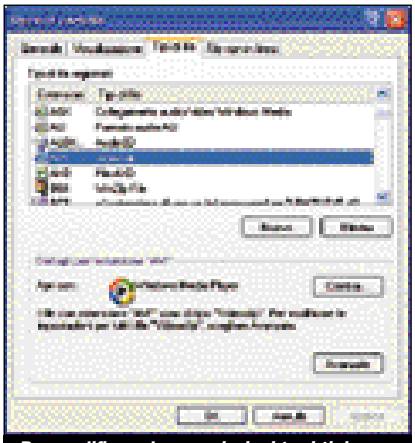
La sottochiave RESOURCEMAP contiene informazioni sulle risorse di sistema allocate ai device, come porte, indirizzi DMA e IRQ



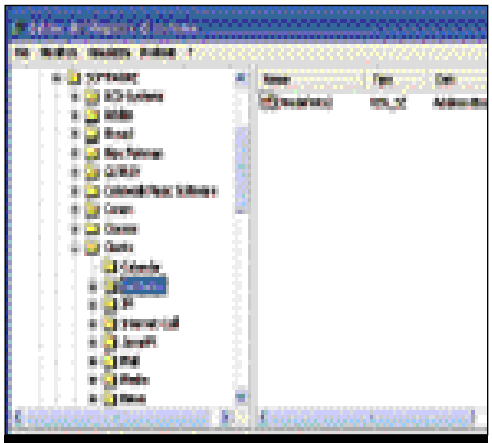
La chiave SAM (Security Account Manager) contiene informazioni su utenti e gruppi, ma non in un formato visibile e modificabile da un editor di registro come Regedit



La sottochiave Classes contiene due tipi di impostazioni; quelle di tipo estensione-file sono le associazioni tra i tipi di file e le applicazioni installate, mentre quelle di tipo definizione-classe contengono informazioni associate a oggetti COM (Component Object Model, architettura Microsoft per costruire applicazioni tramite componenti software)



Per modificare le associazioni tra i tipi di file e i programmi si usa la sezione Tipi di file di Opzioni cartella in Risorse del computer



La sottochiave Clients di SOFTWARE contiene perlopiù informazioni utilizzate per i servizi di posta elettronica

sistemisti sono: HotFix con sottochiavi per ogni patch installata via Windows Update, ProfileList con una sottochiave per ogni profilo utente e Winlogon contenente valori che definiscono il processo di logon, incluso il nome dell'ultimo utente collegato.

ODBC

HKEY_LOCAL_MACHINE\SOFTWARE\ODBC contiene informazioni riguardanti la Open Database Connectivity, che permette ai programmi di accedere ai dati contenuti nei database di altre applicazioni.

Esempi di driver ODBC comuni sono quelli per Access, Oracle, SQL Server, FoxPro e dBase.

Policies

La sottochiave HKEY_LOCAL_MACHINE\SOFTWARE\Policies contiene impostazioni per le conferenze in Rete e per i certificati di sistema.

Program Groups

HKEY_LOCAL_MACHINE\SOFTWARE\Program Groups contiene la sola voce ConvertedToLinks, che indica se i gruppi di programmi esistenti in una versione precedente di Windows sono stati convertiti in occasione dell'aggiornamento a XP. Se Windows XP è stato installato da zero, Program Groups non ha sottochiavi.

Secure

Poco documentata, la sottochiave HKEY_LOCAL_MACHINE\SOFTWARE\Secure è utilizzabile dalle applicazioni per memorizzare impostazioni modificabili solo da utenti amministratori.

Voice

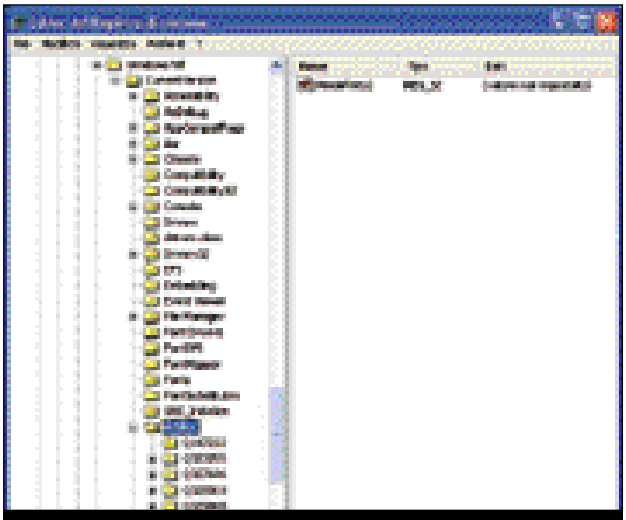
La sottochiave Voice contiene informazioni sul motore testo-voce di Windows XP; non è presente in tutte le installazioni.

SYSTEM

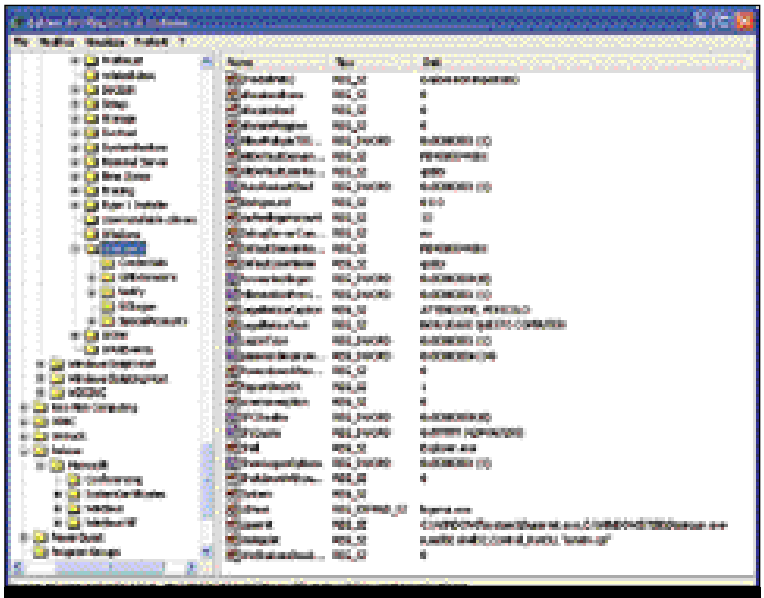
La chiave HKEY_LOCAL_MACHINE\SYSTEM contiene informazioni riguardanti l'avvio del sistema, l'ordine di caricamento dei device driver e dei servizi di sistema e comportamenti del sistema operativo. In SYSTEM sono contenuti i dati che il sistema deve trovare pronti durante l'avvio, anziché rilevarli o calcolarli come avviene per altre sezioni del registro. Questi dati sono organizzati sotto forma di Control Set (insiemi di controllo), che contengono un insieme completo di impostazioni dei device driver e dei servizi di sistema.

Durante la sequenza di boot (avvio) di Windows, dopo la selezione del sistema operativo da avviare (se ci sono più OS installati), segue la selezione del profilo hardware da utilizzare (se ce n'è più di uno) e la possibilità di avviare Windows con l'opzione Ultima configurazione valida (Last Known Good Configuration).

Già a questo punto viene letta la chiave SYSTEM per indivi-



La chiave SOFTWARE\Microsoft contiene un'enorme quantità di dati; in questo esempio si vede che HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\HotFix tiene traccia delle patch installate attraverso Windows Update



Winlogon, un'altra sottochiave di SOFTWARE\Microsoft, contiene informazioni utilizzate durante il logon dell'utente

duare, in HKEY_LOCAL_MACHINE\SYSTEM\Select, qual è, tra i Control Set presenti nel registro, quello corrispondente all'ultima configurazione valida, le cui informazioni sono state registrate subito dopo l'ultimo boot regolare di Windows.

Durante l'avvio di Windows, dopo che il boot loader (NTLDR) si è procurato le informazioni sull'hardware installato e sul profilo hardware selezionato (il più delle volte c'è solo quello di default), fa partire il kernel di Windows (Ntoskrnl.exe) passandogli le informazioni raccolte da Ntdetect.com, quindi carica l'hardware abstraction layer (HAL) corrispondente all'architettura hardware del PC corrente. A questo punto NTLDR carica la sezione SYSTEM di HKEY_LOCAL_MACHINE leggendola dal file WINDOWS\System32\Config\System.

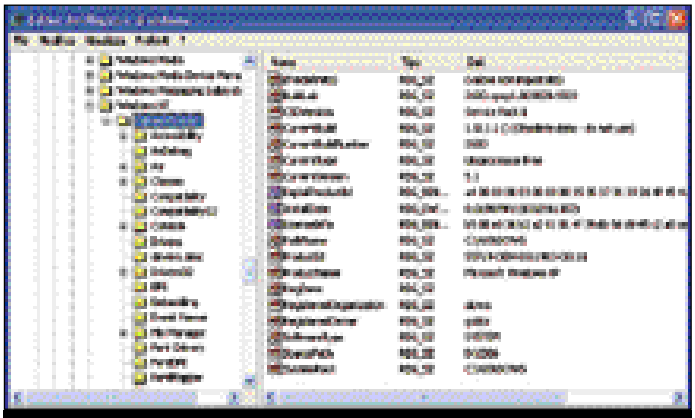
Ora il boot loader abilita l'interfaccia API con il registro e, in base alle impostazioni contenute nella chiave HKEY_LOCAL_MACHINE\SYSTEM\Select, determina qual è il Control Set da usare per avviare il sistema. Per default il loader utilizza il Control Set specificato in Default, ma se è stato richiesto l'uso dell'ultima configurazione valida verrà usato il Control Set specificato in LastGoodKnown. Negli esempi il Control Set di default è il numero 1, mentre quello corrispondente all'ultima configurazione valida è il numero 3.

Una volta stabilito qual è il Control Set da usare, il loader lo copia nella chiave CurrentControlSet ed esegue una scansione di HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services alla ricerca dei device driver con un valore Start di 0x0, che contrassegna i driver da caricare. Questi sono normalmente driver di basso livello, come quelli per gli hard disk. Il valore dell'impostazione Group per ogni device driver stabilisce l'ordine di caricamento, secondo la sequenza definita nella chiave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ServiceGroupOrder. In questa lunga lista, con oltre 60 categorie di driver, gli hard disk si trovano vicino ai primi posti.

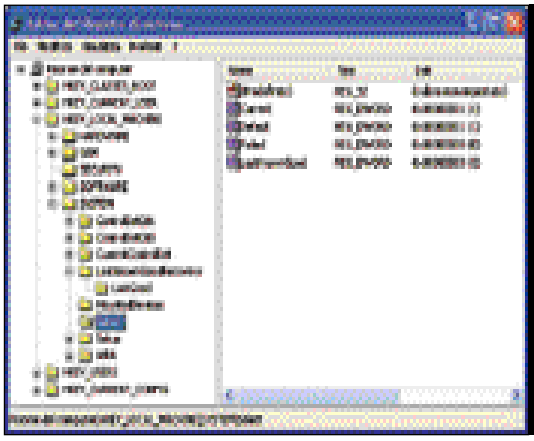
Control Set

Ogni Control Set contiene quattro sottochiavi. La prima è Control, che contiene le numerose impostazioni di configurazione utilizzate per la gestione del sistema, inclusi il nome con cui il computer è identificato nella rete e i sottosistemi da avviare. Tra queste informazioni ci sono i parametri di avvio di Windows, le variabili di sistema e le dimensioni e ubicazione del file di paging.

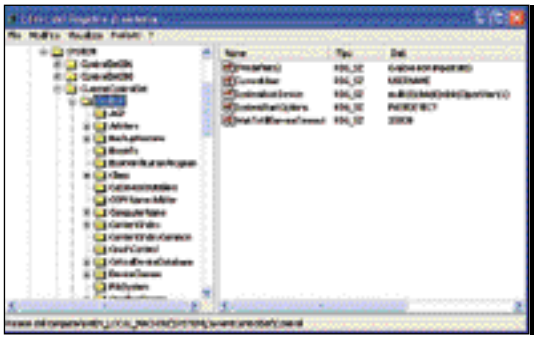
La sottochiave Enum (da enumeration, l'assegnazione di ▷



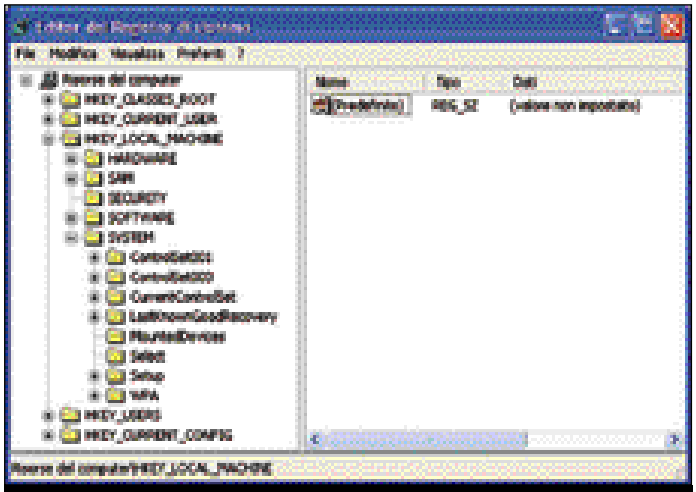
La chiave HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion contiene le informazioni di base sull'installazione di Windows e numerose sottochiavi



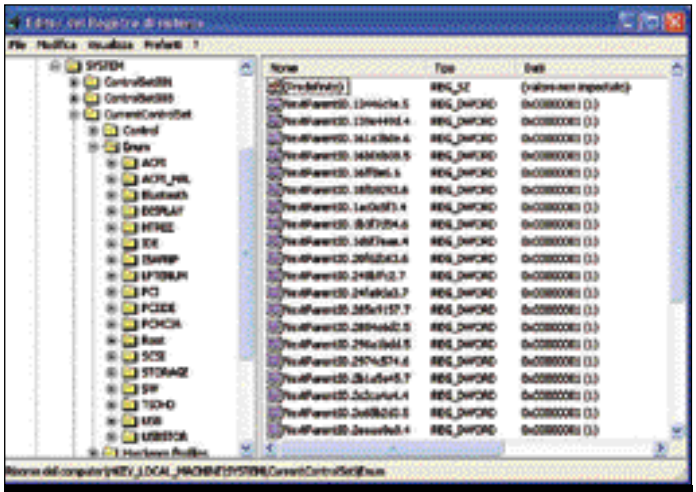
La sottochiave Select identifica quali sono i Control Set disponibili; in questo caso quello corrente è il numero 1, quello di default, mentre quello da usare come Ultima configurazione valida (Last Known Good Configuration) è il numero 3



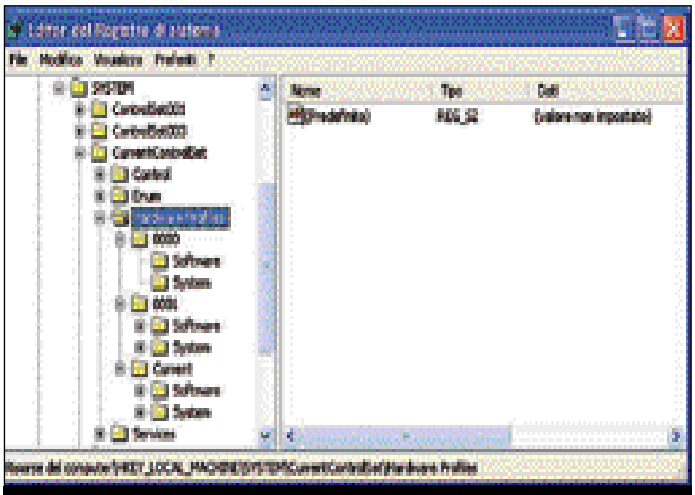
La sottochiave Control dei Control Set contiene numerose impostazioni di configurazione utilizzate per la gestione del sistema



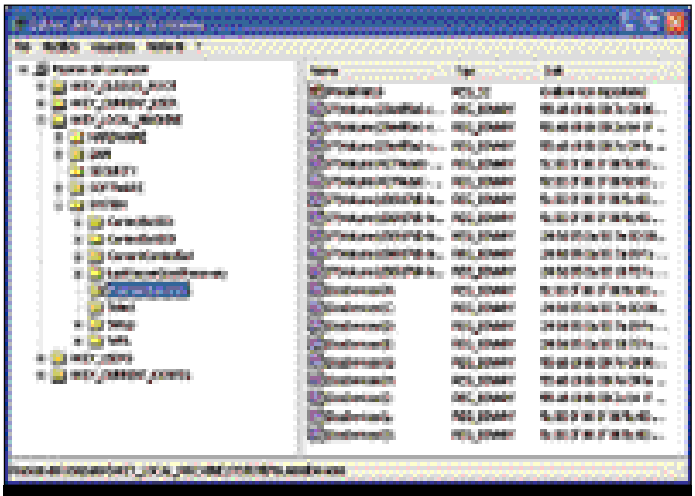
SYSTEM è l'ultima delle suddivisioni di HKEY_LOCAL_MACHINE e contiene informazioni vitali sull'avvio del sistema, il caricamento di driver e servizi e altre operazioni; il grosso di queste informazioni è incluso nei Control Set



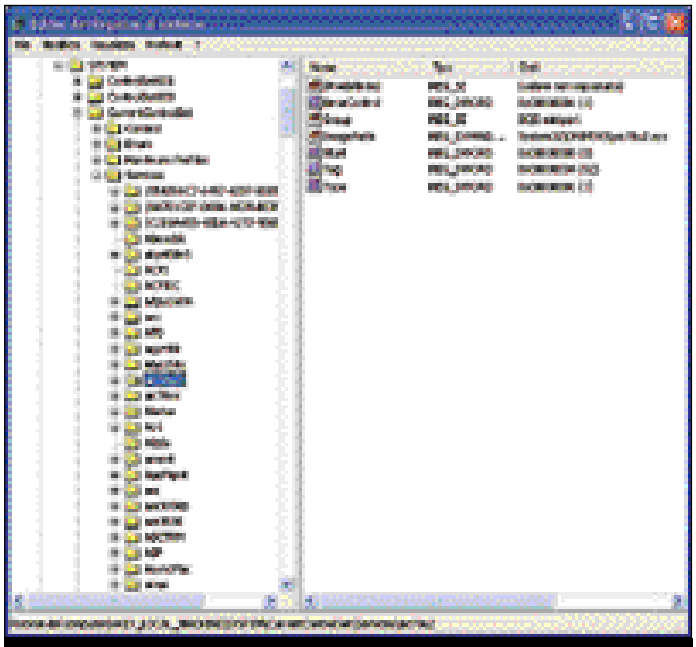
La sezione Criteri delle Proprietà del disco permette di disabilitare la cache in scrittura dell'hard disk se si ha motivo di credere che riduca l'affidabilità del sistema



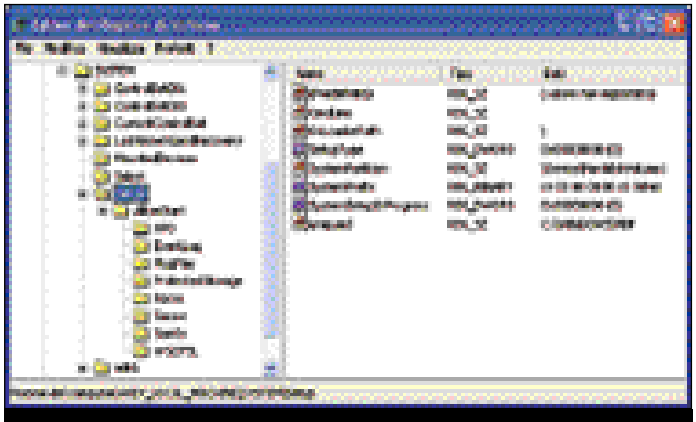
I profili hardware (in questo caso due) sono descritti, per differenza con quello di default, nella sottochiave Hardware Profiles dei Control Set



Tra le informazioni contenute SYSTEM, la sottochiave MountedDevices mostra tutti i drive accessibili, anche in Rete



La sottochiave Services dei Control Set elenca i device driver, i driver di file system e programmi di servizio; sono indicati tra l'altro i driver da caricare e l'ordine di caricamento



Altre sottochiavi di SYSTEM: Select indica i Control Set disponibili, Setup conserva informazioni relative all'installazione di Windows e WPA contiene dati sull'attivazione di Windows XP

un numero ai dispositivi rilevati su ciascun bus) contiene dati di configurazione sui dispositivi hardware. Le sue sottochiavi formano una struttura gerarchica chiamata albero dei device, che inizia alla radice e termina alla fine dei rami inferiori, contenenti dati di configurazione per istanze specifiche di ogni tipo di dispositivo. Le sottochiavi di Enum sono Htree, che rappresenta l'alberatura hardware, e una sottochiave per ogni enumeratore (a cui corrisponde un bus) e i relativi device; la chiave Root corrisponde all'enumeratore di default, usato per i dispositivi non Plug & Play.

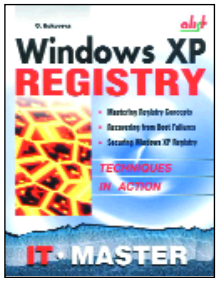
La chiave Harware Profiles contiene impostazioni hardware e configurazioni di driver relativi ai profili hardware (quello di default e quelli eventualmente definiti dall'utente); sono indicate solo le differenze rispetto alle impostazioni standard dei driver e dei servizi.

L'ultima sottochiave, Services, contiene un elenco di device driver, driver di file system e programmi di servizio eseguiti in user mode. Sono indicati i driver da caricare, l'ordine di caricamento e i metodi di chiamata tra i programmi. Le sottochiavi di HKEY_LOCAL_MACHINE\HARDWARE\DEVICEMAP fanno riferimento a voci contenute nella chiave Services dei Control Set. Per esempio sotto DEVICEMAP, nei raggruppamenti per categoria di periferica, c'è la sottochiave PointerClass di cui fa parte \Device \PointerClass0, il cui valore punta alla sottochiave HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Mouclass.

Sotto il ramo SYSTEM, dopo i Control Set e LastKnownGoodRecovery, si trova la chiave MountedDevices, che mostra i drive accessibili al sistema, inclusi quelli di Rete.

Seguono la chiave Select, che come abbiamo visto contiene i riferimenti ai Control Set, la chiave Setup, che conserva informazioni sull'installazione iniziale di Windows XP (da non modificare) e la chiave WPA che non è difficile indovinare serva per la Windows Product Activation (una sottochiave WPA è presente anche in CurrentControlSet\Control\Session Manager).

Qui termina, per il momento, questa sintetica panoramica su HKEY_LOCAL_MACHINE. Nei prossimi numeri di *PC Open* riprenderemo l'argomento considerando in maggiore dettaglio sezioni di particolare interesse. ■



Il libro Windows XP Registry di Oga Kokoreva (editore A-List) *è un buon punto di partenza per conoscere il registro di sistema*

▶ Dentro Windows

Registro di sistema, dalla parte degli utenti

Panoramica sulla sezione del registry che si occupa del profilo degli utilizzatori del personal computer

di Giorgio Gobbi

articoli sul CD Guida

Continuiamo nella descrizione panoramica, senza entrare troppo in dettaglio, degli hive (alveari o chiavi principali) che formano la struttura del registro di sistema di Windows XP. Sul numero di maggio abbiamo visto che HKEY_LOCAL_MACHINE (che include gli alias HKEY_CLASSES_ROOT e HKEY_CURRENT_CONFIG) costituisce il grosso del registro, con un'enorme massa di informazioni sulla composizione hardware e software del sistema (indipendentemente dagli utenti), più due sezioni di informazioni sulla sicurezza (legate agli utenti).

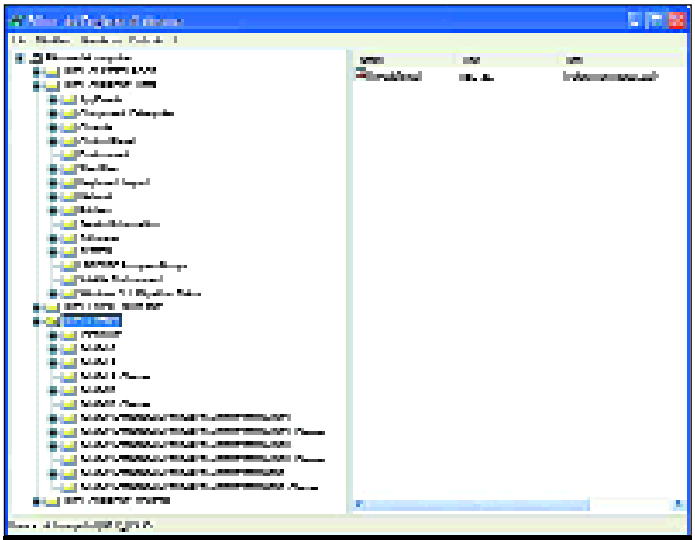
In questa occasione esploriamo la parte restante del registro, ovvero HKEY_USERS, che contiene i profili di tutti gli utenti attivi, incluse variabili di ambiente, impostazioni del desktop, impostazioni di rete e impostazioni applicative. La chiave HKEY_CURRENT_USER, contenente il profilo dell'utente correntemente connesso (logged-on) al sistema, non è altro che un puntatore alla sezione di HKEY_USERS che descrive l'utente corrente.

A differenza delle precedenti versioni di Windows, prive di un'architettura di protezione, Windows NT, 2000 e XP richiedono che ogni utente sia registrato, ovvero possegga un account che ne stabilisca l'identità e i privilegi. Un account utente (user account) è una registrazione contenente tutte le informazioni necessarie per la definizione di un utente in Windows. Queste informazioni includono il nome dell'utente e la password necessari per l'accesso al sistema, i gruppi a cui appartiene l'utente (per esempio *Users*, *Power Users*, *Administrators*) e i diritti e le autorizzazioni dell'utente per l'utilizzo del computer e della rete e per l'accesso alle relative risorse (dischi, directory, file, stampanti, e via dicendo).

In generale un utente possiede un account, una sorta di descrizione fiscale della sua identità e dei suoi diritti, e un profilo, che descrive la configurazione (le preferenze, il desktop, le connessioni di rete e via dicendo) utilizzata dall'utente per interagire con il sistema e con le applicazioni (dallo sfondo del desktop al cursore del mouse, alle preferenze di Internet Explorer e coì via). Gli account sono contenuti nel registro di sistema, mentre i profili si trovano per default nella partizione di sistema, sotto forma di sottoalberi della directory Documents and Settings che hanno i nomi degli utenti.

Se avete installato Windows XP in C:, troverete sotto *C:\Documents and Settings* una serie di directory predefinite (*Administrator*, *Default User*, *All Users*, *LocalService*, *NetworkService*) e le directory con i nomi degli utenti che avete definito voi.

Ora sappiamo qualcosa di utenti e account, ma non abbastanza per curiosare in HKEY_USERS, quindi introduciamo qualche altro concetto di base.



Come al solito, le chiavi e i valori del registro di sistema sono visti attraverso l'editor di registro Regedit, qui aperto sulle chiavi specifiche per gli utenti, HKEY_CURRENT_USER e HKEY_USERS; le sottochiavi che iniziano con S-1-5-21 si riferiscono agli utilizzatori del PC, mentre gli utenti S-1-5-18/19/20 sono servizi di sistema

Le puntate precedenti

1 - **Un registro per tenere il sistema sotto controllo**, PC Open, aprile 2002

2 - **Il backup del registro di sistema**, PC Open, giugno 2002

3 - **Windows XP, registro e dintorni**, PC Open, dicembre 2002

4 - **Configurare al meglio il registro di Windows XP**, PC Open, marzo 2003

5 - **Ripristinare i file del registro**, PC Open, aprile 2003

6 - **La chiave HKEY_LOCAL_MACHINE**, PC Open, maggio 2003

SID

Abbiamo visto che ogni profilo utente è riconoscibile perché la sua directory ha il nome dell'utente. Tuttavia Windows, al suo interno, fa riferimento agli utenti non per nome ma attraverso dei codici chiamati Security Identifier o SID, che in italiano vengono tradotti di solito come Identificatori di protezione. In effetti Windows non ha utenti soltanto in carne e ossa, ma anche oggetti software, come certi servizi di sistema.

In Windows XP qualunque entità soggetta ad autenticazione (la verifica che un'entità od oggetto sia colui o ciò che afferma di essere) si chiama Security Principal, che potremmo tradurre come soggetto di protezione (la traduzione principio di protezione che compare nella traduzione ▷

italiana di Windows XP Registry Guide di Microsoft Press è fuorviante). Nella definizione di Microsoft, un Security Principal è qualsiasi entità riconosciuta dal sistema di protezione e i soggetti di protezione includono sia utenti umani sia processi autonomi.

Tornando al SID, possiamo ora definirlo con maggiore precisione. Un SID è un valore di lunghezza variabile che identifica in modo univoco un utente, un gruppo, un servizio o un account. I meccanismi di controllo degli accessi in Windows XP identificano qualunque Security Principal (qualunque oggetto che abbia a che fare con il sistema di protezione) attraverso un SID. In un computer o in una rete, ogni account riceve un SID al momento della sua creazione e il meccanismo di assegnazione è tale da garantire l'unicità dell'identificatore nell'ambito del computer o del dominio (per le reti basate su domain server).

Se ora diamo un'occhiata alla finestra di Regedit, aperta su HKEY_USERS, vediamo la chiave .DEFAULT e un elenco di SID sotto forma di stringhe che iniziano per S e contengono gruppi di cifre separati da trattini, come per esempio S-1-5-21-2210005112-2826650621-2974146706-1004. La S iniziale indica che si tratta di un SID. La cifra successiva indica la versione di SID, che è solitamente 1. Le due cifre successive, separate da un trattino, rappresentano l'Authority (autorità identificatrice) e la Subauthority. Il più delle volte, l'Authority vale 5, che corrisponde all'autorità NT. In HKEY_USERS si può notare che i SID iniziano solitamente con S-1-5 e che si differenziano per i numeri successivi.

I SID standard per utenti e gruppi, descritti da Microsoft nell'articolo 243330 della Knowledge Base, sono parecchie decine, ma quelli che trovate in HKEY_USERS sono solo alcuni. Prima di vedere a chi appartengono, spendiamo qualche parola sulla chiave .DEFAULT.

HKEY_USERS\.DEFAULT

Questa chiave contiene le impostazioni di utente utilizzate da Windows XP prima che qualche utente esegua il logon. È un concetto diverso dal profilo utente di default, che viene utilizzato da Windows per creare le impostazioni utilizzate la prima volta che un utente esegue il logon.

HKEY_USERS\S-1-5-18

La Subauthority 18 identifica il SID dell'account LocalSystem, un account di servizio utilizzato dal sistema operativo. Il profilo di questo account viene caricato quando un programma o un servizio viene eseguito sotto l'account LocalSystem.

HKEY_USERS\S-1-5-19

Questa è la chiave che identifica l'account LocalService. Il Service Control Manager (gestore dei servizi) utilizza questo account per eseguire servizi locali che non richiedono l'esecuzione sotto LocalSystem.

HKEY_USERS\S-1-5-20

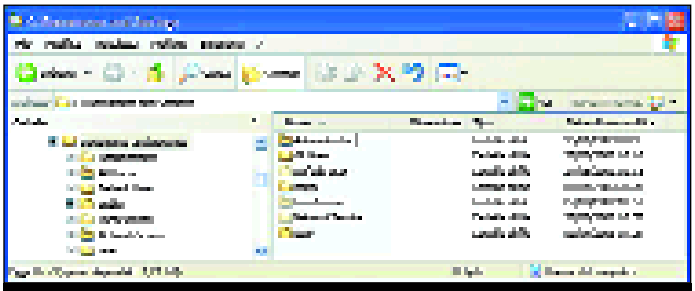
S-1-5-20 è il SID dell'account NetworkService, utilizzato per eseguire servizi di rete che non richiedono l'esecuzione sotto LocalSystem.

Gli account con SID S-1-5-18, S-1-5-19 e S-1-5-20 possono essere ignorati quando si cercano in HKEY_USERS informazioni riguardanti gli utenti umani.

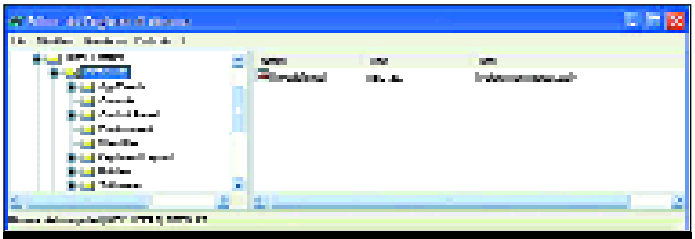
I SID degli utenti logged-on

Dopo i SID dei servizi di sistema, HKEY_USERS mostra i SID degli utenti in carne e ossa, solitamente identificati da un SID che inizia per S-1-5-21. Nelle illustrazioni trovate l'esempio di un'installazione con tre utenti, di cui uno è l'utente standard Administrator e altri due sono stati creati durante e dopo l'installazione di Windows XP.

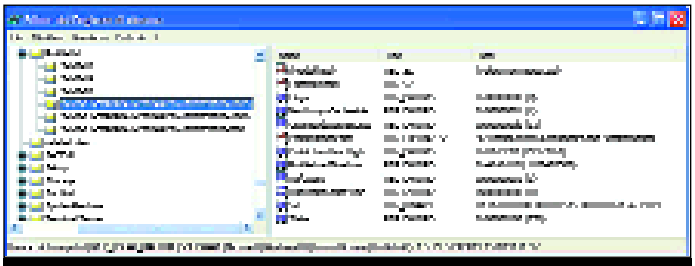
Nell'esaminare HKEY_USERS vediamo i SID ma non i nomi degli utenti, quindi ci serve un modo per associare gli uni agli altri. L'associazione tra i nomi degli utenti e i SID è contenuta nella chiave di registro HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList. Espandendo ProfileList, vediamo che le sue sottochiavi sono i SID di sistema e i SID degli utenti umani. I nomi degli utenti si trovano nel pannello di destra di Regedit come valori della voce ProfileImagePath.



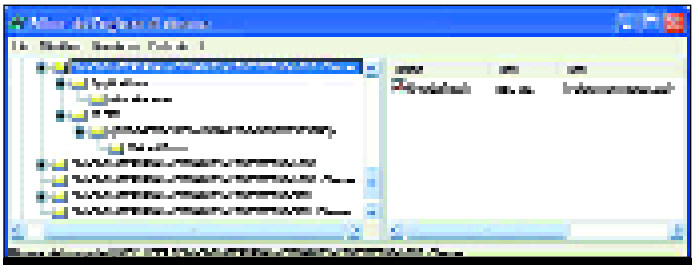
I profili degli utenti, che descrivono la configurazione utilizzata da ogni utente per interagire con il sistema e con le applicazioni, si trovano per default nella partizione di sistema, come sottoalberi della directory Documents and Settings



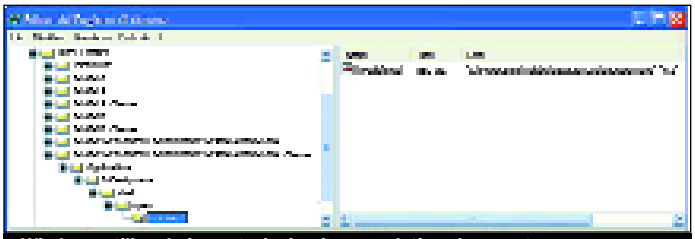
La chiave HKEY_USERS\.DEFAULT contiene le impostazioni di utente utilizzate da Windows XP prima che qualche utente esegua il logon



L'associazione tra i nomi degli utenti e i corrispondenti SID (Identificatori di protezione) è contenuta nella chiave di registro HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList



Le chiavi con il nome formato da un SID seguito da _Classes descrivono programmi associati a un utente e, nelle sottochiavi, includono caratteristiche e comportamenti del programma che si applicano all'utente specifico



Windows utilizza le impostazioni software relative al computer (HKEY_LOCAL_MACHINE\SOFTWARE\Classes) e quelle relative all'utente (SID seguito da _Classes) dando la priorità a queste ultime quando diverse da quelle generali

Gli utenti elencati in HKEY_USERS sono utenti attivi; se per esempio avete creato tre utenti ma uno solo è connesso (logged-on) al momento, vedrete solo questo. Tuttavia in HKEY_USERS compaiono anche gli utenti di cui qualche altro utente sta usando le credenziali per eseguire un'applicazione. Un esempio è il caso di un utente limitato (l'utente normale del gruppo Users) che esegue un'applicazione attraverso l'opzione Esegui come... (clic destro sul nome del programma) utilizzando nome utente e password di un utente con privilegi superiori. In questo caso anche l'utente che presta i propri privilegi compare nell'elenco degli utenti attivi di HKEY_ USERS.

Le chiavi con il nome formato da un SID seguito da _Classes, in HKEY_USERS, sono simili a quelle già viste in HKEY_LOCAL_MACHINE\SOFTWARE\Classes; descrivono programmi associati a un utente e, nelle sottochiavi, includono particolari caratteristiche e comportamenti del programma che si applicano all'utente specifico. Queste personalizzazioni hanno la precedenza su quelle analoghe contenute in HKEY_LOCAL_MACHINE\SOFTWARE\Classes; Windows mescola le due fonti di informazioni, con il vantaggio di poter definire contemporaneamente impostazioni comuni (per computer) e personalizzate (per utente).

Altri SID

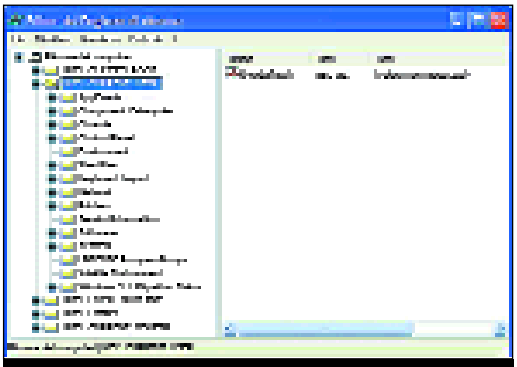
Rinviamo alla documentazione di Microsoft per un approfondimento sui SID, limitandoci qui a qualche esempio dei SID utilizzati da Windows per identificare i gruppi di utenti.

S-1-1-0 rappresenta il gruppo Everyone, che comprende tutti gli utenti del computer, inclusi quelli anonimi che utilizzano eventualmente l'utente Guest (se attivato). In questo SID il valore del campo Authority vale 1, che rappresenta la World Authority. Altri valori di Authority sono 2 (Local Authority), 3 (Creator Authority), 4 (Non-unique Authority) e il comune 5 (NT Authority).

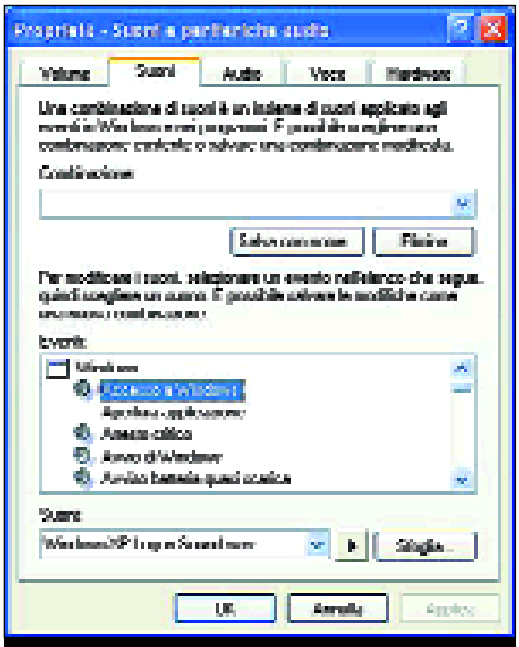
S-1-5-1 rappresenta il gruppo Dialup degli utenti che hanno eseguito il Logon tramite una connessione dialup (via modem).

S-1-5-2 rappresenta il gruppo Network degli utenti che hanno eseguito il Logon tramite una connessione di rete.

S-1-5-32-544 rappresenta il gruppo Administrators, il cui membro di default, dopo l'installazione di Windows, è l'utente Administrator (con SID S-1-5-21-....). Ci sono parecchi altri gruppi predefiniti di utenti, tra cui Users (S-1-5-32-545) e Power Users (S-1-5-32-547).



La struttura di HKEY_CURRENT_USER è la stessa che ha ogni utente attivo elencato in HKEY_USERS



Per modificare i suoni emessi da Windows nelle diverse circostanze, si utilizza l'applet Suoni e periferiche audio del Pannello di controllo

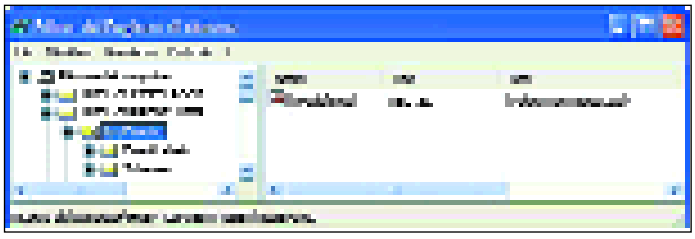
Identificatori globali

Insieme ai SID, c'è un altro tipo di identificatore che viene ampiamente utilizzato in Windows: il GUID o Globally Unique Identifier. I GUID sono numeri che identificano in modo univoco computer, dispositivi, applicazioni, componenti software e altri oggetti. Tutti i GUID sono costituiti da 16 byte e vengono rappresentati attraverso gruppi di 8-4-4-4-12 cifre esadecimali, come ad esempio {5645C8C3-E277-11CF-8FDA-00AA00A14F93}, esempio reale del GUID di un componente software di Microsoft. Come dice il nome, i GUID sono identificatori unici a livello globale e sono generati da appositi programmi (come Guidgen.exe) e anche dallo stesso Windows XP.

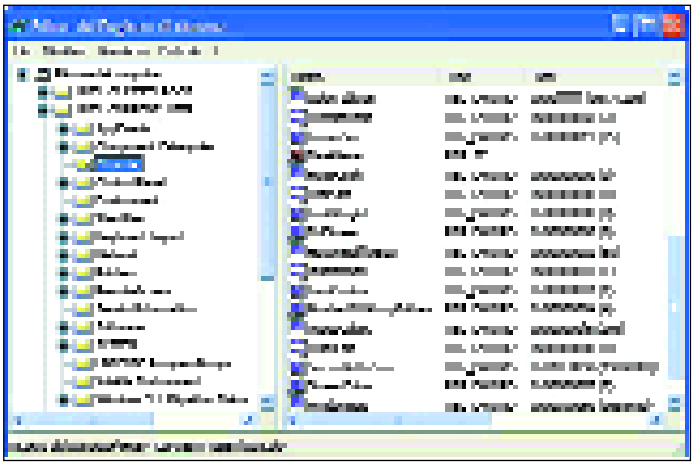
Nel registro trovate una gran quantità di GUID associati soprattutto ai componenti OLE (*Object Linking and Embedding*) per il collegamento tra moduli applicativi e di sistema. In generale i GUID vengono usati come mezzo di collegamento tra applicazioni, tipi di file, componenti OLE e il sistema operativo.

Componenti diversi, anche di ugual nome, hanno GUID diversi, con la possibile eccezione di versioni diverse dello stesso programma che hanno lo stesso GUID per motivi di compatibilità. Per assicurare l'unicità, ogni GUID viene calcolato utilizzando l'indirizzo MAC (*Media Access Control*), che identifica in modo unico ogni interfaccia di rete Ethernet, e includendo nell'algoritmo la data e ora corrente e la generazione di un numero casuale.

GUID, UUID (*Universally* ▷



HKEY_CURRENT_USER\AppEvents contiene i nomi degli eventi che danno luogo a un'emissione acustica, insieme ai nomi dei relativi file audio



HKEY_CURRENT_USER\Console contiene i dati di configurazione della finestra prompt (cmd.exe), ovvero la console che funge da interfaccia per le applicazioni in modalità testo

Unique ID) e CLSID (*Class ID*) sono nomi diversi per lo stesso concetto, usati per indicare classi specifiche di oggetti.

Descrizione degli utenti

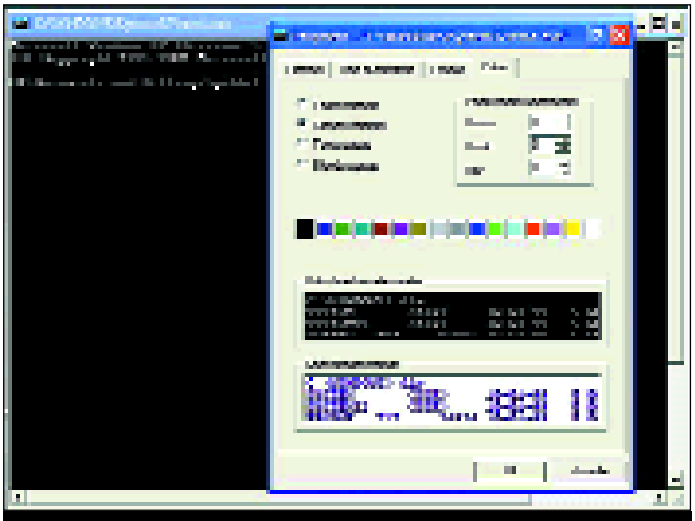
Per comodità possiamo espandere la chiave HKEY_CURRENT_USER, che contiene le sottochiavi dell'utente corrente (quello, tra i vari utenti di HKEY_USERS, che ha eseguito il logon locale e sta usando la console). Tutti gli altri utenti hanno la stesse sottochiavi, di cui diamo una breve descrizione.

HKEY_CURRENT_USER\AppEvents definisce eventi legati ad applicazioni, come i suoni da emettere nelle varie circostanze. Il modo più facile di modificare l'associazione tra gli eventi e i suoni emessi da Windows (ed eventualmente da qualche applicazione) è tramite l'applet Suoni e periferiche audio (sezione Suoni) del *Pannello di controllo*. La chiave AppEvents contiene due sottochiavi: EventLabels contiene le associazioni tra ogni evento e il suo nome, lo stesso che ritrovate in Suoni e periferiche audio; Schemes associa gli eventi ai suoni da produrre.

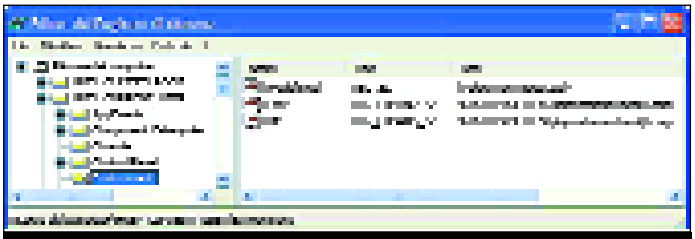
HKEY_CURRENT_USER\Console contiene i dati di configurazione della finestra prompt (cmd.exe), ovvero la console che funge da interfaccia per le applicazioni in modalità testo. Le impostazioni della chiave Console includono le dimensioni della finestra, i colori di testo e sfondo, le dimensioni del cursore, le dimensioni e stile dei caratteri, e via dicendo.

Per modificare le caratteristiche della finestra prompt (solo per la sessione corrente o per tutte le sessioni), non occorre l'editing del registro, basta fare clic sull'icona di sistema, nell'angolo in alto a sinistra della finestra prompt, e selezionare *Proprietà*. Quattro sezioni permettono di modificare a piacimento tutte le caratteristiche dell'interfaccia.

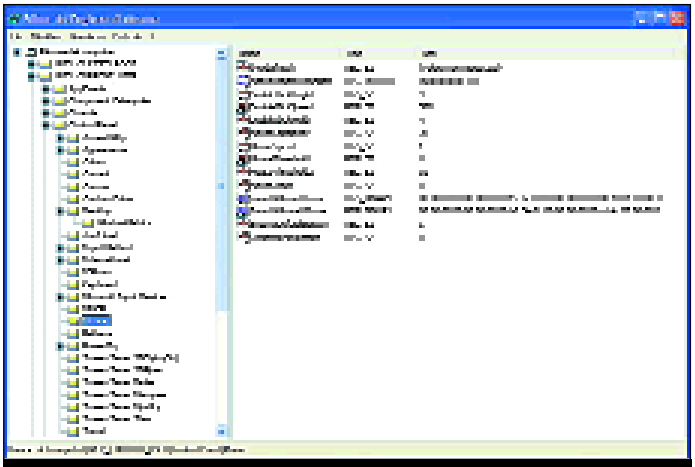
HKEY_CURRENT_USER\Control Panel contiene due dozzine di sottochiavi che memorizzano la maggior par-



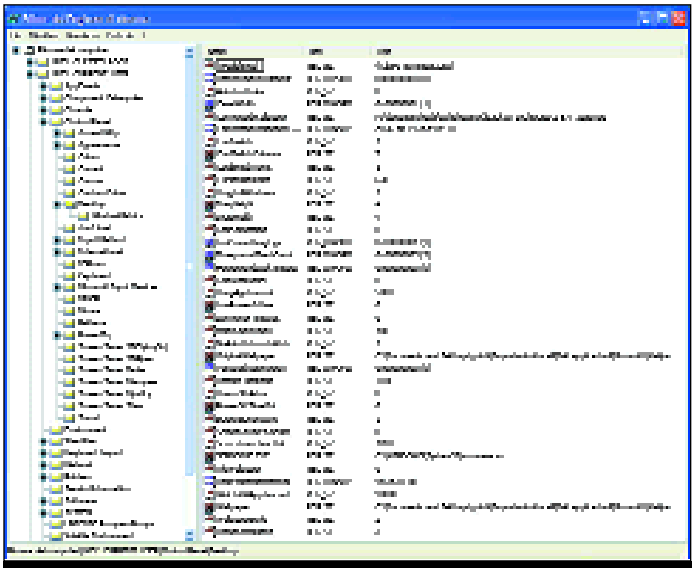
Per modificare la configurazione della finestra prompt basta fare clic sull'icona di sistema, nell'angolo in alto a sinistra della finestra prompt, e selezionare Proprietà, *che offre quattro sezioni di impostazioni*



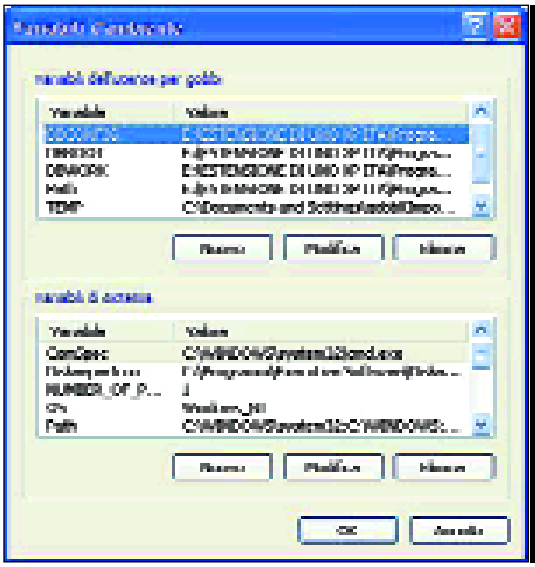
HKEY_CURRENT_USER\Environment contiene impostazioni corrispondenti a variabili di sistema specifiche per l'utente corrente



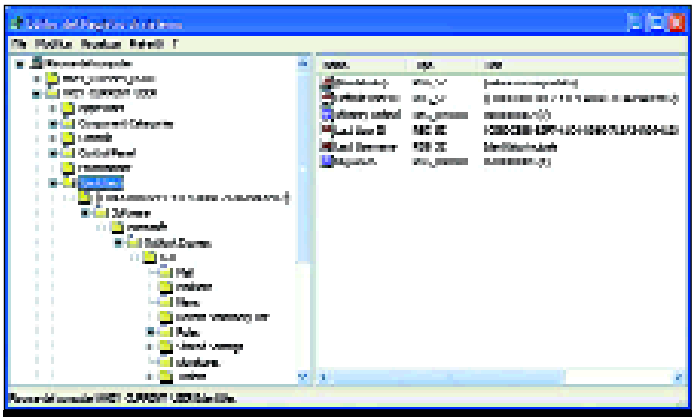
La chiave HKEY_CURRENT_USER\Control Panel\Mouse controlla i parametri di configurazione del mouse



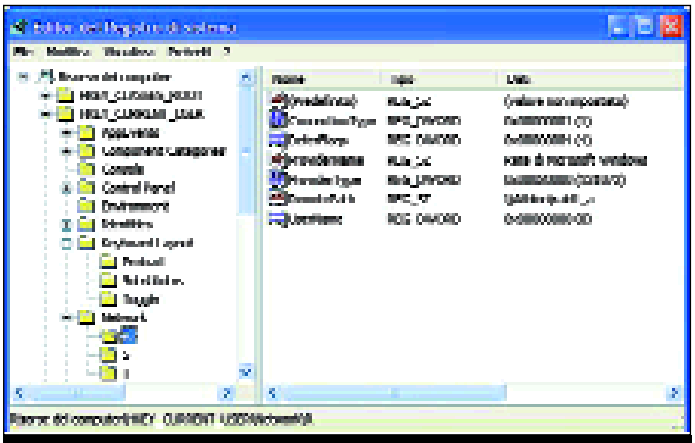
HKEY_CURRENT_USER\Control Panel contiene la maggior parte delle impostazioni che si possono modificare attraverso le applicazioni del Pannello di controllo*; qui si vede la sottochiave Desktop che controlla decine di parametri dell'interfaccia utente di Windows*



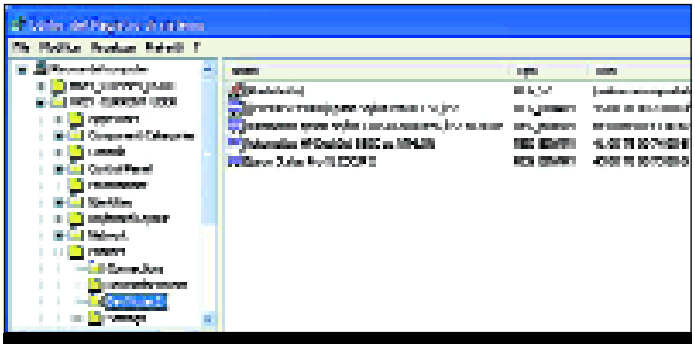
Le variabili di ambiente sono facilmente modificabili attraverso Pannello di controllo, Sistema, Avanzate, Variabili d'ambiente



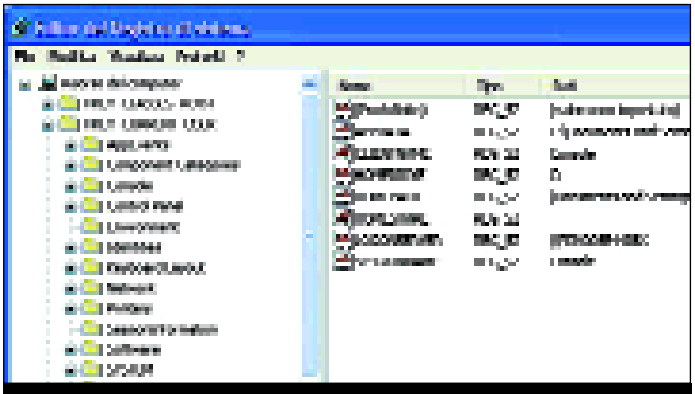
HKEY_CURRENT_USER\Identities contiene la configurazione per alcune applicazioni specifiche per il particolare utente; per default si tratta di informazioni relative all'uso di Outlook Express



HKEY_CURRENT_USER\Network contiene le informazioni di configurazione per ogni drive di rete che l'utente ha mappato in modo permanente



HKEY_CURRENT_USER\Printers descrive le stampanti installate, localmente e in rete, che sono accessibili all'utente corrente; tra le sottochiavi, DevModes2 descrive le configurazioni per tutte le stampanti accessibili



HKEY_CURRENT_USER\Volatile Environment contiene alcune informazioni generali sul computer, il profilo dell'utente corrente e la sessione

te delle impostazioni che si possono modificare attraverso le applicazioni del *Pannello di controllo*. Ad esempio, la chiave Desktop (con sottochiave WindowMetrics) controlla decine di parametri dell'interfaccia utente di Windows, mentre la chiave Mouse controlla i parametri di configurazione del mouse.

HKEY_CURRENT_USER\Environment contiene impostazioni corrispondenti a variabili di sistema specifiche per l'utente correntemente connesso al sistema. Le variabili di ambiente sono facilmente assegnabili e modificabili attraverso *Pannello di controllo*, *Sistema*, *Avanzate*, *Variabili d'ambiente*.

HKEY_CURRENT_USER\Identities contiene la configurazione per alcune applicazioni specifiche per il particolare utente. Tipicamente, si tratta di informazioni relative all'uso di Outlook Express.

HKEY_CURRENT_USER\Keyboard Layout specifica, attraverso le sue sottochiavi, la lingua utilizzata per il layout di tastiera corrente.

HKEY_CURRENT_USER\Network contiene le informazioni di configurazione per ogni drive di rete che l'utente ha mappato in modo permanente (attraverso *Esplora risorse*, *Strumenti*, *Connetti unità di rete*...).

HKEY_CURRENT_USER\Printers descrive le stampanti installate, localmente e in rete, che sono accessibili all'utente corrente. Il modo per modificare queste impostazioni è attraverso *Start*, *Stampanti e fax*.

Tra le sottochiavi, Connections descrive le stampanti connesse in modo remoto; DevModePerUser descrive le configurazioni utente per le stampanti; DevModes2 descrive le configurazioni per tutte le stampanti accessibili; Settings contiene informazioni sulle stampanti locali.

HKEY_CURRENT_USER\SessionInformation contiene informazioni dinamiche sulla sessione corrente; la sottochiave ProgramCount indica il numero di programmi attivi in esecuzione.

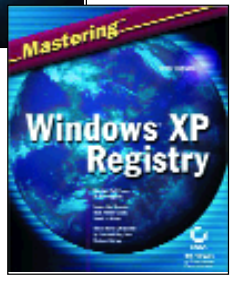
HKEY_CURRENT_USER\Software contiene impostazioni di configurazione per il software installato localmente e accessibile all'utente corrente. Queste informazioni hanno la stessa struttura già vista per la chiave HKEY_LOCAL_MACHINE\SOFTWARE.

HKEY_CURRENT_USER\SYSTEM contiene informazioni utilizzate dal programma di backup e ripristino di Windows XP (in *Accessori*, *Utilità di sistema*).

HKEY_CURRENT_USER\UNICODE Program Groups e HKEY_CURRENT_USER\Windows 3.1 Migration Status sono presenti per motivi di compatibilità; vengono usate solo se Windows XP è stato installato come aggiornamento di certe versioni precedenti di Windows.

HKEY_CURRENT_USER\Volatile Environment contiene alcune informazioni generali sul computer, il profilo dell'utente corrente e la sessione.

Tutte le sottochiavi di HKEY_CURRENT_USER, valide per l'utente correntemente logged-on, valgono anche per le descrizioni degli altri utenti in HKEY_USERS. ■



I libri Mastering Windows XP Registry *(Peter Hibson, Sybex) e* Windows XP Registry Guide *(Jerry Honeycutt, Microsoft Press) sono altre due utili fonti di informazioni sul registro di sistema, oltre al volume* Windows XP Registry *(Olga Kokoreva, A-List) presentato sul numero scorso*