

Laboratorio di Amministratore di Sistema

7. Procedure avanzate

[Cisco ITESS II - Chapter 11]

Università di Venezia – Facoltà di Informatica
feb-mag 2012 - [A. Memo](#)



Advanced NOS Administration

11.1 I backup

11.2 Mapping unità

11.3 Partizione e processi di gestione

11.4 Risorse di monitoraggio

11.5 Analisi e Ottimizzazione delle prestazioni di rete

Overview of Backup Methods

- Il processo di backup implica la copia dei dati da un computer ad un altro supporto di memorizzazione affidabile per custodirli.
- Una volta che i dati sono stati archiviati, il sistema amministratore può quindi ripristinare i dati nel sistema da qualsiasi backup precedentemente registrato.
- Considerazioni che sono rilevanti per i dispositivi di archiviazione:
 - Costo
 - Size
 - gestibilità
 - Affidabilità



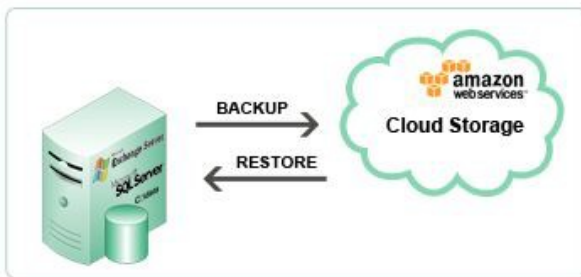
Zmanda Cloud Backup

Windows Server and Desktop Protection



Zmanda Cloud Backup for Windows

Zmanda Cloud Backup (ZCB) is a radically simple-to-use and cost-effective backup and disaster recovery solution. ZCB backs up Windows servers, desktops and live applications such as Microsoft Exchange and SQL Server to Amazon's highly dependable online storage.



LTO ULTRIUM 3, capacità di 800 GB,
fattore di compressione 2:1. Alta velocità di
trasferimento: 40-80 MB / sec
compressione 2:1; nativo 20-40MB/sec.





Backup (1)

- Per backup si intende sia la copia dei file che dei dati
- Il backup serve a ripristinare i dati, una volta che siano andati persi
- La perdita dei dati può avvenire per
 - cause legate agli operatori, persone fisiche (80%)
 - cause tecniche (14%)
 - cause ambientali (6%)

Overview of Backup Methods

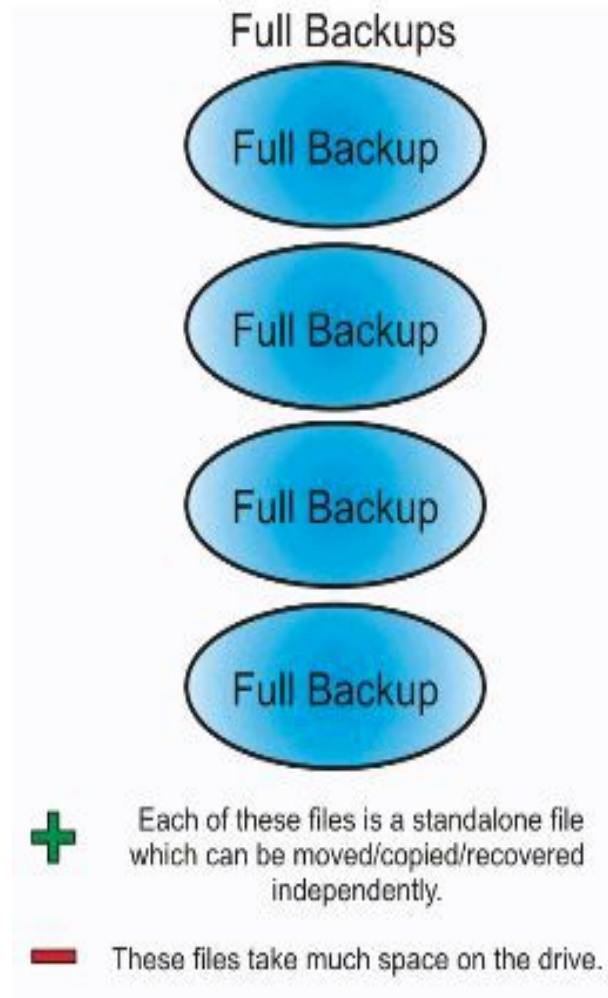
- Dispositivi di backup comunemente usati includono unità a nastro, unità disco rimovibili, registrabili compact disc, HDs
- Ci sono quattro tipi di procedure di backup che definiscono come il backup avrà luogo:
 - Full - sarà il backup di tutto il contenuto del disco rigido (tutti i giorni)
 - Parziale - esegue il backup dei file selezionati (al giorno)
 - Incrementale - solo i file che sono stati modificati dopo l'ultimo backup verranno selezionati per il backup
 - Differenziale - esegue il backup dei file creati o modificati dopo l'ultimo backup normale o incrementale

Backup (2)



- Fattori da prendere in esame per decidere la strategia di backup ottimale:
 - quali file devono far parte del backup
 - backup di rete o locale
 - frequenza del backup
 - quando effettuare il backup
 - che metodi di backup attuare
 - che tecnologie adottare

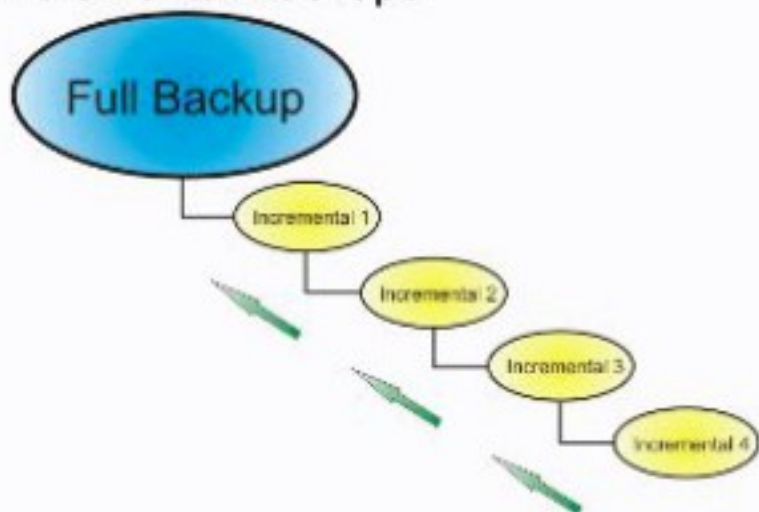
Backup Normale





Backup Incrementale

Incremental Backups



These files take minimum space on the drive. Every incremental contains the data which was changed after the previous incremental backup operation was performed.

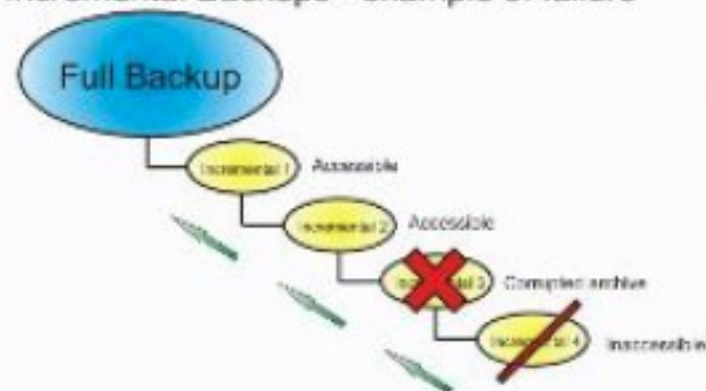


These files work in "chain" and in order to recover you should have all the previous incremental backup files and the full backup.



If the "chain" of incrementals is broken (one of the files is corrupted) you will not be able to recover next incrementals

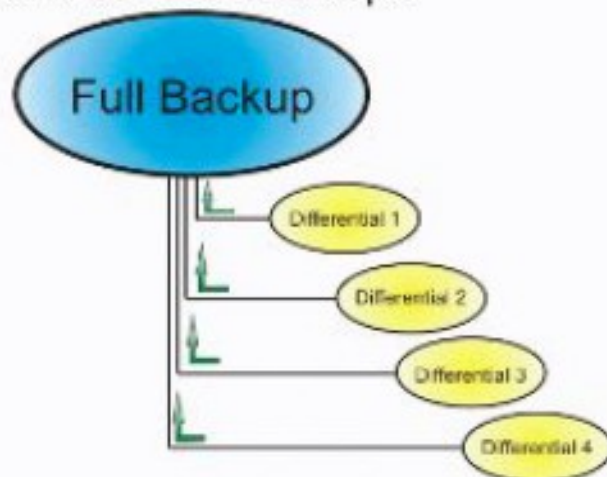
Incremental Backups - example of failure





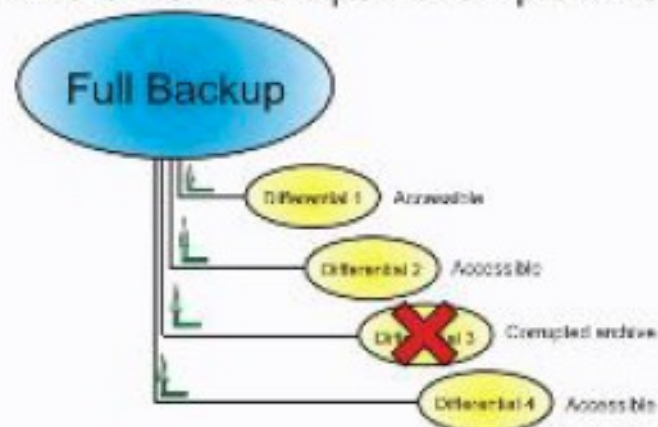
Backup Differenziale

Differential Backups



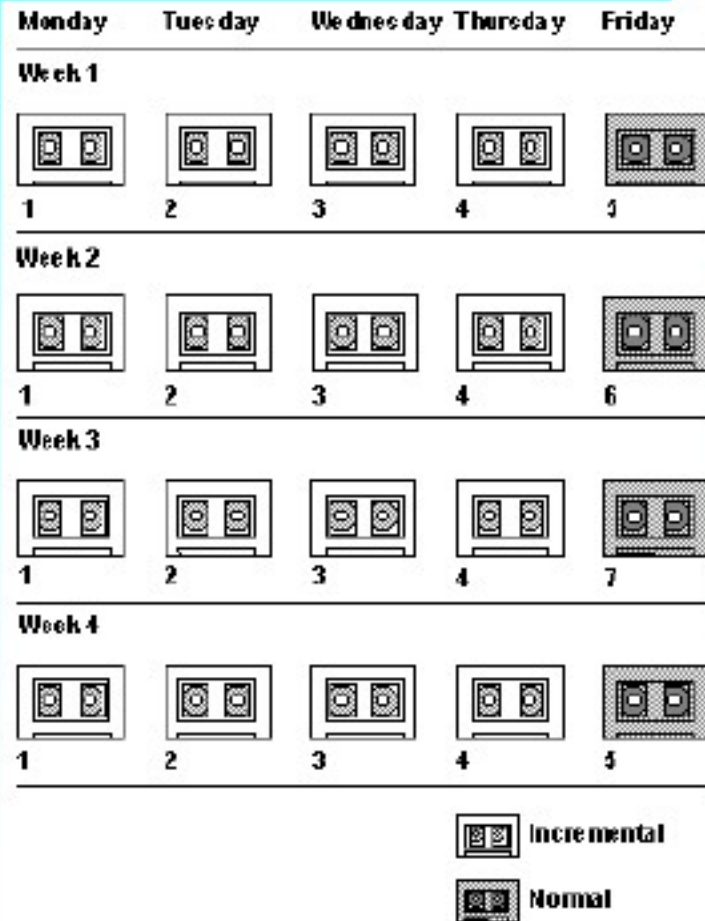
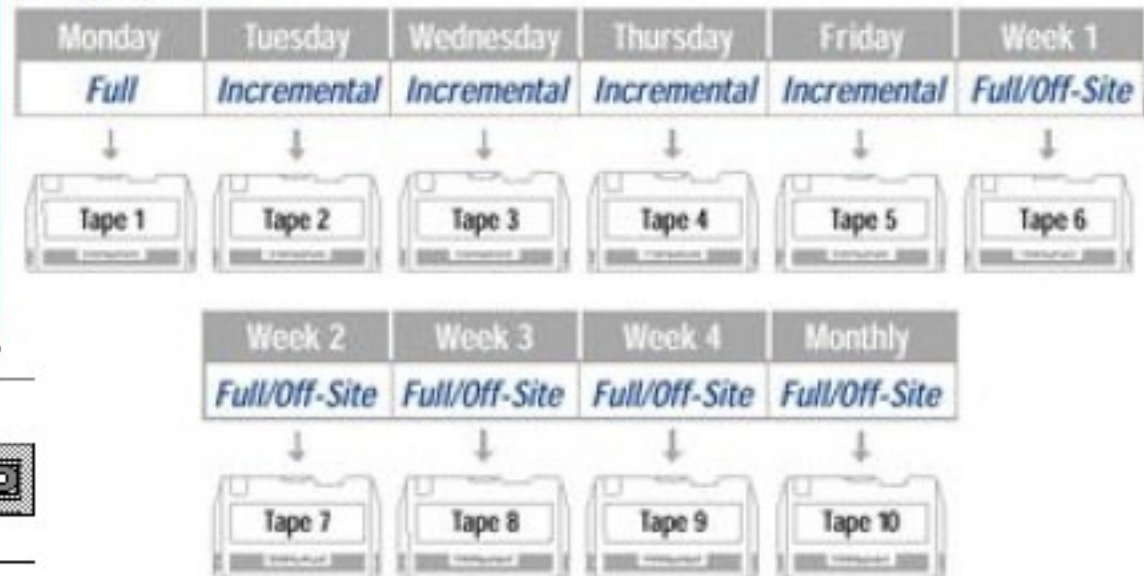
- These files do not take too much space on the drive. Every differential contains the data which was changed after the full backup operation was performed.
- These files work in "pair" and in order to recover you should have full backup file.
- If one of the differentials is broken (the file is corrupted) it will not affect the previous or next differentials. Though if the full backup is corrupted you will not be able to recover.

Differential Backups - example of failure

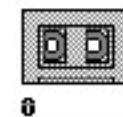


Strategie di backup

10-Day Tape Rotation



Monthly off-site





Un esempio di
backup on the
cloud



Ecco come il back up dei dati aiuta le aziende di medie dimensioni a essere più competitive.

Oggi le medie aziende devono gestire volumi d'informazioni che crescono e si moltiplicano velocemente. Non possono permettersi di perdere dati preziosi su cui basano tutte le operazioni di business. Con budget sempre più ristretti e minori risorse a disposizione per molte aziende è difficile mantenere all'interno un sistema di back up e recovery affidabile. Ecco perché IBM e i suoi Business Partner stanno utilizzando la potenza del cloud computing per offrire alle medie aziende la stessa protezione dei dati che usano le grandi imprese: un servizio studiato per ridurre i rischi e rispondere alle loro esigenze di budget.

E' il nuovo Servizio di back up basato sul cloud di IBM. Si avvale di un'infrastruttura intelligente che effettua un salvataggio dei dati in uno dei data center IBM. Nel momento in cui i dati vengono salvati, sono protetti e al sicuro. Sempre e ovunque.

*il prezzo base annuale del servizio per un pacchetto "small" da 100GB è a partire da 2844,00 (importo per ogni GB mensile aggiuntivo 2,37). Tutti i prezzi riportati sono indicativi ed IVA esclusa, aggiornati al momento di andare in stampa. IBM si riserva il diritto di modificarli e di modificare anche le specifiche relative ai prodotti. Prodotti, programmi e servizi possono essere ritirati da IBM senza preavviso. IBM, il logo IBM, ibm.com e l'icona del pianeta sono marchi registrati di International Business Machines Corporation in diversi Paesi del mondo. La lista aggiornata dei marchi registrati di IBM è disponibile sul sito www.ibm.com/legal/copytrade.shtml, alla voce "Copyright and trademark information". ©2011 IBM Corp. Tutti i diritti riservati.



1. Riduci i costi complessivi e di gestione fino al 40%.

Il tuo Business Partner IBM può aiutarti a confrontare i costi dei sistemi interni alla tua azienda con quelli di un servizio scalabile basato sul cloud e gestito da IBM evitando di impegnare capitali.



2. Un backup automatizzato e più sicuro.

Il backup viene effettuato automaticamente nella finestra temporale stabilita.



3. Hai quello che ti serve, quando ti serve.

Nel cloud i tuoi dati sono custoditi in più versioni, subito disponibili, così puoi prendere più velocemente decisioni più efficaci.









4. Libera risorse preziose.

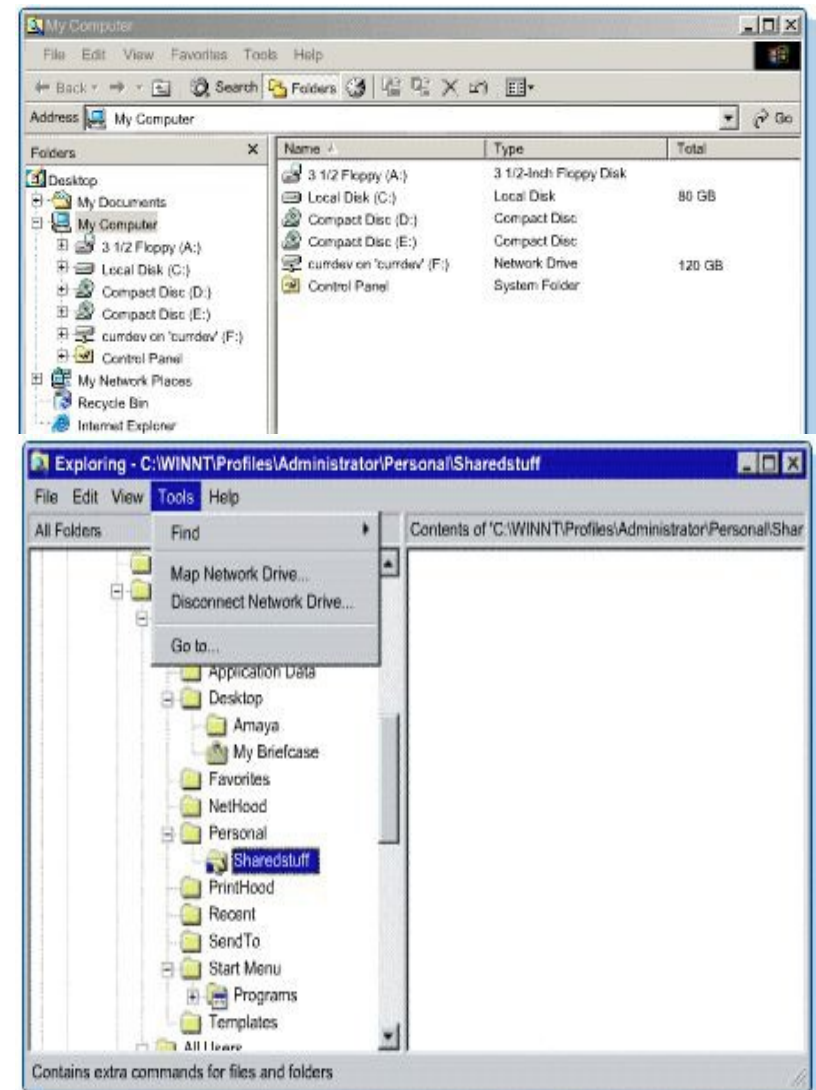
Il 95% del risparmio sui costi in azienda deriva dalla riduzione di hardware, software e infrastruttura di backup. E il servizio di backup ti consente di indirizzare il personale IT verso iniziative più strategiche.

What is Drive Mapping?

- La mappatura del drive è uno strumento utile che consente ad un amministratore di condividere le risorse che sono memorizzati su un server.
- Richiede due passaggi:
 - Definire il percorso per la risorsa
 - assegnare un driver letter
- computer client che sono collegati alla rete assegnano un driver letter che agirà come un percorso diretto per accedere a quelle risorse memorizzate su un server in rete.
- Dopo che l'utente identifica una risorsa di rete da utilizzare a livello locale, la risorsa può essere "mappata" come unità.

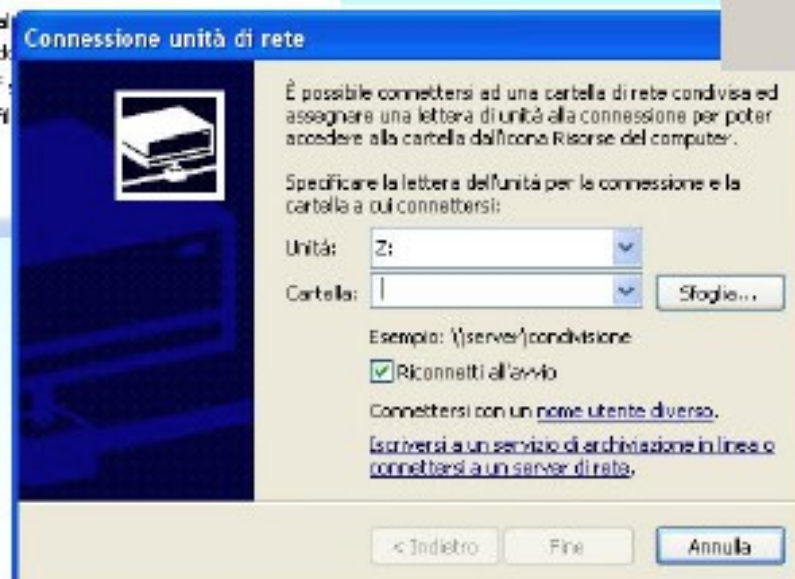
Hard Disk Drives	
 Local Disk (C:)	Local Disk
 New Volume (D:)	Local Disk
Devices with Removable Storage	
 3 1/2 Floppy (A:)	3 1/2-Inch Floppy Disk
 MADDEN02 (E:)	CD Drive
 CD-RW Drive (F:)	CD Drive
Network Drives	
 Shared Files on 'Svr1-phx' (G:)	Network Drive

- Per mappare un disco con Windows Explorer, accedere alla cartella sul sistema remoto in Esplora risorse di Windows selezionando Rete> directory> Nome server> nome cartella condivisa.
- Un altro modo per farlo è quello di scegliere il menu da Strumenti e quindi scegliere Connetti unità di rete.





Connessione unità di rete



Mapping Drives in Windows Networks

- Invece di unità di mappatura tramite Esplora risorse, il comando net use può essere utilizzato. Uso :

`net use drive_letter: \\computer_name\share_name [/user:utente password]`

`net use z: \\Server01\Data`

`net use z: \\Server01\Data /user:Bob passBob`

`net use z: /delete`

- net use può anche essere incorporato in uno script di accesso che viene eseguito automaticamente quando l'utente si collega alla rete.

Mapping Drives in Linux Networks

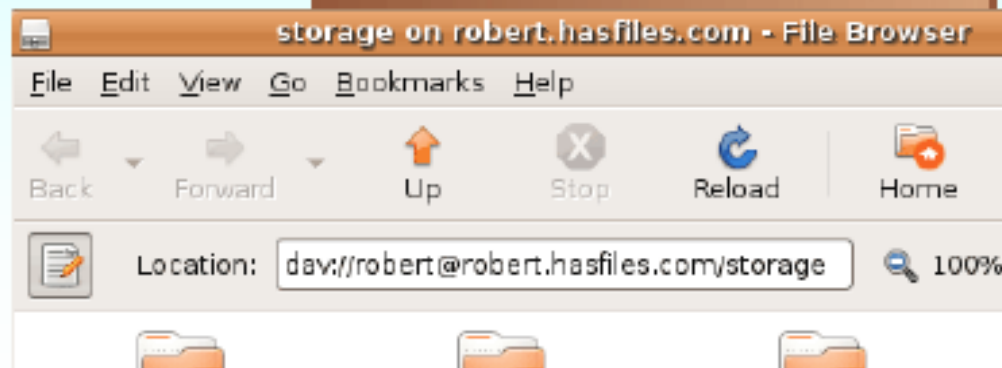
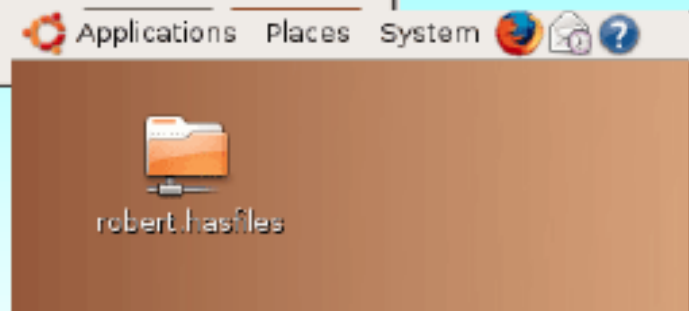
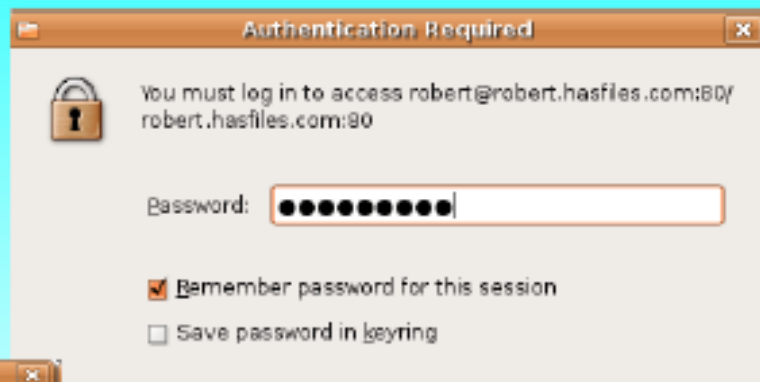
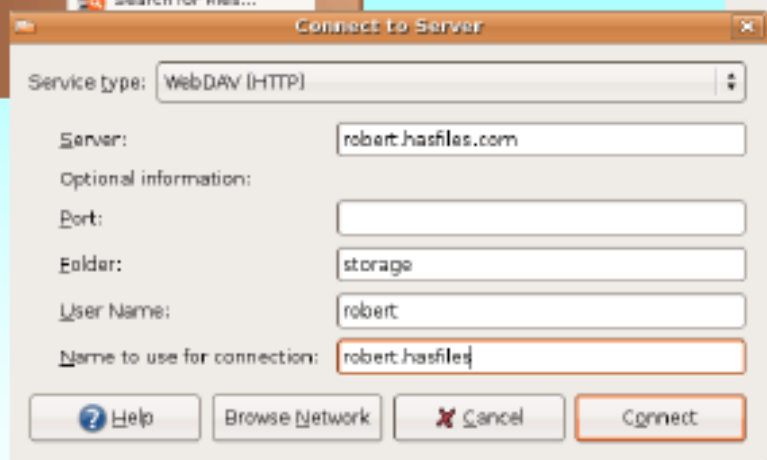
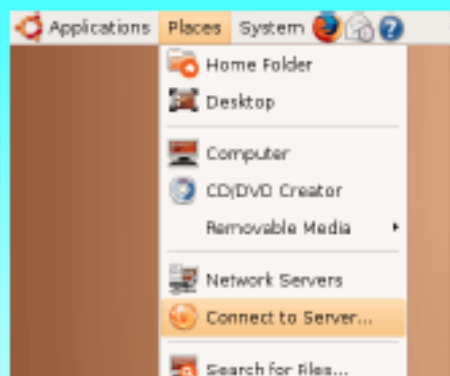
- Per mappare un drive in un server Linux:
 - con un client Windows: è necessario il demone Samba caricato
 - con un client Linux, usare il comando mount per stabilire una connessione alla directory condivisa sul server.

```
# mount //servername/sharename /localdirectory
```

```
# mkdir /localdirectory
```

- La Local directory designata che punta alla remote share indicata con la prima parte del comando è chiamata il punto di mount di directory.
 - La posizione mount point deve esistere già prima di una share che possa essere mappato ad esso.

Accesso remoto via HTTP



Partitions

Using fdisk, mkfs, and fsck

- fdisk è un comando-testo che richiede l'uso di una sola lettera per manipolare le opzioni.

`fdisk / dev/hda2`

`-> p -> ... -> w`

- Una volta apportate le modifiche alla partizione, un filesystem deve essere creato sulla partizione.
- Questo è indicato anche come la formattazione della partizione.

Option	Description
d	Deletes a partition
n	Creates a new partition
p	Prints or displays the partition layout
q	Ends the session without saving any changes
t	Changes a partitions type code
w	Saves the changes made and quits



Fdisk in Windows (old)

```
Microsoft Windows 98
Programma di impostazione del disco rigido
(C)Copyright Microsoft Corp. 1983 - 1998
```

Opzioni di FDISK

Unità disco rigido corrente: 1

Scegliere una delle seguenti opzioni:

1. Crea partizione o unità logica DOS
2. Imposta partizione attiva
3. Elimina partizione o unità logica DOS
4. Visualizza informazioni sulla partizione
5. Cambia l'unità disco rigido corrente

Digitare il numero della selezione: [1]

Premere Esc per uscire da FDISK

Visualizza informazioni sulla partizione

Unità disco rigido corrente: 1

Partizione	Stato	Tipo	Etichetta	Mbyte	Sistema	Uso
C: 1	0	PRM DOS	HDD C	8746	FAT32	100%

Lo spazio su disco totale è pari a 8746 MB (1 MB = 1048576 byte)



fdisk in Ubuntu

```
Disk /dev/sda: 400.0 GB, 400088457216 bytes
255 heads, 63 sectors/track, 48641 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x43af43af
```

Device	Boot	Start	End	Blocks	Id	System
/dev/sda1	*	1	48641	390708801	7	HPFS/NTFS

```
Disk /dev/sdb: 1000.2 GB, 1000204886016 bytes
255 heads, 63 sectors/track, 121601 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0xb62f5470
```

Device	Boot	Start	End	Blocks	Id	System
/dev/sdb1	*	1	95977	770935221	7	HPFS/NTFS
/dev/sdb2		95978	108725	102398310	f	W95 Ext'd (LBA)
/dev/sdb3		108726	121478	102438472+	83	Linux
/dev/sdb4		121479	121601	987997+	82	Linux swap / Solaris
/dev/sdb5		95978	108725	102398278+	7	HPFS/NTFS

Gparted di Ubuntu

GParted

GParedt Edit View Device Partition Help

New Delete Resize/Move Copy Paste Undo Apply

/dev/hda (1.97 GB)

/dev/hda1
1.85 GB

ext3 extended linux-swap used unused

Harddisk Information:

Model: IBM-DTLA-307020
Size: 1.97 GB
Path: /dev/hda
Real Path: /dev/hda

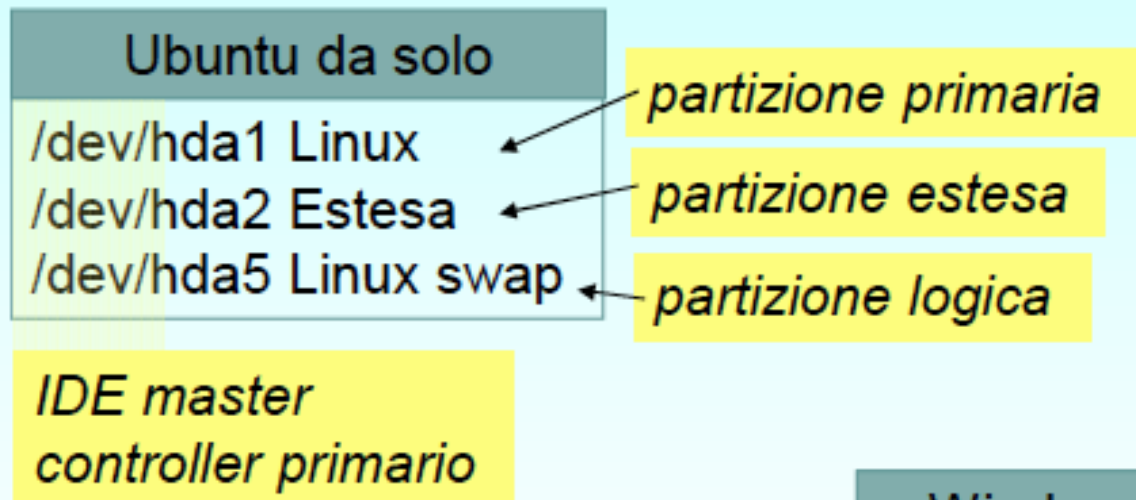
DiskLabelType: msdos
Heads: 255
Sectors/Track: 63
Cylinders: 257
Total Sectors: 4128705

Partition	Filesystem	Size	Used	Unused	Flags
/dev/hda1	ext3	1.85 GB	1.85 GB	0.00 MB	boot
▼ /dev/hda2	extended	125.51 MB	---	---	
/dev/hda5	linux-swap	125.48 MB	---	---	

0 operations pending



Partizioni tipiche in Ubuntu



Windows + Ubuntu	
/dev/hda1	HPFS/NTFS
/dev/hda2	Estesa
/dev/hda3	Linux
/dev/hda5	Linux swap

Using fdisk, mkfs, and fsck

- Utilizzare l'utilità mkfs per creare un filesystem in Linux.

`mkfs [-V] [-t tipofs] [opzioni] dispositivo [blocchi]`

- Una volta che i cambiamenti alla partizione sono stati fatti, un filesystem deve essere creato sulla partizione.
- Questo è indicato anche come formattazione del partizione.

Option	Description
-v	Adding this option to the command will display additional output at the filesystem is created.
-t fstype	This option allows the user to specify the filesystem type that will be created. The fstype would be replaced with something like ext3 for an ext3 filesystem, or msdos for a FAT filesystem, for example.
Options	This parameter is used to specify options specific to the particular filesystem.
device	This parameter specifies the device on which the filesystem was created. Usually it will be the same parameter used with the fdisk command.
blocks	This parameter specifies the size of the filesystems blocks (usually 1024 bytes in size). This value will not always need to be used, because the block size can be determined from the size of the partition.

Using fdisk, mkfs, and fsck

- L'utility fsck viene utilizzata per controllare i file system e riparare file danneggiati.

`fsck [-A] [-V] [-t FS_Type] [-a] [-l] [-r] [-s] filesystem`

`# fsck-t ext2 / dev/hda1`

- Una buona pratica è quella di smontare un sistema di file prima di archiviarlo.
- Per controllare il file system di root, si dovrebbe avviare da un recupero / setup floppy.
- Utilizzare questo programma di utilità spesso per verificare integrità del file system.
- Se fsck effettua le modifiche, riavviare il sistema immediatamente.

Option	Description
-A	This parameter specifies that all files systems marked in <code>/etc/fstab</code> will be checked.
-C	This parameter will display a text-mode progress indicator while the file system is being checked.
-V	This will produce the same output for this command as with the <code>mkfs</code> utility.
-N	This parameter will display the results of what <code>fsck</code> would do, but not actually doing it.
-fsck- options	This parameter is used to specify filesystem check options that fsck cannot interpret. Examples are <code>-a</code> or <code>-p</code> , which perform and automatically check, <code>-r</code> , which performs an interactive check, or <code>-f</code> , which forces a full system check.
filesystems	Specifies the filesystem that is being checked.

Managing System Processes with cron Jobs

- Il modo per pianificare le operazioni da eseguire ad intervalli regolari su un sistema Linux è con i programmi Cron.
- Conosciuto anche come posti di lavoro Cron, in cui pianificano le attività di sistema di manutenzione che vengono eseguite automaticamente (es: svuota directory / tmp).
- Cron è controllato dalle voci nel file / etc / spool / cron and / etc / cron.d directory and file / etc / crontab.
- Cron non è un comando, ma piuttosto è un demone che viene eseguito una volta ogni minuto, scansiona i file igation conf, ed esegue i compiti specificati.
- Ci sono due tipi di Cron jobs: cron system e cron utente.

Managing System Processes with cron Jobs

- Per creare un sistema Cron Job, è necessario modificare il file / etc / crontab.
- Il file inizia con il set di variabili ambientali. Questi impostano alcuni parametri del cron job quali il PATH e MAILTO
- Le altre linee di questo file specificano il minuto, ora, giorno, mese e giorno della settimana il lavoro verrà eseguito (formato 24 ore).
- [*] = Tutto, [xy] = da X a Y, [/ x] = ogni x min, [x, y] = a x e y min.s

The /etc/crontab File

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

#run-parts
01 * * * * root run-parts /etc/cron.hourly
02 * * * * root run-parts /etc/cron.daily
22 * * * * root run-parts /etc/cron.weekly
42 * * * * root run-parts /etc/cron.monthly

0-59/5 * * * * root /usr/bin/mrtg /etc/mrtg/mrtg.cfg
```

- 0 8 * * *
root echo "Buongiorno!"
- / 5 * 15 * *
root / bin / ls / var / log> / temp / ls.out

1. minute 0-59
2. hour 0-23
3. day of month 1-31
4. month 1-12
5. day of week 0-7
6. proprietario
7. il comando viene eseguito

* Può essere usato come tutti,
gamma (0-4,8-12) e l'elenco (1,2,5,9)
sono ammessi

Altra possibilità di System Cron Job



Altra possibilità è la creazione di uno script (sh, bash, perl o altro) per l'esecuzione dell'operazione desiderata. Tale script andrà inserito in una delle directory seguenti

- /etc/cron.hourly

- /etc/cron.daily

- /etc/cron.monthly

- /etc/cron.weekly

per poter essere eseguito ad intervalli ben definiti (se non specificato, alle 4:00)

Managing System Processes with cron Jobs

- Per creare un Cron Job utente, è necessario utilizzare il crontab utility.

```
crontab [user-u] [-l |-e |-r] [file]
```

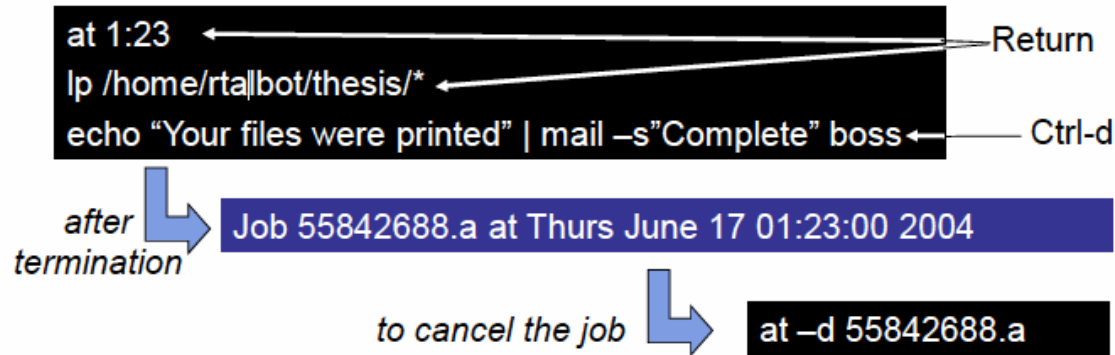
- Se un utente non è specificato, il job di cron dell'utente sarà creato per l'utente corrente.
- file è il file che contiene i comandi crontab con la stessa sintassi utilizzata per i processi di sistema Cron.

```
crontab -u jsmith myTest.cron
```

```
# /home/jsmith/myTest.cron  
# User Cron Job Test  
MAILTO=jsmith@localhost  
* * * * * jsmith echo "How are you?"
```

Managing System Processes with cron Jobs

- Il comando **at** è simile ad usare cron, al momento e / o la data specificata dal comando.



- Per i diversi comandi, è meglio metterli in un file

```
at 8:00 -f scheduledJobs
```


Managing System Processes with at command

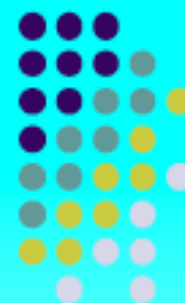
Managing System Processes with Cron Jobs

Format	Action
<code>at hh:mm</code>	Schedules job at the hour (hh) and minute (mm) specified,using a 24-hour clock.
<code>at hh:mm month day year</code>	Schedules job at the hour (hh) minute (mm), month, day,and year specified.
<code>at -l</code>	Lists scheduled jobs; an alias for the atq command.
<code>at now +count time-units</code>	Schedules the job right now plus count number of time-units; time units can be minutes, hours, days, or weeks.
<code>at -d job_id</code>	Cancels the job with the job number matching job_id; analias for the atrm command.

Core Dumps

- Core dump è una registrazione della memoria che un programma stava usando al momento del crash.
- L'obiettivo di Core Dump è quello di permettere ai programmatori di studiare il file , di capire esattamente che cosa ha causato il programma di crash.
- Per individuare i file di base (non solo) su un sistema Linux:

```
# Find core /-name
```
- Le principali proprietà del file Core sono:
 - Il proprietario del file indica che ha eseguito il programma
 - La data di creazione del file core è la data in cui il crash si è verificato e quando il core dump è stato creato
 - Creating Program properties dei file core vi diranno che programma si è bloccato e ha generato il file di core dump (usare gdb)



```
arpum - PuTTY
I A hello.c
#include <stdio.h>

int main()
{
    int* pointer = NULL;
    puts("Hello world");
    *pointer = 42;
    return 0;
}
File hello.c saved
```



```
arpum - PuTTY
berkes@arpum:~$ ulimit -c unlimited
berkes@arpum:~$ gcc -o hello -g -Wall hello.c
berkes@arpum:~$ ./hello
Hello world
Segmentation fault (core dumped)
berkes@arpum:~$ ls -l core*
-rw----- 1 berkes users 65536 Jan 25 17:38 core
berkes@arpum:~$
```

```
arpum - PuTTY
Segmentation fault (core dumped)
berkes@arpum:~$ ls -l core*
-rw----- 1 berkes users 65536 Jan 25 18:21 core
berkes@arpum:~$ gdb hello core
Core was generated by './hello'.
Program terminated with signal 11, Segmentation fault.
Reading symbols from /lib/libc.so.6...done.
Loaded symbols for /lib/libc.so.6
Reading symbols from /lib/ld-linux.so.2...done.
Loaded symbols for /lib/ld-linux.so.2
#0  0x0804834e in main () at hello.c:7
7      *pointer = 42;
(gdb) bt
#0  0x0804834e in main () at hello.c:7
#1  0x4002ebb9 in __libc_start_main () from /lib/libc.so.6
(gdb) quit
berkes@arpum:~$
```



Ubuntu core dumps

```
core.3737
Overview [threaddump] 02:54:31 PM [heapdump] 02:54:29 PM
core.3737
Thread Dump

Thread 3802 *Timer-5*: (state = BLOCKED)
  at java.lang.Object.wait(Native Method)
  - waiting on <0xaa1266c8> (a java.util.TaskQueue)
  at java.util.TimerThread.mainLoop(Timer.java:509)
  - locked <0xaa1266c8> (a java.util.TaskQueue)
  at java.util.TimerThread.run(Timer.java:462)

Thread 3740 *DestroyJavaVM*: (state = BLOCKED)

Thread 3801 *Timer-4*: (state = BLOCKED)
  at java.lang.Object.wait(Native Method)
  - waiting on <0xaa1216b0> (a java.util.TaskQueue)
  at java.util.TimerThread.mainLoop(Timer.java:509)
  - locked <0xaa1216b0> (a java.util.TaskQueue)
  at java.util.TimerThread.run(Timer.java:462)

Thread 3800 *pool-1-thread-5*: (state = BLOCKED)
  at sun.misc.Unsafe.park(Native Method)
  at java.util.concurrent.locks.LockSupport.parkNanos(LockSupport.java:198)
  at java.util.concurrent.SynchronousQueue$TransferStack.awaitFulfill(SynchronousQueue.java:424)
  at java.util.concurrent.SynchronousQueue$TransferStack.transfer(SynchronousQueue.java:323)
  at java.util.concurrent.SynchronousQueue.poll(SynchronousQueue.java:874)
  at java.util.concurrent.ThreadPoolExecutor.getTask(ThreadPoolExecutor.java:944)
  at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:906)
  at java.lang.Thread.run(Thread.java:619)

Thread 3798 *ContainerBackgroundProcessor[StandardEngine[con.sun.appserv]]*: (state = BLOCKED)
  at java.lang.Thread.sleep(Native Method)
  at org.apache.catalina.core.ContainerBase$ContainerBackgroundProcessor.run(ContainerBase.java:1800)
  at java.lang.Thread.run(Thread.java:619)

Thread 3797 *ContainerBackgroundProcessor[StandardEngine[con.sun.appserv].StandardHost[server].StandardContext[/__WSApplictien
  at java.lang.Thread.sleep(Native Method)
  at org.apache.catalina.core.ContainerBase$ContainerBackgroundProcessor.run(ContainerBase.java:1800)
  at java.lang.Thread.run(Thread.java:619)

Thread 3796 *ContainerBackgroundProcessor[StandardEngine[con.sun.appserv].StandardHost[server].StandardContext[/__wscx-service
  at java.lang.Thread.sleep(Native Method)
  at org.apache.catalina.core.ContainerBase$ContainerBackgroundProcessor.run(ContainerBase.java:1800)
  at java.lang.Thread.run(Thread.java:619)

Thread 3794 *ContainerBackgroundProcessor[StandardEngine[con.sun.appserv].StandardHost[server].StandardContext[]]*: (state =
  at java.lang.Thread.sleep(Native Method)
  at org.apache.catalina.core.ContainerBase$ContainerBackgroundProcessor.run(ContainerBase.java:1800)
  at java.lang.Thread.run(Thread.java:619)
```

Core Dumps

- Al fine di gestire in modo efficace i processi di sistema su un Sistema Linux, è importante essere in grado di determinare quali processi sono in esecuzione su un sistema ,e quali sono critici e non critici.
- processi che sono attualmente in esecuzione su un Sistema Linux possono essere visti usando il ps comando.
- Example:

`ps -A -forest`

Option	Description
<code>-A, -e</code>	If the <code>ps</code> command is issued by itself, it will only display the processes that are currently running in the terminal, which doesn't provide much information. These options will cause the <code>ps</code> command to display information about all the processes that are currently running on the system. The <code>-A</code> and <code>-e</code> options will display all the process that are currently running on the system. The <code>-x</code> option will display all the processes that are being used by the user who enters the command.
<code>-u user</code>	This option will let the user display all the processes being used by a specific user. The user's username or user ID can be entered here.
<code>-H, -f, -forest</code>	These options will group processes together in a hierarchy to show the parent-to-child relationship between processes.
<code>-w</code>	By default the <code>ps</code> command shortens its output, so that it all can be displayed on the terminal screen. This option will tell the <code>ps</code> command not to do this. This is helpful when redirecting the output to a text file, which accepts wide output and can be read. To redirect the output to a text file, type use

Core Dumps

Example: `ps -A -forest`

```
[rtalbot@cisco-test1 etc]$ ps -A --forest
PID TTY          TIME CMD
  1 ?            00:00:04 init
  2 ?            00:00:00 keventd
  3 ?            00:00:00 kapid
  4 ?            00:00:00 ksoftirqd_CPU0
  5 ?            00:00:00 kswapd
  6 ?            00:00:00 bdfush
```

```
1088 tty5      00:00:00 mingetty
1087 tty6      00:00:00 mingetty
1088 ?         00:00:00 kdm
1096 ?         1-16:12:44 \_ X
1097 ?         00:00:00 \_ kdm
1109 ?         00:00:00 \_ startkde
1219 ?         00:00:00 \_ kwrapper
1190 ?         00:00:00 kdeinit
1207 ?         00:00:06 \_ artsd
1222 ?         00:00:01 \_ kdeinit
1228 ?         00:00:18 \_ autorun
11433 ?        00:00:04 \_ kdeinit
11435 pts/1      00:00:00 \_ bash
11834 pts/1      00:00:00 \_ ps
1193 ?         00:00:00 kdeinit
```

```
# ps uxf
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1343 0.0 0.5 2360 1024 pts/3 S 16:29 0:00 su -
root 1347 0.0 0.6 2448 1300 pts/3 S 16:29 0:00 - bash
```

Important Information in the `ps -A -forest`

Value	Description
Username	This value is not displayed in this example. However if the <code>-u</code> user option had been added, then the corresponding username would precede the entries.
Process ID (PID)	This is the process number that is used to identify the process. It is important, because it is what is used to terminate or kill a process, which will be described later.
Parent Process ID (PPID)	This is the same as the PID. However, it corresponds to the parent process, and the PID refers to the child process.
TTY	This identifies a terminal and is referred to as the Teletype. For example not all processes will have TTY-like daemons and X programs. Text-mode programs do have these numbers, and they refer to a console or remote login session.
CPU Time	There are two items that are of concern here, the <code>TIME</code> and <code>%CPU</code> headings. The <code>TIME</code> heading indicates the total amount of CPU time consumed, and the <code>%CPU</code> heading represents the percentage of CPU time that is currently being used when the <code>ps</code> command is executed. This heading can help determine what processes might be consuming too much CPU time and need to be terminated. Terminating (killing) processes will be covered in the next section.
CPU Priority	It is possible to give certain processes priority over other processes by restricting CPU usage. The priority of a process is given by its priority code. The default value is zero. Positive numbers represent decreased priority, and negative numbers represent increased priority.
Memory Use	There are a few headings that represent the process memory use. This can help identify certain processes that might be causing a system performance to decrease. For example, the Resident Set Size (RSS) heading represents the memory used by the program, and <code>%MEM</code> shows what percentage of memory the process is using.
Command	The last column represents the command that was used to launch the process.

Core Dumps

- Il comando top ha funzioni molto simili allo strumento di prestazioni di Windows 2000, il quale fornisce dettagliate informazioni riguardanti CPU e RAM.
- Il comando kill può essere usato per terminare il processo.

`# kill -s signal pid`

- L'opzione segnale rappresenta il segnale specificato che è inviato al processo.
- Ci sono 63 diversi parametri che possono essere inseriti per il segnale che viene inviato al processo. Ognuno termina il processo in modo diverso.

```
2:45pm up 5 days, 1:12, 2 users, load average: 0.10, 0.04, 0.14
62 processes: 58 sleeping, 4 running, 0 zombie, 0 stopped
CPU states: 26.0% user, 2.9% system, 0.0% nice, 10.9% idle
Mem: 126068K av, 118236K used, 7832K free, OK shrd, 27564K buff
Swap: 1028152K av, 21764K used, 1006388K free, 34292K cached
```

PID	USER	PRI	NI	SIZE	RSS	SHARE	STAT	%CPU	%MEM	TIME	COMMAND
14882	rtalbot	15	0	12464	12M	10420	S	13.9	9.8	0:00	ksnapshot
1096	root	15	0	12464	12M	10420	S	13.9	9.8	2412m	X
1207	rtalbot	15	0	3940	3792	2540	R	0.7	3.0	0:08	artsd
1222	rtalbot	15	0	9856	8980	8464	S	0.5	7.1	0:04	kdeinit
14846	rtalbot	15	0	11772	11M	9900	R	0.5	9.0	0:01	kdeinit
14883	rtalbot	16	0	7448	6924	6656	S	0.5	5.4	0:00	kdeinit
1218	rtalbot	15	0	9348	8320	8064	S	0.1	6.5	0:01	
224	rtalbot	15	0	10644	9892	9240	S	0.1	7.8		
	rtalbot	15	0	11252	10M	9196	S	0.1			
	rtalbot	15	0	9388	8368	8092	S				
		15	0	1032	1032	836					

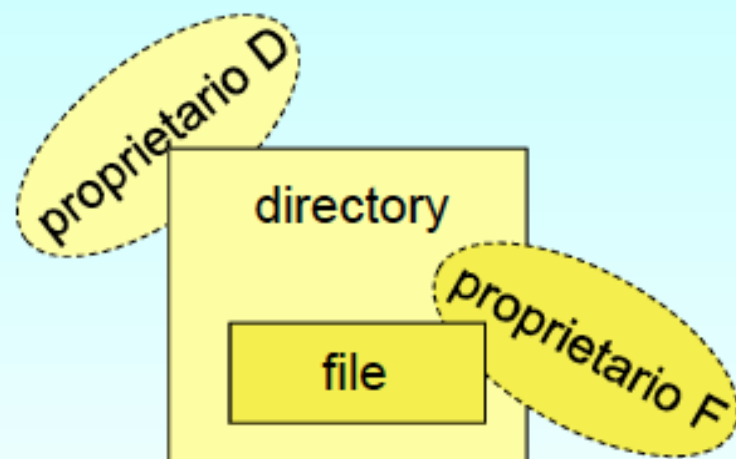
Assigning Permissions for Processes

- In genere, i programmi hanno gli stessi tipi di permesso e sono in grado di leggere gli stessi file con gli stessi permessi dell'utente che esegue il programma.
- Gli utenti normali non possono eseguire il comando su, perché richiede i privilegi di root.
- Programmi come questi vengono eseguiti utilizzando il SUID (Set User ID) o SGID (Set Group ID) bit, che permette di eseguire il programma con l'autorizzazione di chi è proprietario del file, invece che con i permessi d'utente che esegue il programma.

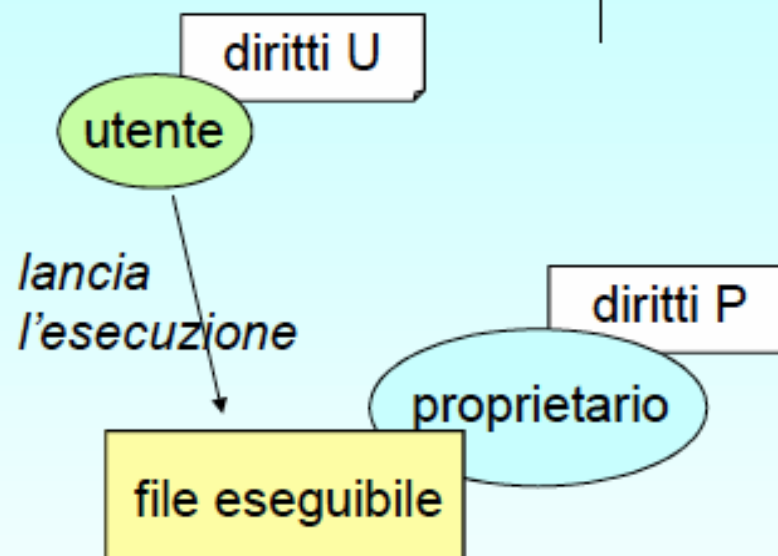
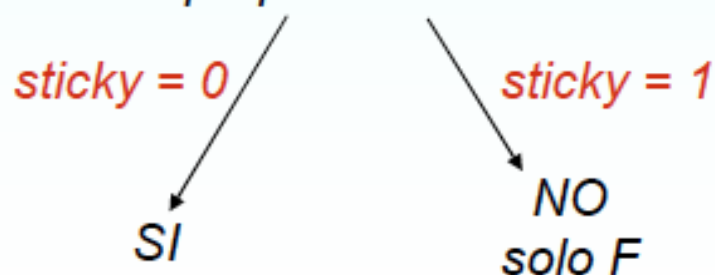
There are a few security risks involved when using the SUID or SGID bit to allow programs to run with the permission of the other users:

- Applying the SUID root permissions for the fdisk command could allow a user to completely erase the hard drive of the server.
- Another security risk is if there are bugs in any of the SUID or SGID programs. If these programs contain problems or bugs and they are executed by users who should not have the permission to do so, those programs could potentially cause more damage to the system than if they were executed with the normal privileges.

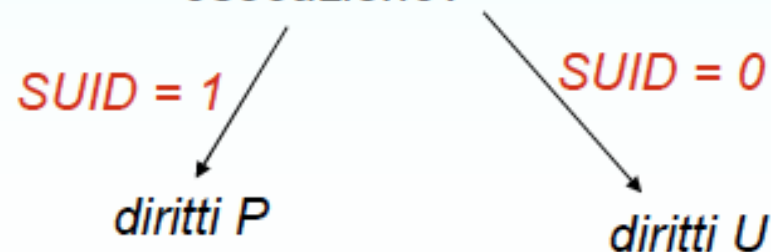
Sticky bit, SUID, SGID



L'utente D (con diritti di accesso alla directory) può modificare il file dell'utente F proprietario del file?



che diritti ha il programma in esecuzione?



Other command for managing processes

- **bg**: colloca il lavoro corrente o di processo specificato in background
- **fg**: colloca il lavoro corrente o di processo specificato in foreground.
- **Nice** : eseguire un programma con priorità di schedulazione modificata; la gamma di priorità su un sistema Linux è di -20 (più scheduling favorevole) a 19 (meno favorevole). [-n xxx] xxx aggiungere alla priorità (valore predefinito 10). Utenti non-root possono modificare solo i propri valori di nice tra 0 e 20
- **renice**: cambiare la priorità di un programma in esecuzione .
[-u user] cambierà la priorità di tutti i processi utente



Comandi &, jobs, bg e fg

- Per lanciare un processo e restituire il controllo alla shell, aggiungere \$ alla fine del comando (background):

```
$ telnet &
```

```
[1] 6694
```

```
$ ftp &
```

```
[2] 6851
```

```
$ ps
```

PID	TTY	TIME	CMD
6192	tty1	00:00:00	bash
6694	tty1	00:00:00	telnet
6851	tty1	00:00:00	ftp
6860	tty1	00:00:00	ps

```
$ jobs
```

[1]-	Stopped	telnet
[2]+	Stopped	ftp



Comandi &, jobs, bg e fg

- Per portare in foreground un processo:

```
$ fg %1          (e poi CTRL Z per sospendere il processo)
```

```
telnet
telnet>
[1]+  Stopped          telnet
```

- Per riportare in background un processo:

```
$ bg %1
```

```
telnet
telnet>
[1]+  Stopped          telnet
```

- CTRL Z per sospendere (stop, ma non quit)
- CTRL C per terminare (o altro comando del processo)



Priorità

- Eseguo un programma in background, per potergli modificare le priorità:

```
$ telnet &
```

```
[1] 8287
```

```
$ ps aux | grep telnet
```

```
1000 8287 0.0 0.0 3169 856 tty1 T 10:37 0:00 telnet
1000 8298 0.0 0.0 3004 752 tty1 R+ 10:37 0:00 grep telnet
```

```
$ renice 0 8287
```

```
8287: old priority 0, new priority 0
```

```
$ renice -1 8287
```

```
renice 8287: setpriority: Permission denied
```



Priorità

- Solo con diritti di root posso migliorare la priorità:



```
$ sudo renice -1 8287
```




```
8287: old priority 0, new priority -1
```


```
$ ps aux | grep telnet
```

```
1000 8287 0.0 0.0 3160 856 tty1 T< 10:37 0:00 telnet
1000 8720 0.0 0.0 3004 768 tty1 S+ 10:48 0:00 grep telnet
```

Disk Management

Volume	Layout	Tipo	File System	Stato	Capacità	Spazio libero	% disponibile	Tolleranza d'errore	Overhead
	Partizione	Di base		Integro (Partizione sconosciuta)	15,03 GB	15,03 GB	100 %	No	0%
	Partizione	Di base		Integro (Partizione sconosciuta)	1,26 GB	1,26 GB	100 %	No	0%
(C:)	Partizione	Di base	NTFS	Integro (Sistema)	60,04 GB	22,55 GB	37 %	No	0%
(G:)	Partizione	Di base	FAT	Integro (Attivo)	3,83 GB	1,40 GB	36 %	No	0%
Volume (E:)	Partizione	Di base	NTFS	Integro	232,88 GB	199,28 GB	85 %	No	0%

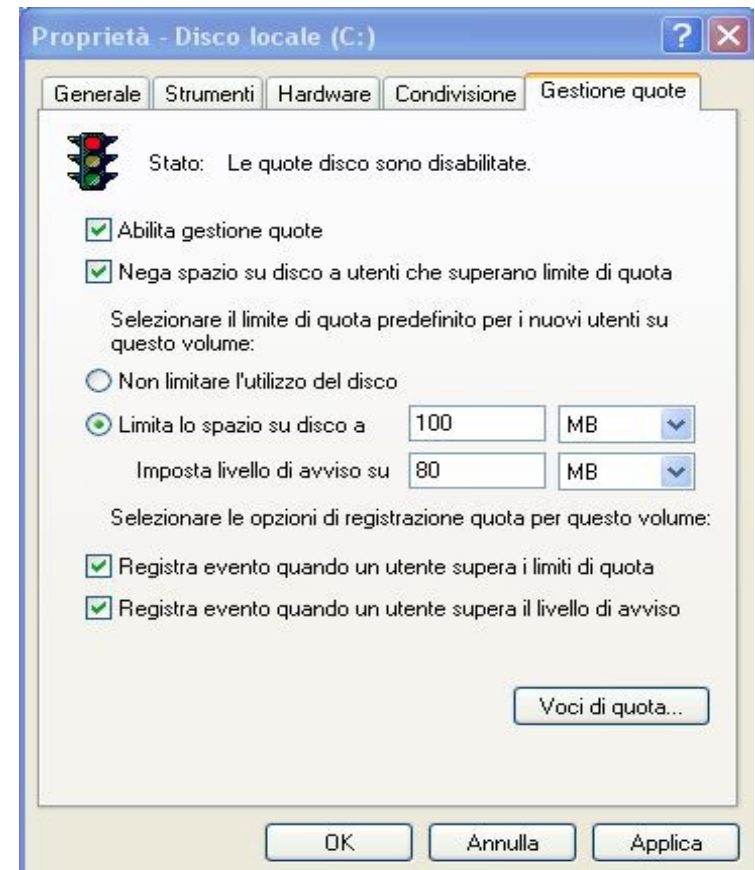
 Disco 0 Di base 232,88 GB Pronto	Volume (E:) 232,88 GB NTFS Integro		
 Disco 1 Di base 76,33 GB Pronto	(C:) 60,04 GB NTFS Integro (Sistema)	15,03 GB Integro (Partizione sconosciuta)	1,26 GB Integro (Partizione sconosciuta)
 Disco 2 Rimovibile 3,83 GB Pronto	(G:) 3,83 GB FAT Integro (Attivo)		

 Partizione primaria

Regolarmente con controllo degli errori e la deframmentazione programmi e la gestione continua di spazio libero su disco, gli amministratori di sistema sono grado di mantenere un sano hard disk.

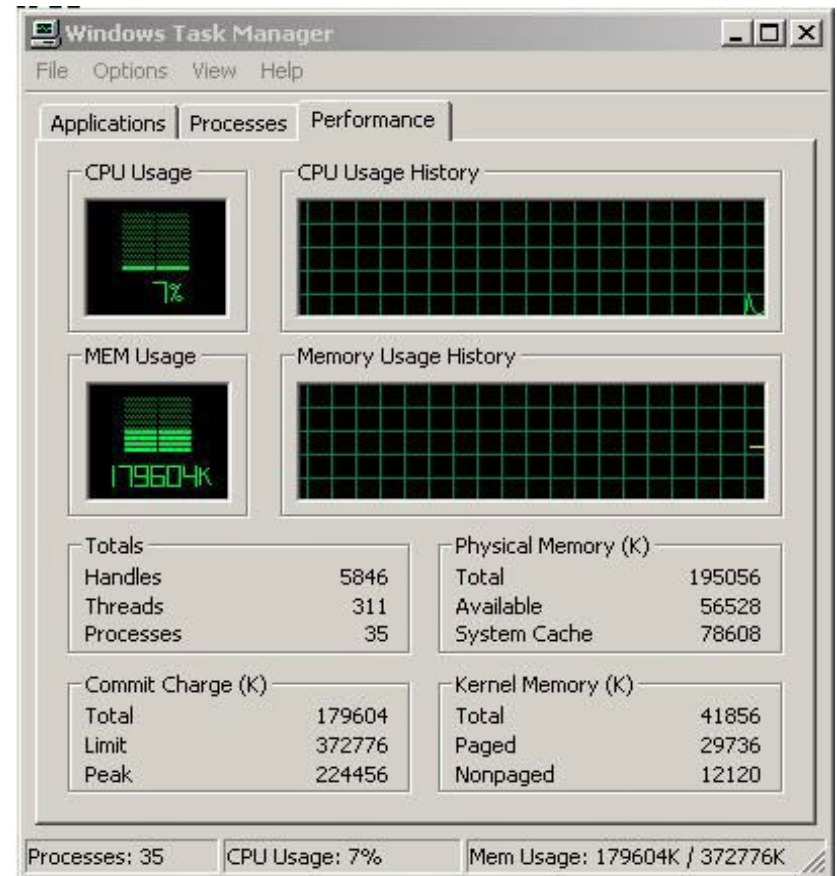
Disk Management

- Un disco di prevenzione è uno strumento di gestione disponibile per gli amministratori di sistema per l'uso di "contingenti" per gli account utente.
- Una quota funge da stoccaggio massimale che limita la quantità di dati di ciascun utente in grado di memorizzare in rete.

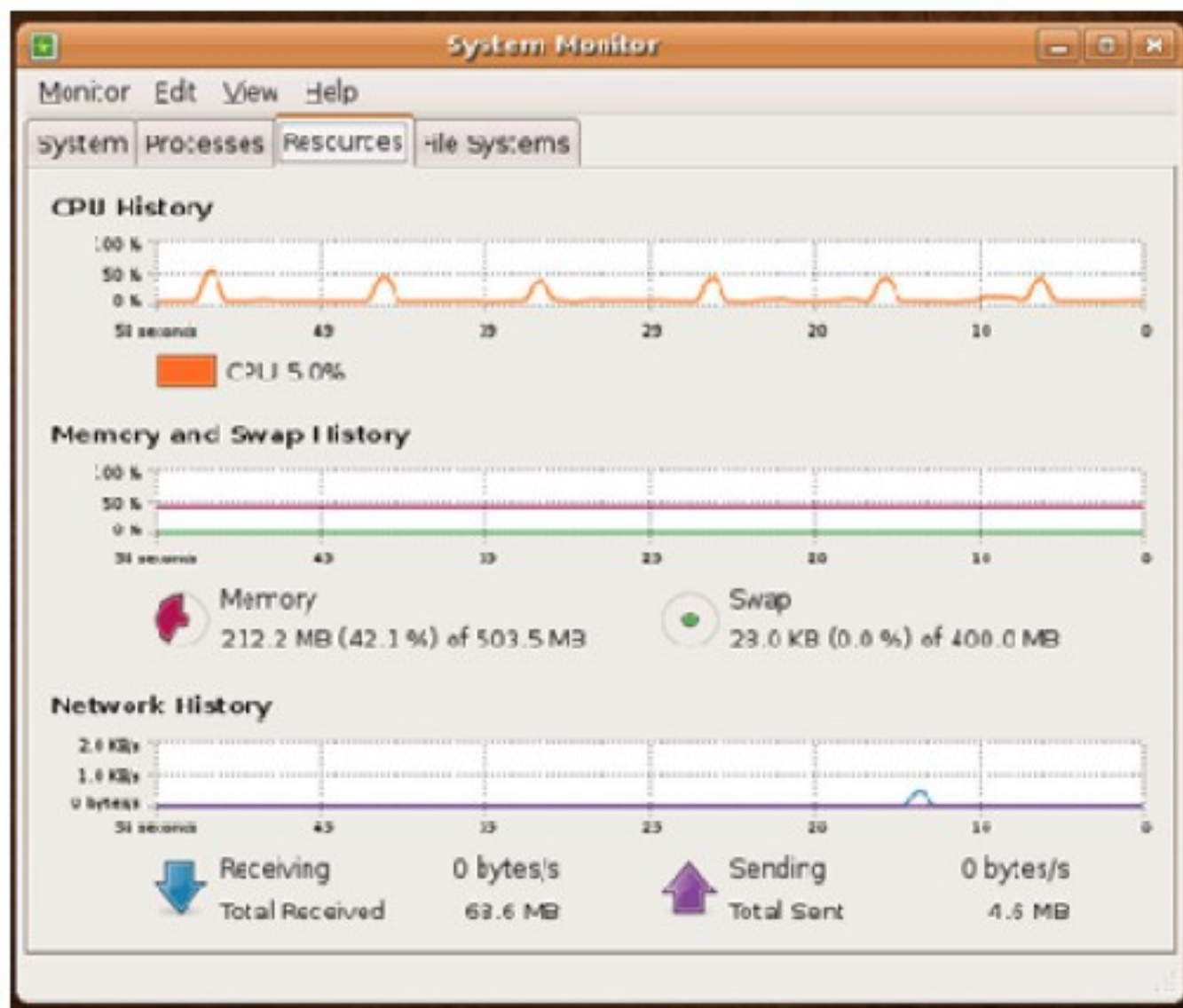


Memory Usage

- Strumenti di diagnostica RAM (memoria) che consentono intensiva analisi sulle applicazioni e i relativi processi in corso che se necessario saranno terminati , sono in genere costruiti nella maggior parte delle piattaforme NOS.
- Gli amministratori di sistema possono compensare la mancanza di memoria attraverso l'uso di "memoria virtuale".
- Alloca la memoria virtuale spazio sul disco rigido e lo tratta come un prolungamento della RAM di sistema.

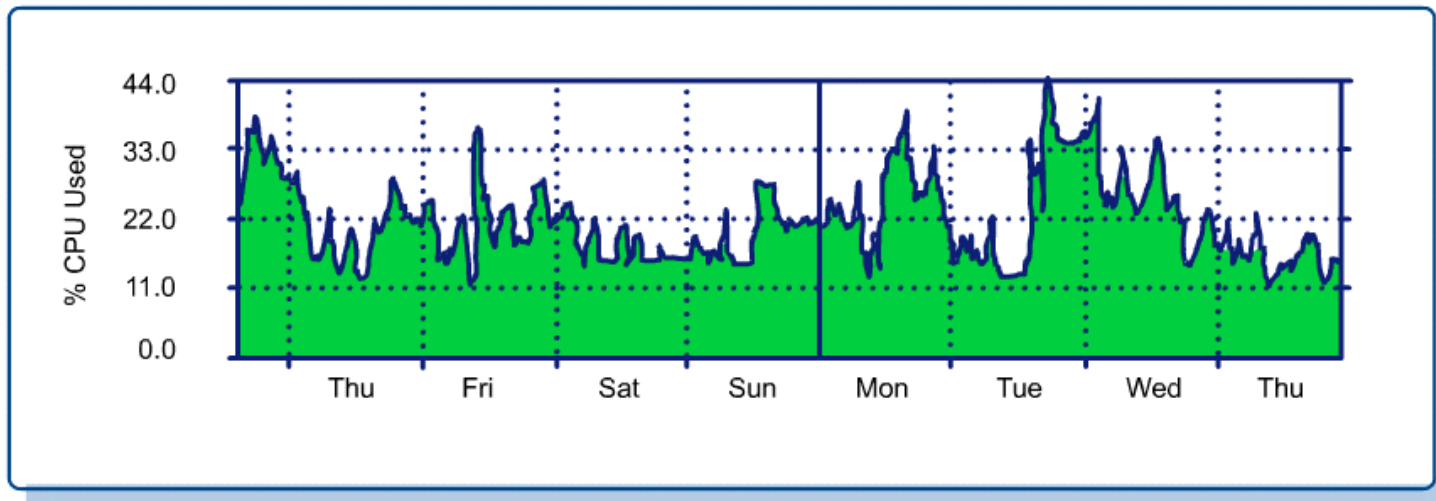


Ubuntu System Monitor



CPU Usage

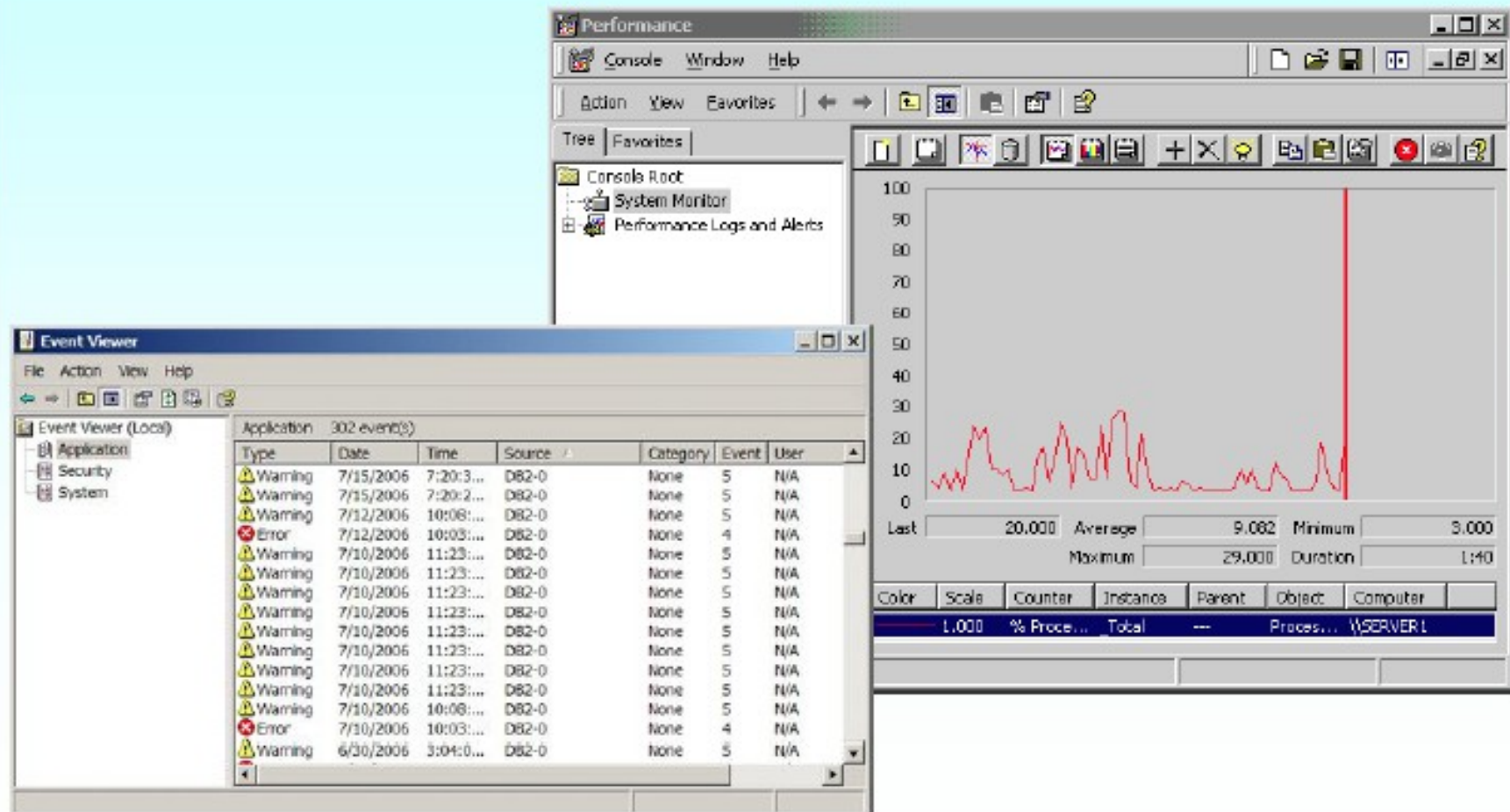
- Tutte le informazioni utilizzate dai NOS, tra cui il NOS stesso, vengono elaborate milioni di volte al secondo dal CPU e stampate su schermo per una visione dell'utente.
- Built-in strumenti vengono comunemente fornite per permettere sistema amministratori di monitorare l'attuale livello di CPU attività.
- Questo feedback è spesso presentata in termini di percentuale della CPU attualmente utilizzato ed è rinfrescato ad intervalli frequenti.



Reviewing Daily Logs

- La maggior parte dei programmi per computer, i server, i processi di login, come così come il kernel del sistema, record di sintesi dei loro attività nel file di log.
- Queste sintesi possono essere usate e revisionate per vari cose, tra cui il software che potrebbe essere difettoso o tentativi di entrare nel sistema.
- In Windows 2000, lo strumento Gestione computer consente agli utenti di sfogliare gli eventi registrati generati da il NOS.
- Due categorie sotto le Utilità di sistema sono "Visualizzatore eventi" e "Avvisi e registri di prestazioni"

Reviewing Daily Logs



Reviewing Daily Logs

- Linux utilizza log daemon per controllare gli eventi che sono inserito nel registro di sistema.
- Nella maggior parte dei sistemi Linux , i file di registro si trovano nella / var / log.
- I file log sono gestiti dal sistema log daemon (syslogd) e dal daemon log del kernel (klogd).
- Questi due demoni sono configurati utilizzando syslog.conf

The syslog.conf File

```
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.* /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none /var/log/messages

# The authpriv file has restricted access.
authpriv.* /var/log/secure

# Log all the mail messages in one place.
mail.* /var/log/maillog

# Log cron stuff
cron.* /var/log/cron

# Everybody gets emergency messages
*.emerg *

# Save news errors of level crit and higher in a special file.
uucp,news.crit /var/log/spooler

# Save boot messages also to boot.log
local7.* /var/log/boot.log
~
"/etc/syslog.conf" [readonly] 26L, 693C 1,1 All
```

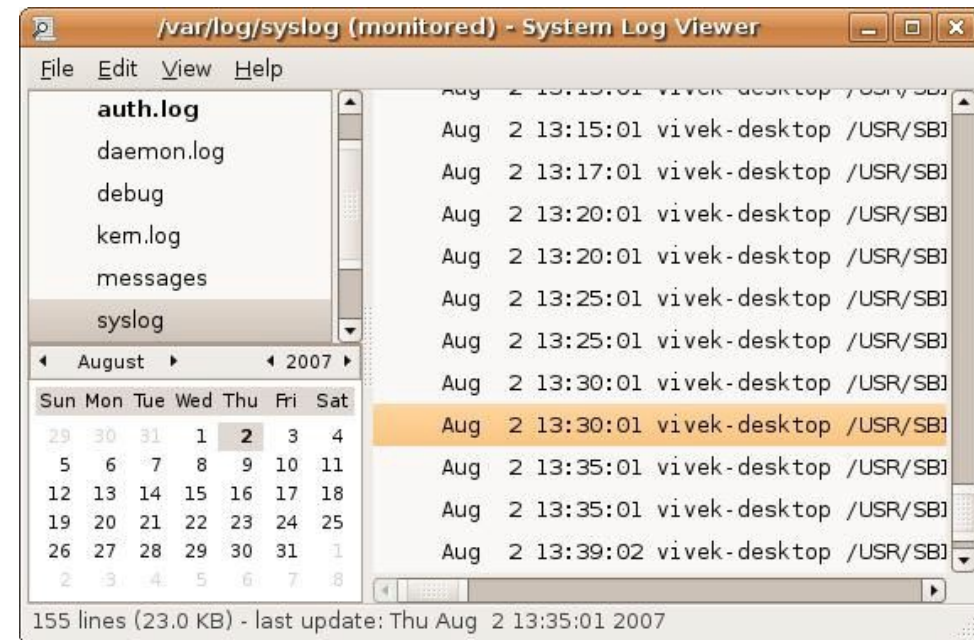

Reviewing Daily Logs

I file di log di Linux e l'utilizzo:

- / var / log / messages: messaggi di registro generali
- / var / log / boot: Sistema di log di boot
- / var / log / auth.log: Accesso utente e autenticazione
- / var / log / daemon.log: Servizi in esecuzione come squid, ntpd e altri messaggio di log per questo file
- / var / log / faillog: l'utente non è riuscita file di log di accesso

Text view:

```
tail -f /var/log/auth.log  
more /var/log/daemon.log  
cat /var/log/mysql.err  
less /var/log/messages  
grep -i fail /var/log/boot
```





Ubuntu /var/log

- Vediamo un file di log:

```
$ ls -al /var/log/auth*
```

```
-rw-r----- 1 syslog adm      554 2009-04-20 15:17 auth.log
-rw-r----- 1 syslog adm 149.078 2009-04-20 15:11 auth.log.0
-rw-r----- 1 syslog adm   9.467 2009-04-18 10:42 auth.log.1.gz
-rw-r----- 1 syslog adm    876 2009-04-16 12:30 auth.log.2.gz
```

```
$ cat /var/log/auth.log | grep "Apr 21"
```

```
Apr 21 14:11:04 amemo CRON[9747]: PAM unable to dlopen(/lib/sec
Apr 21 14:11:04 amemo CRON[9747]: PAM [error: /lib/security/pam
Apr 21 14:11:04 amemo CRON[9747]: PAM adding faulty module: /li
Apr 21 14:11:04 amemo CRON[9747]: pam_unix(cron:session): sessi
```

PAM (Pluggable authentication module) è un modulo aggiuntivo ad OpenLDAP e forza i client all'utilizzo di password normalizzate. Utilizza la libreria libpam-cracklib ed un dizionario di password non accettabili.

Ubuntu /var/log



/var/log/auth.log (monitored) - System Log Viewer

File Edit View Help

▼ /var/log

- auth.log
- daemon.log
- messages
- syslog
- Xorg.0.log

▼ 25/04/2009

```
Apr 25 15:17:01 alessandro-laptop CRON[9747]: PAM unable to dlopen(/lib/security/pam_smbpass.so)
Apr 25 15:17:01 alessandro-laptop CRON[9747]: PAM [error: /lib/security/pam_smbpass.so: cannot open sha
Apr 25 15:17:01 alessandro-laptop CRON[9747]: PAM adding faulty module: /lib/security/pam_smbpass.so
Apr 25 15:17:01 alessandro-laptop CRON[9747]: pam_unix(cron:session): session opened for user root by
Apr 25 15:17:01 alessandro-laptop CRON[9747]: pam_unix(cron:session): session closed for user root
```

◀ aprile ▶ 2009 ▶

lun	mar	mer	gio	ven	sab	dom
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3
4	5	6	7	8	9	10

5 lines (554 bytes) - last update: Sat Apr 25 15:17:01 2009

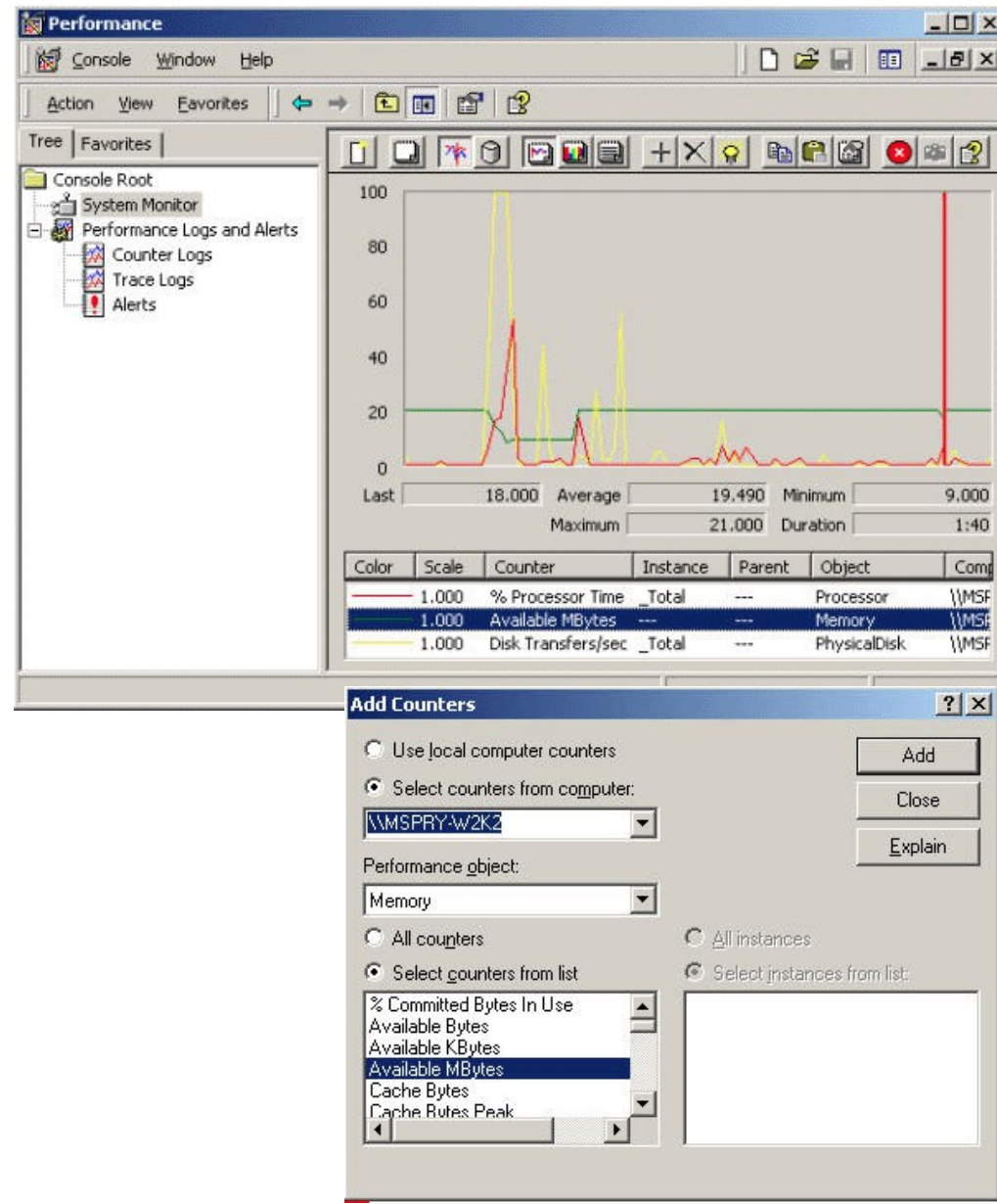
alessandro@alessandro-laptop: ~

File Edit View Terminal Tabs Help

```
Apr 25 15:17:01 alessandro-laptop CRON[9747]: PAM unable to dlopen(/lib/security/pam_smbpass.so)
Apr 25 15:17:01 alessandro-laptop CRON[9747]: PAM [error: /lib/security/pam_smbpass.so: cannot open shared object file: No such file
or directory]
Apr 25 15:17:01 alessandro-laptop CRON[9747]: PAM adding faulty module: /lib/security/pam_smbpass.so
Apr 25 15:17:01 alessandro-laptop CRON[9747]: pam_unix(cron:session): session opened for user root by (uid=0)
Apr 25 15:17:01 alessandro-laptop CRON[9747]: pam_unix(cron:session): session closed for user root
Apr 25 15:54:41 alessandro-laptop gnome-keyring-daemon[5714]: adding removable location: volume_uuid_E122_237A at /media/PKBACK# 001
(END)
```

Checking Resource Usage on Windows 2000 and Windows XP

- Le risorse di sistema sono monitorati in Windows 2000 e Windows XP con lo Strumento Prestazioni.
- Questa applicazione si trova sotto il menu Start> Programmi> Sistema Amministrazione> Opzione di menu Prestazioni.
- Gli utenti possono quindi fare clic destro su il grafico e selezionare Aggiungi Contatori per specificare quali risorse di sistema monitorare nel grafico.



Checking Resource Usage on Linux

- Il comando **df** serve per visualizzare la quantità di spazio disco attualmente disponibile per i vari file system sulla macchina.
- Quando viene specificato un nome di directory, il comando **du** restituisce l'uso del disco per entrambi i contenuti della directory e il contenuto di tutte le sottodirectory sotto esso.
- Le funzioni di comando **top** molto simile al Windows 2000 Strumento prestazioni, fornisce informazioni dettagliate per quanto riguarda CPU e RAM.



Il comando df

- Il comando **df** (*disk space of the file system*) visualizza l'ammontare di spazio libero e occupato su tutti i dischi attualmente montati.
 - [**-h**] Aggiunge a ciascuna dimensione un suffisso, come M per megabyte binario («mebibyte»)
 - [**-i**] Dà informazioni sull'uso degli inode, invece che dei blocchi
 - [**-l**] Limita il risultato ai soli filesystem locali
 - [**-T**] Stampa il tipo di ciascun filesystem

```
rtalbot@cisco-test1:~ -Shell - Konsole
Session Edit View Settings Help

[rtalbot@cisco-test1 rtalbot]$ df -hT
Filesystem      Type      Size  Used Avail Use% Mounted on
/dev/hda1       ext3      4.9G  1.5G  3.1G  32% /
/dev/hda3       ext3     12G   6.2G  5.6G  52% /home
none            tmpfs     62M    0    61M   0% /dev/shm
[rtalbot@cisco-test1 rtalbot]$
```



Il comando du

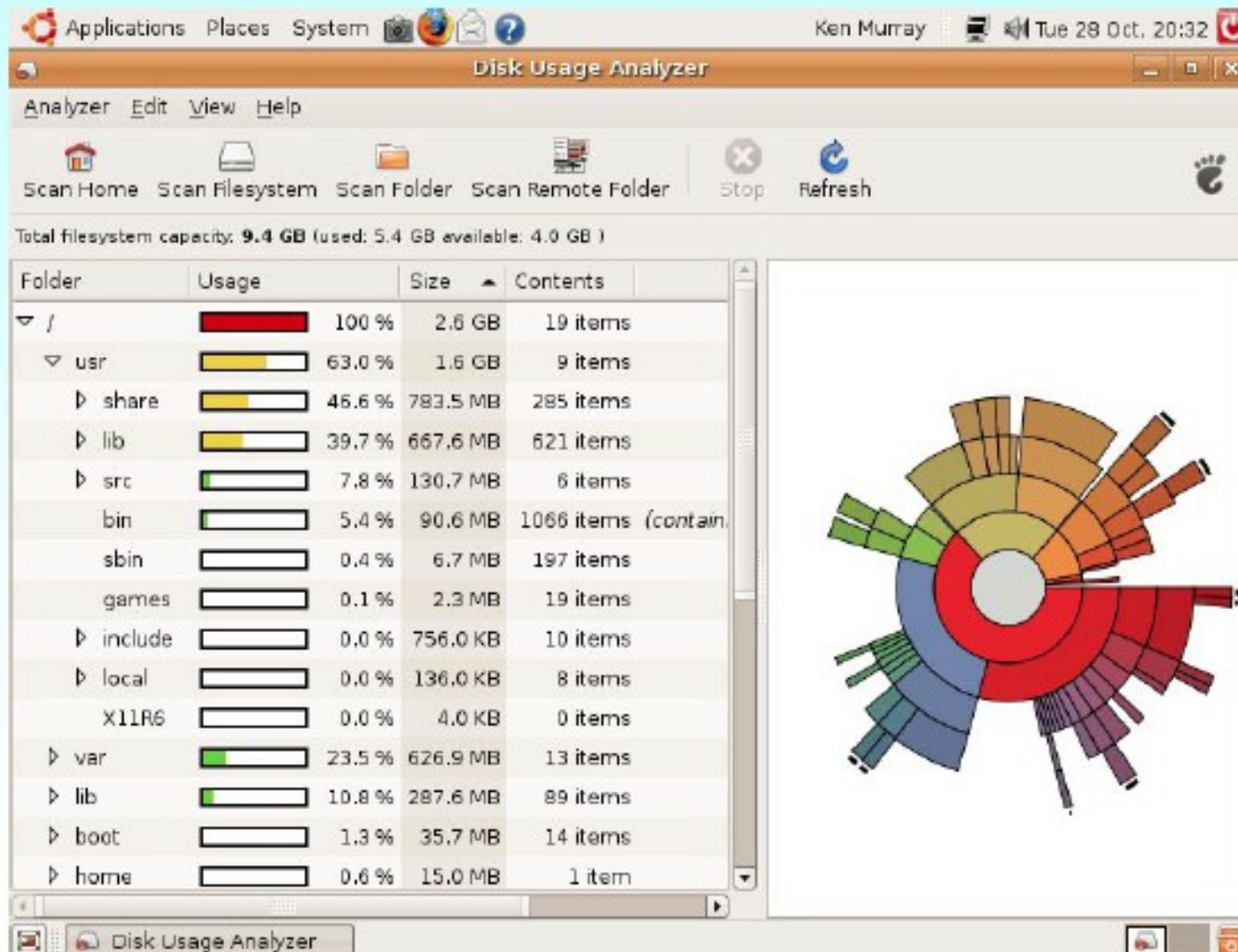
- Il comando **du** (*disk usage statistics*) visualizza la quantità usata di spazio su disco da una certa directory

The du Command

```
[rtalbot@cisco-test1 rtalbot]$ su root
Password:
[root@cisco-test1 rtalbot]# du /usr -h --max-depth=1
142M    /usr/bin
483M    /usr/lib
3.0M    /usr/libexec
12M     /usr/sbin
640M    /usr/share
88M     /usr/x11R6
4.0k    /usr/dict
4.0k    /usr/etc
3.9M    /usr/games
4.3M    /usr/include
92k     /usr/local
4.0k    /usr/src
1.4M    /usr/kerberos
8.8M    /usr/i386-glibc21-linux
1.4G    /usr/
[root@cisco-test1 rtalbot]#
```

- [-c]** produce un totale finale
- [-h]** risultati in formato comprensibile
- [-S]** esclude le sottodirectory
- [-s]** solo il totale per ogni argomento
- [-x]** salta le dir. degli altri file system
- [--max-depth=N]** fino ad una profondità di N livelli

Disk Usage grafica (baobab)





Il comando top

- Il comando **top** mostra i processi che usano più CPU, e fornisce in tempo reale istantanee dell'attività del processore.

```
mc@hardy: ~  
File Modifica Visualizza Terminale Scheda Ajuto  
Cpu(s):100.0%us, 0.0%sy, 0.0%ni, 0.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st  
Mem: 515608k total, 510012k used, 5596k free, 18584k buffers  
Swap: 987956k total, 0k used, 987956k free, 228452k cached  


| PID  | USER | PR | NI | VIRT  | RES  | SHR  | S | %CPU | %MEM | TIME+   | COMMAND         |
|------|------|----|----|-------|------|------|---|------|------|---------|-----------------|
| 6017 | mc   | 20 | 0  | 67132 | 6464 | 5152 | S | 96.9 | 1.3  | 0:26.39 | evolution-data- |
| 5580 | root | 20 | 0  | 59668 | 33n  | 9468 | S | 0.7  | 6.6  | 0:02.22 | Xorg            |
| 5985 | mc   | 20 | 0  | 30408 | 18n  | 9812 | S | 0.7  | 3.7  | 0:00.50 | python          |
| 6117 | mc   | 20 | 0  | 70832 | 43n  | 6828 | S | 0.7  | 8.6  | 0:05.06 | compiz          |
| 1    | root | 20 | 0  | 2844  | 1692 | 544  | S | 0.0  | 0.3  | 0:01.18 | init            |
| 2    | root | 15 | -5 | 0     | 0    | 0    | S | 0.0  | 0.0  | 0:00.00 | kthreadd        |
| 3    | root | RT | -5 | 0     | 0    | 0    | S | 0.0  | 0.0  | 0:00.00 | migration/0     |
| 4    | root | 15 | -5 | 0     | 0    | 0    | S | 0.0  | 0.0  | 0:00.00 | ksoftirqd/0     |
| 5    | root | RT | -5 | 0     | 0    | 0    | S | 0.0  | 0.0  | 0:00.00 | watchdog/0      |
| 6    | root | 15 | -5 | 0     | 0    | 0    | S | 0.0  | 0.0  | 0:00.00 | events/0        |
| 7    | root | 15 | -5 | 0     | 0    | 0    | S | 0.0  | 0.0  | 0:00.00 | khelper         |
| 42   | root | 15 | -5 | 0     | 0    | 0    | S | 0.0  | 0.0  | 0:00.02 | kblockd/0       |
| 45   | root | 15 | -5 | 0     | 0    | 0    | S | 0.0  | 0.0  | 0:00.00 | kacpid          |
| 46   | root | 15 | -5 | 0     | 0    | 0    | S | 0.0  | 0.0  | 0:00.00 | kacpi_notify    |
| 155  | root | 15 | -5 | 0     | 0    | 0    | S | 0.0  | 0.0  | 0:00.00 | kseriod         |
| 193  | root | 20 | 0  | 0     | 0    | 0    | S | 0.0  | 0.0  | 0:00.00 | pdflush         |
| 194  | root | 20 | 0  | 0     | 0    | 0    | S | 0.0  | 0.0  | 0:00.00 | pdflush         |

  
mc@hardy:~$ kill -9 6017  
mc@hardy:~$
```

- Mostra una lista dei task del sistema che fanno un uso più intenso della CPU, e può mettere a disposizione un'interfaccia interattiva per manipolare i processi.