Sistemi Operativi e informatica[1]

Massimo Marchi

Dip. Scienze dell'Informatica
Università degli Studi di Milano, Italia
marchi@dsi.unimi.it

a.a. 2011/12

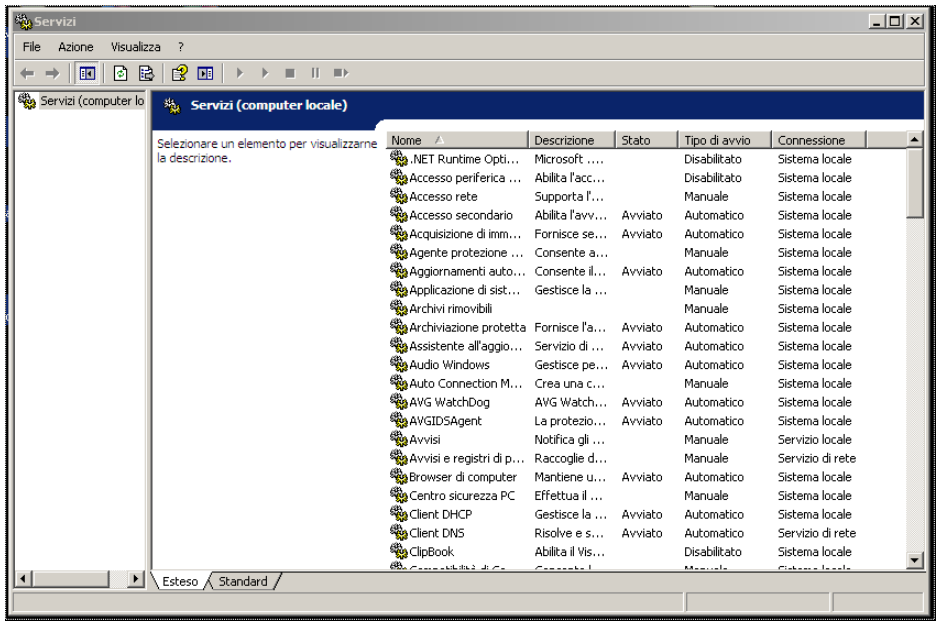
Shell di Windows

La shell di Windows non si presta bene allo scripting. Esistono porting di alcune (non recenti) versioni Bash per la CLI di Windows. E' possibile anche installare un interprete Perl per Windows o usare MatLab e le sue funzioni dedicate al file system pre realizzare semplici script.
Alcuni comandi MS-DOS eseguibili da CLI (*Esegui.. cmd*):

- **dir** : lista la directory
- **type** : stampa un file
- **cd** : cambia directory o mostra la posizione corrente

Servizi di Windows

Allo startup vengono lanciati alcuni servizi di sistema. L'elenco completo è visibile nella console di aministrazione dei servizi (*Pannello di controllo->Strumenti di Amministrazione->Servizi* oppure
Esegui.. services.msc)



Servizi di Windows:esempi

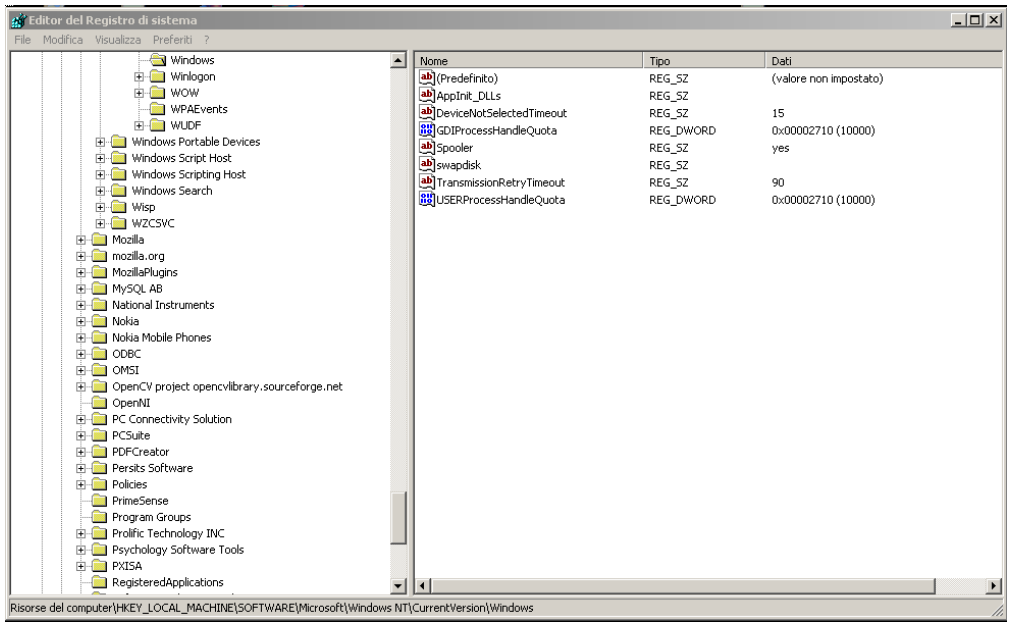
Alcuni servizi importanti:

- **Windows Installer, Servizio trasferimento intelligente in background** : indispensabili per installare o aggiornare software
- **Aggiornamenti Automatici**
- **Windows firewall**
- **Notifica degli eventi di sistema** : servizio di logging, usato dai processi per comunicare messaggi ed errori.

Nei calcolatori che usano applicativi di rete, il tempo locale della macchina è fondamentale che venga tenuto allineato al tempo globale attraverso il servizio NTP (*W32Time*).

Registry

Il **Registry** è contiene tutti i settaggi di Windows. E' possibile (non consigliabile) editarlo manualmente attraverso *regedit*:



Esistono programmi di protezione, come *TeaTimer*, che possono monitorare gli accessi al registry in modo da intercettare eventuali modifiche indesiderate.

Registry: Esempi

Alcuni punti del registry alterati da malware:

`HKCU\Software\Microsoft\Windows\CurrentVersion\Run`

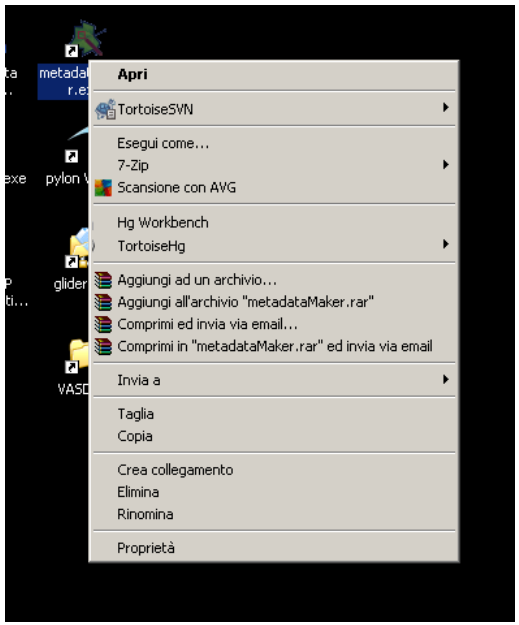
Contiene le chiavi corrispondenti ai programmi lanciati dall'utente al logon

`HKLM\SOFTWARE\Microsoft\Windows NT\...`
`CurrentVersion\SvcHost`

Contiene le chiavi corrispondenti ai servizi lanciati da *svchost.exe* all'avvio

Run as...

A volte può essere utile lanciare un dato programma con le credenziali di un altro utente. Se il se il servizio relativo è attivo, è possibile accedere conil tasto destro sull'eseguibile alla funzionalità *Esegui come..*

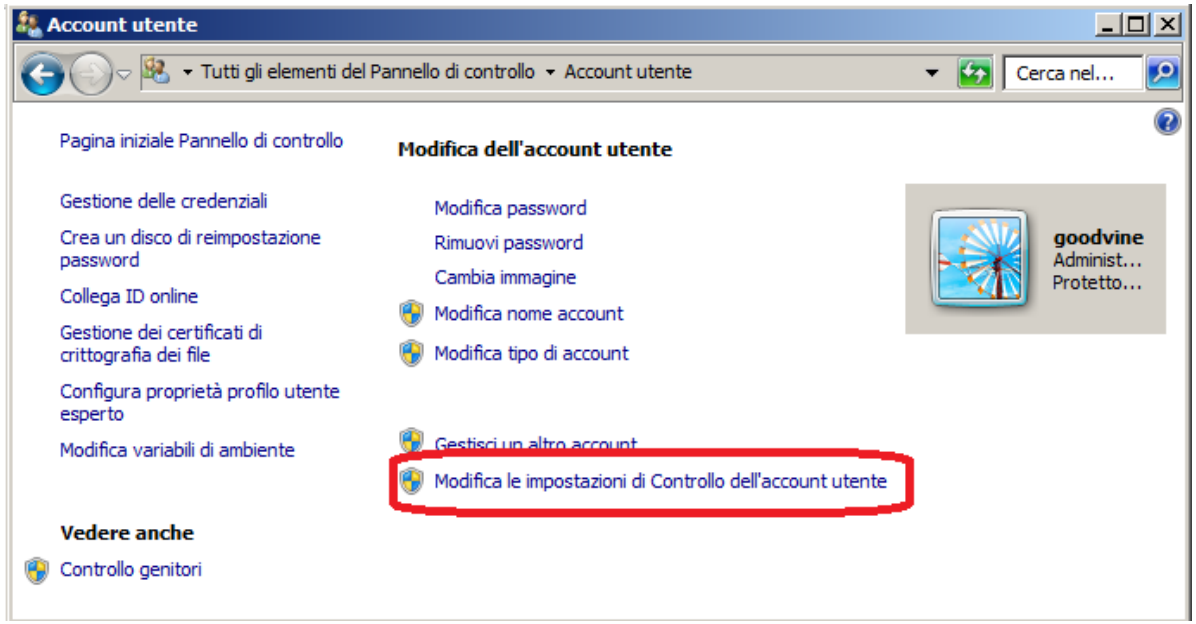


Controllo dei processi: Windows Defender

Da Windows Vista in poi è stato introdotto il sistema di protezione **Windows Defender**. Il sistema monitora l'attività dei processi, in particolare riguardo alla privacy ed agli addon di Internet Explorer. Nel caso venga richiesta una operazione potenzialmente pericolosa, il sistema blocca l'operazione o chiede conferma.
Sistemi analoghi sono presenti anche negli antivirus più evoluti. Oltre a verificare che gli eseguibili non contengano una segnatura di un infezione conosciuta, l'AV controlla anche le operazioni compiute da ogni processo. A queste operazioni vengono applicate delle *policy* di sicurezza che decidono se autorizzare, negare o chiedere conferma all'utente.

User Account Control (UAC)

Da Windows Vista in poi è stato introdotto un ulteriore livello di protezione per gli account di l'amministratore, lo **User Account Control** (UAC). Prima di compiere operazioni potenzialmente dannose per il sistema, il SO chiede la conferma all'utente.
E' possibile disattivare questa funzionalità modificando le *policy* associate all'utente:



Norme generali Anti-Intrusione

- Usare password non banali
- Sui sistemi sensibili ridurre al minimo il numero di utenti abilitati (se possibile solo l'amministratore)
- Tenere i propri dati ed usare per il proprio lavoro un sistema diverso da quello amministrato.
- Usare password differenti per differenti livelli di sicurezza. Preferenzialmente usare sistemi alternativi alla tastiera per autenticarsi (*agent*, token, impronte digitali).
- Usare una password per Administrator difficile.
- Non usare mai l'account Administrator, creare piuttosto un altro account con privilegi di amministratore (in caso di problemi questo account può essere facilmente ricreato).
- Configurare (ed incoraggiare ad usare) profili personali distinti per ogni utente.

Norme generali Anti-Intrusione

- Su sistemi sensibili usare sempre software originale e sicuro. Se inevitabile, usare la virtualizzazione per creare un'ambiente isolato dove far girare software non sicuro.
- Tenere aggiornati Windows, Antivirus e programmi in uso.
- Disattivare l'esecuzione automatica dei supporti removibili.
- Proteggere la rete a cui sono collegati i sistemi sensibili.
- Su sistemi particolarmente esposti valutare la possibilità di reinstallare periodicamente un'immagine sicura del sistema.

Norme generali per la Sicurezza dei Dati

- Programmare backup frequenti dei dati e dei sistemi
- Proteggere fisicamente lo storage dei dati da manomissioni e danneggiamenti
- Valutare il grado di importanza dei dati ed il tempo di fault sopportabile dagli utenti e configurare il sistema in modo da rispondere ai requisiti richiesti. Richieste minime:
  - Usare almeno dischi Raid 5 con controller hardware per lo storage dei dati.
  - Usare UPS sulla linea di alimentazione dello storage e del sistema di elaborazione dei dati.
  - Minimizzare il numero di operazioni che prevedono la cancellazione dei dati *raw*.
  - Non esporre direttamente a Internet lo storage ed il sistema di elaborazione dei dati.