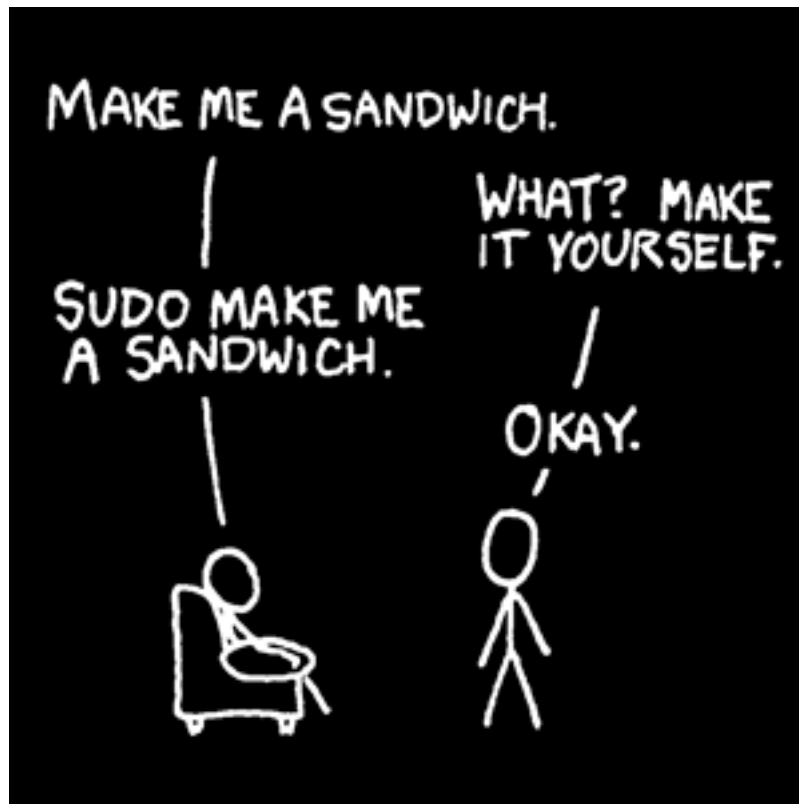


SUDARE CON WINDOWS - mini howto

(do you sudo? - Schley Andrew Kutz -)

Augusto Scatolini (webmaster@comunecampagnano.it)

Ver. 1.0 Marzo 2010



Il titolo di questa mini guida è un semplice gioco di parole per indicare la possibilità di usare il comando GNU/Linux **sudo** in ambito Windows.

sudo (abbreviazione dalla lingua inglese di *super user do*, esegui come superutente) è un programma per i sistemi operativi Unix e Unix-like che, con dei vincoli, permette di eseguire altri programmi assumendo l'identità (e di conseguenza anche i privilegi) di altri utenti.

I vincoli con cui **sudo** esegue programmi sono espressi nel file di configurazione `/etc/sudoers`, che normalmente è modificabile solo dall'utente `root`: in esso sono definiti gli utenti che possono eseguire comandi tramite **sudo**, le identità che possono assumere ed i comandi che possono eseguire con eventuali vincoli sui parametri, con o senza richiesta di autenticazione.

Nell'uso comune **sudo** viene configurato dall'amministratore di sistema per consentire a utenti non privilegiati di eseguire programmi assumendo l'identità dell'utente `root`, autenticandosi però con le proprie credenziali invece che con quelle di `root`. Al contrario del comando **su** ciò permette di evitare di dover diffondere le credenziali di `root`, semplificando così la gestione della sicurezza.

<http://it.wikipedia.org/wiki/Sudo>

L'applicazione originariamente, **sudo** fu scritta nel 1980 da Bob Cogheshall e Cliff Spenser nel dipartimento di "Computer Science" a SUNY/Bufalo. In seguito vari programmatori hanno contribuito nel 1984, 1985, '86, '91, '94, '95, '96, '99, '01, '05.

sudo, attualmente è mantenuto da Todd Miller <Todd.Miller@courtesan.com>

<http://gratisoft.us/sudo/history.html>

Quindi con il comando **sudo** l'utente – non root – eleva i propri privilegi e riesce ad eseguire quei comandi e/o programmi che richiedono appunto i privilegi di root. Un esempio molto chiaro è quello dell'installazione di programmi, ad esempio per installare un programma come firefox, l'utente digiterà sul terminale : **sudo apt-get install firefox**
Il sistema risponderà chiedendo la password dell'utente e non quella di root.

gksudo è il Frontend grafico per il comando sudo disponibile in ambiente GNOME mentre **kdesudo** è il Frontend grafico per il comando sudo disponibile in KDE

Per capire bene il comando **sudo** è molto importante capire la differenza con il comando **su**

su (abbreviazione dalla lingua inglese di switch user o di substitute user, cambia utente o sostituisci utente) è un comando dei sistemi operativi Unix e Unix-like che permette di avviare una shell testuale assumendo l'identità di un altro utente del sistema. La shell avviata è quella predefinita per l'utente di cui si assume l'identità, ed è possibile passarle parametri per farle ad esempio eseguire direttamente un comando, che a questo punto sarà eseguito con la nuova identità.

su viene tipicamente usato da utenti non privilegiati per avviare una shell nei panni di root, e da root per avviare una shell nei panni di utenti ordinari.

Normalmente su richiede di effettuare un'autenticazione con le credenziali dell'utente di cui si vuole assumere l'identità. Ciò non è richiesto quando su viene eseguito

[http://it.wikipedia.org/wiki/Su_\(Unix\)](http://it.wikipedia.org/wiki/Su_(Unix))

Nel mondo Windows esiste l'equivalente del comando su, è il comando “**esegui come**” o “**run as**” ma non esiste l'equivalente del comando sudo.

Vista la scomodità e a volte l'inutilità dell'uso del comando “esegui come” perché ogni utente ha il suo ambiente, la sua home directory, ecc succede che gli utenti Windows, praticamente, lavorano sempre con le credenziali di Administrator o con quelle di un utente che fa parte del gruppo Administrators.

Non ci vuole un genio per capire che in questa modalità il livello di sicurezza diminuisce drasticamente.

Nel mondo Unix e Unix-like come GNU/Linux questo è stato capito da più di trenta anni! Non aggiungo commenti.

Sudo per Windows (sudowin)

Il ricercatore Senior e scienziato sviluppatore presso Hyper9 Schley Andrew Kutz nel 2005 ha scritto Sudo per Windows (**sudowin**)

Il progetto (funzionante) si trova presso <http://sourceforge.net/projects/sudowin/>

Dal sito si può scaricare il pacchetto msi

<http://sourceforge.net/projects/sudowin/files/sudowin/sudowin-0.4.2-r208/sudowin-bin-0.4.2-r208.msi/download>

oppure l'eseguibile zippato

<http://sourceforge.net/projects/sudowin/files/sudowin/sudowin-0.4.2-r208/sudowin-bin-0.4.2-r208.exe.zip/download>

La documentazione (55 pagine in inglese) è disponibile presso

http://www.sans.org/reading_room/whitepapers/bestprac/sudo_for_windows_sudowin_1726?show=1726.php&cat=bestprac




L'applicazione di tipo client-server è alquanto complessa e ha dei file di configurazione in formato XML, permette all'amministratore della macchina Windows di stabilire quali utenti (limitati) possono usufruire del comando e per quali applicazioni tale comando può essere utilizzato.

Permette, in definitiva, una configurazione molto granulare.

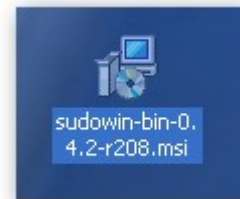
Ai fini pratici, per un uso molto semplice (pedagogico), installeremo il programma, configureremo un utente limitato all'uso di sudowin e gli permetteremo di usare un paio di programmi come superutente.

Una volta entrati sul sito del progetto scaricare il file sudowin-bin-0.4.2-r208.msi

ovvero l'ultimo disponibile

Browse Files for Sudo for Windows				
File/Folder Name	Platform	Size	Date ↓	Downloads
Newest Files				
 sudowin-src-0.4.2-r208.zip		184.8 KB	2008-09-30	2,211
 sudowin-bin-0.4.2-r208.msi		511.0 KB	2008-09-30	10,195
 sudowin-bin-0.4.2-r208.exe.zip		473.0 KB	2008-09-30	5,773

scaricarlo sul desktop e lanciarlo con un doppio click



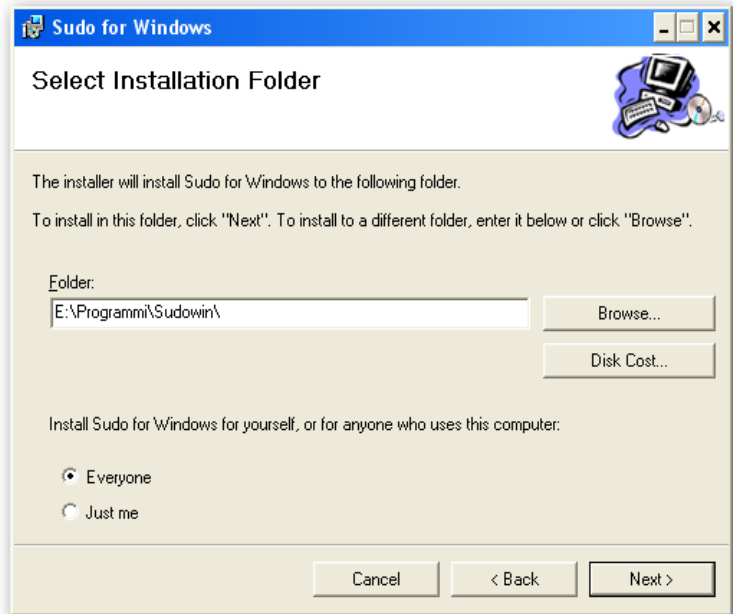
l'installazione è classica, confermare tutte le opzioni proposte



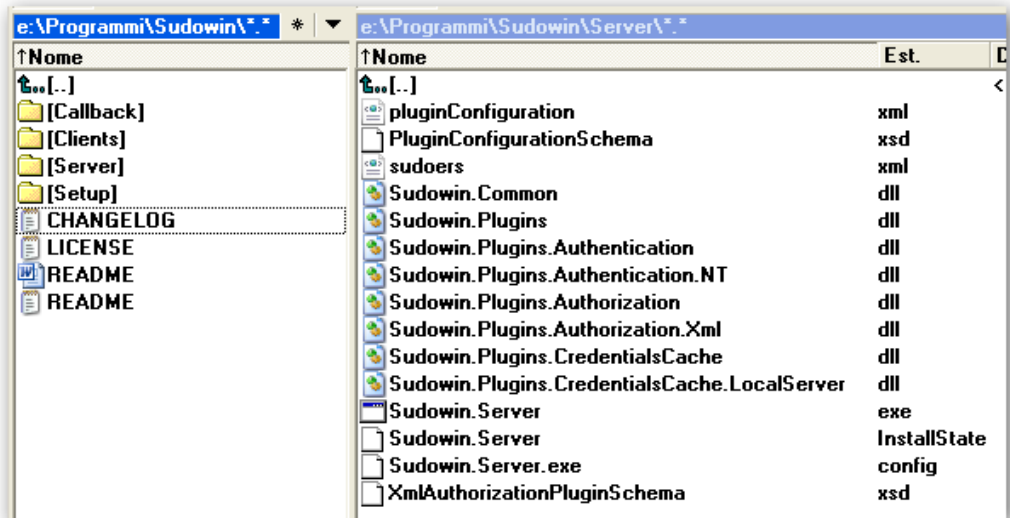
next, next,



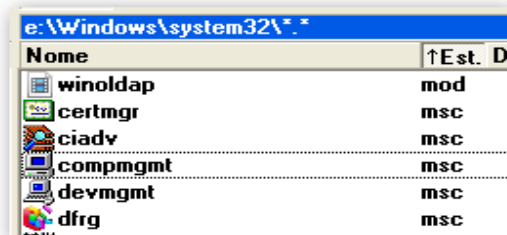
next, next,



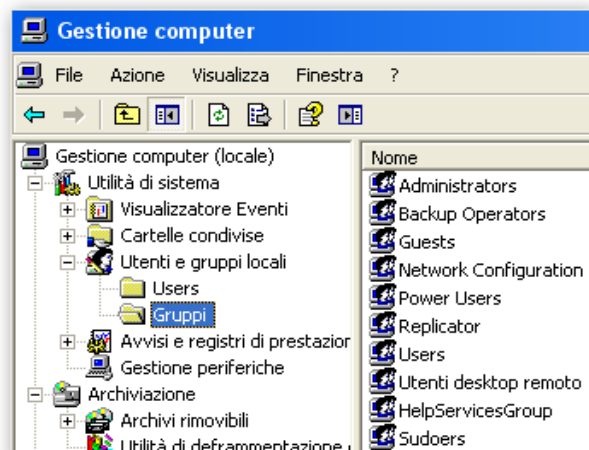
il programma verrà installato



a questo punto lanciando compmgmt.msc che si trova in C:\Windows\system32\ si avvierà il programma Gestione Computer.



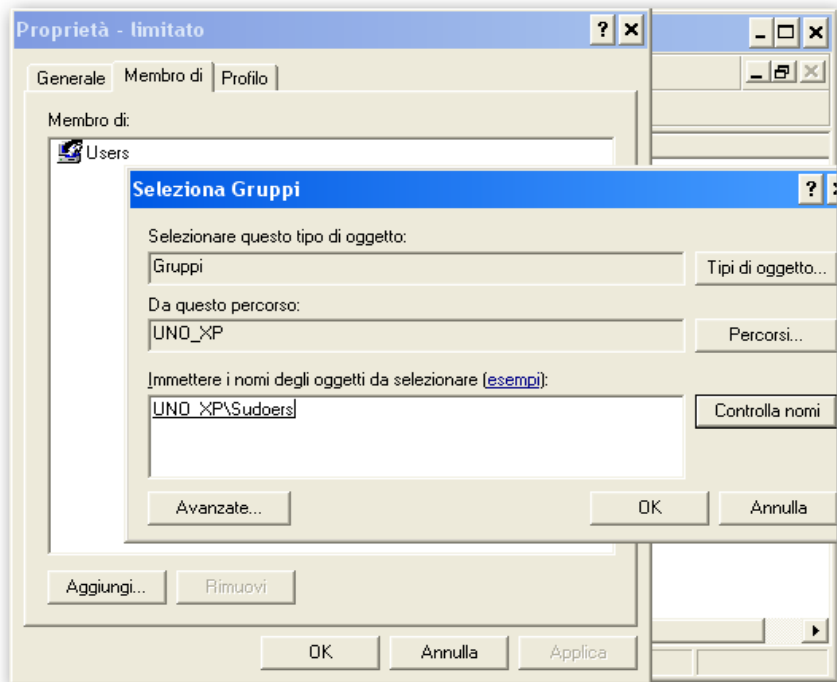
Navigando fino a Gruppi si noterà l'installazione di sudowin ha creato il nuovo gruppo **SUDOERS**



ora dal menù Users creiamo un nuovo utente limitato che chiameremo “limitato” con password = “limitato”



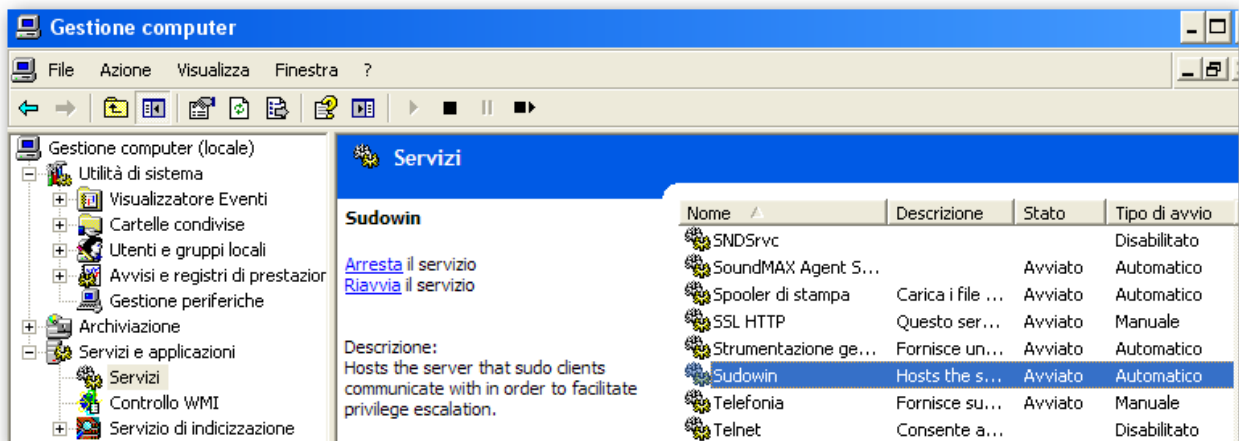
nelle proprietà dell'utente “limitato” e precisamente in “Membro di “ noteremo un unico gruppo (Users).



Inseriamolo anche nel gruppo Sudoers

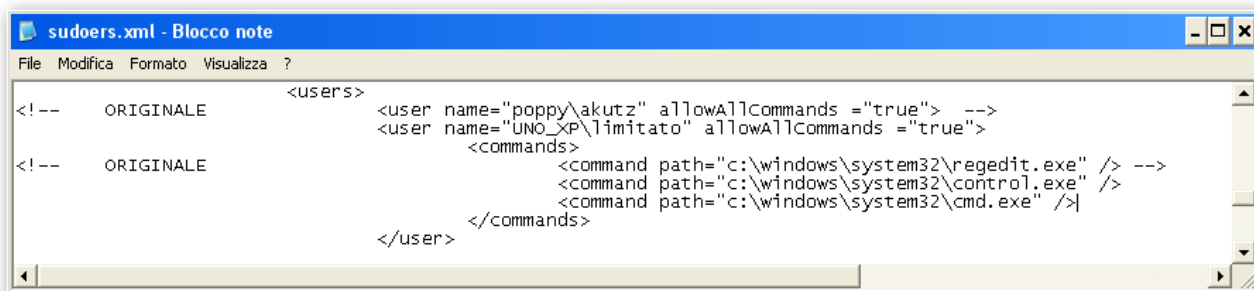


Sempre da Gestione computer” → “Servizi e applicazioni” → “Servizi” si può verificare che il servizio Sudowin (lato server) è in esecuzione ed è in modalità “automatico”



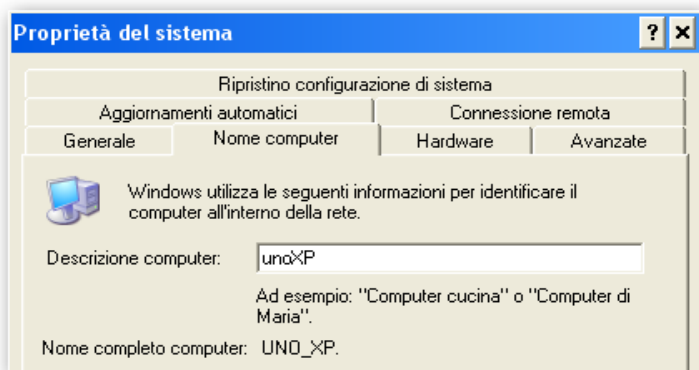
A questo punto si apre il file sudoers.xml con un editor ASCII come notepad (blocco note) e si apportano due semplici modifiche:

- 1) alla voce user name= scriveremo il nome del nuovo utente limitato nella forma NOMECOMPUTER\nomeutente
- 2) al punto <command path= scriveremo quale comando potrà essere usato dall'utente limitato con la funzione sudo



```
sudoers.xml - Blocco note
File Modifica Formato Visualizza ?
<!-- ORIGINALE <users> <user name="poppy\akutz" allowAllCommands ="true"> -->
<!-- ORIGINALE <user name="UNO_XP\limitato" allowAllCommands ="true">
<!-- ORIGINALE <commands>
<!-- ORIGINALE <command path="c:\windows\system32\regedit.exe" /> -->
<!-- ORIGINALE <command path="c:\windows\system32\control.exe" />
<!-- ORIGINALE <command path="c:\windows\system32\cmd.exe" />
<!-- ORIGINALE </commands>
<!-- ORIGINALE </user>
```

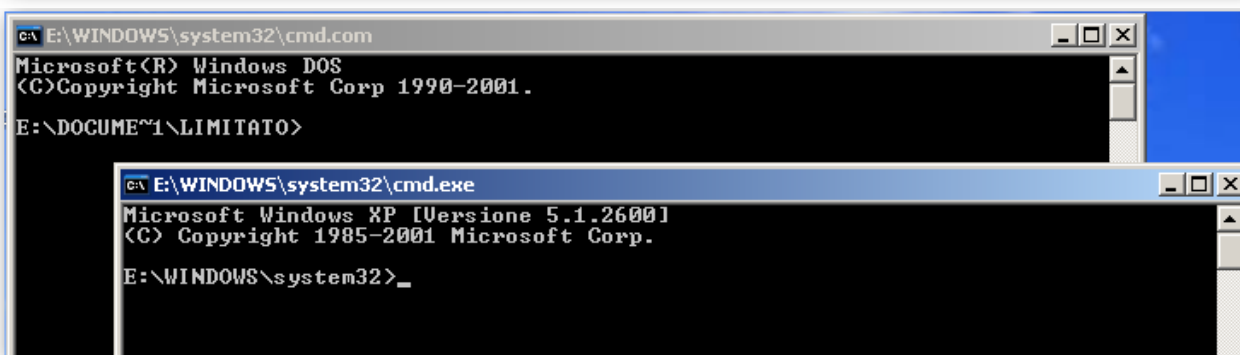
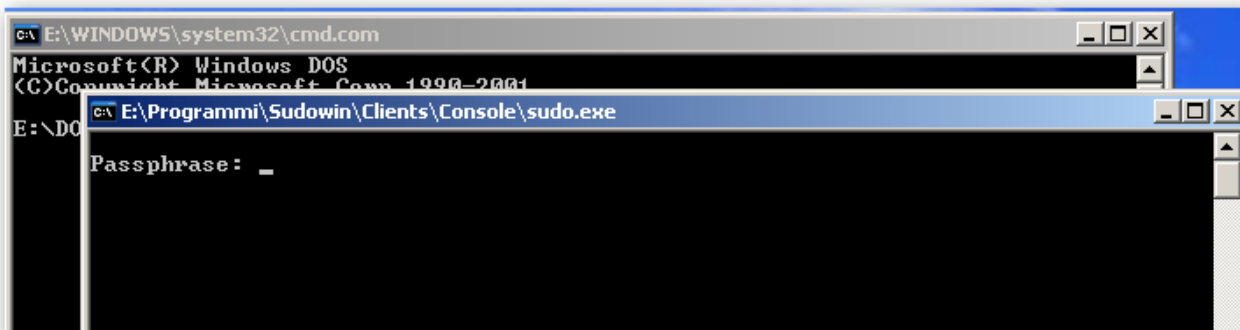
Se non ci ricordiamo il nome del computer, lo si legge nel riquadro Nome computer delle Proprietà del sistema



Sessione utente limitato

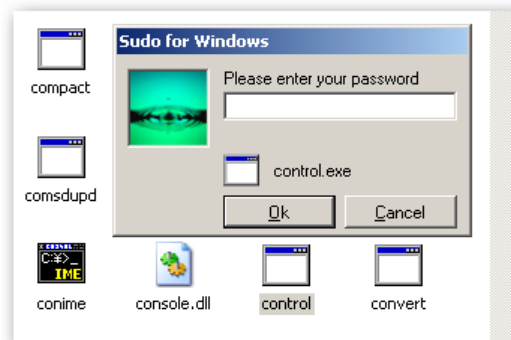
Dopo una disconnessione dall'utente Administrator e una riconnessione come utente limitato facciamo un semplice test con il comando CMD (Prompt del DOS)

- 1) pulsante start → esegui → cmd [appare la finestra DOS nella cartella dell'utente limitato]
- 2) pulsante start → esegui → sudo cmd ci verrà chiesta la password di limitato



- 3) [appare la finestra DOS nella cartella Windows\system32

Se invece andiamo in C:\Windows\ e clicchiamo con il tasto destro su control.exe (Pannello di Controllo) apparirà una finestra grafica dove ci verrà chiesta la password dell'utente limitato



FINE

Questo documento è rilasciato con licenza Copyleft
(tutti i rovesci sono riservati)
altre miniguide

<http://www.comunecampagnano.it/gnu/miniguide.htm>