

I LOG dell'Amministratore ai fini Privacy - mini howto

Augusto Scatolini (webmaster@comunecampagnano.it)

Ver. 1.0 (maggio 2009)



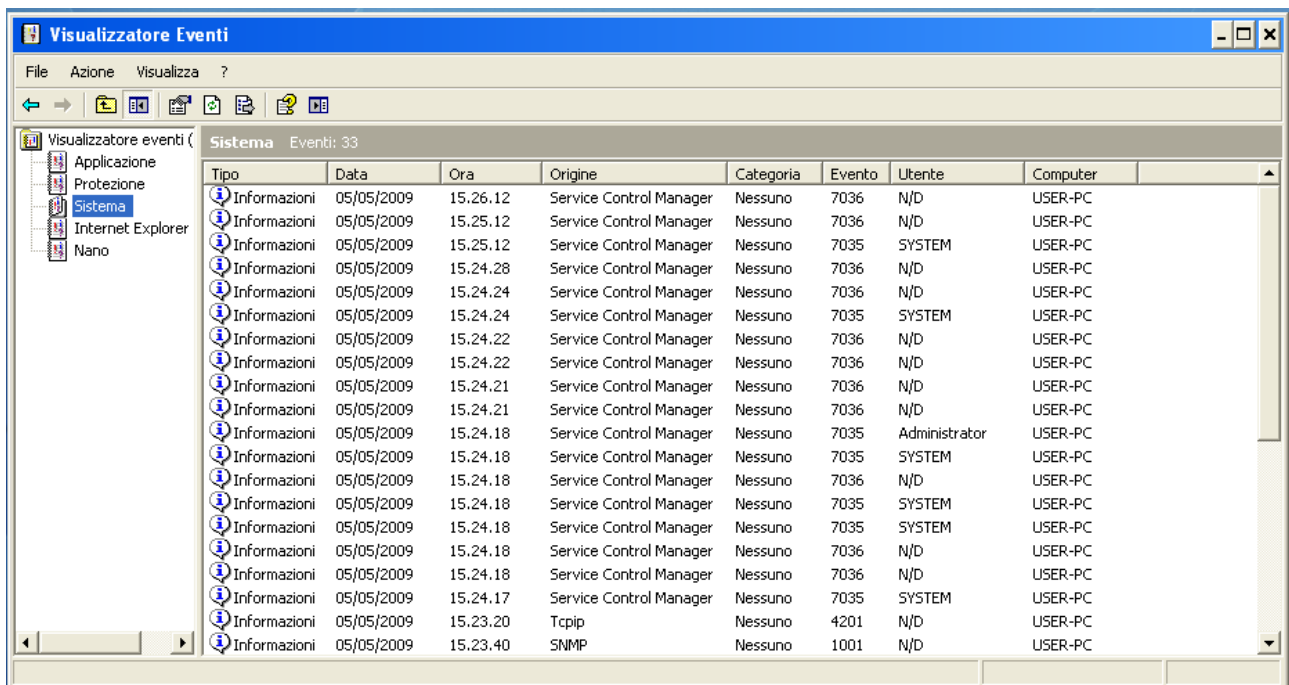
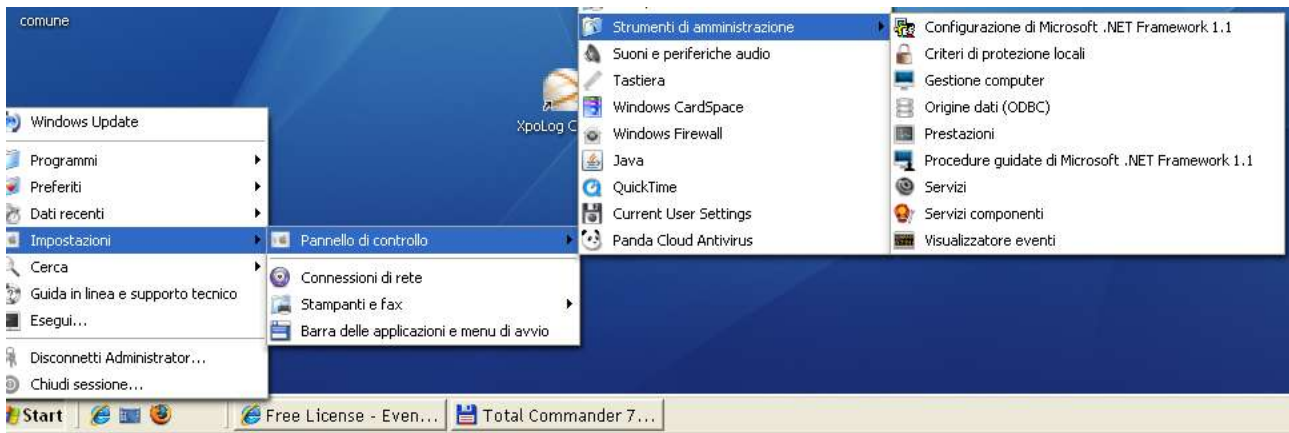
GLI EVENTI DI SISTEMA (LOG) DI WINDOWS

GLI EVENTI DI SISTEMA (LOG) DI GNU/Linux

L'unico modo per visualizzarne il contenuto è attraverso un apposita applicazione che si chiama **eventvwr.msc** che si trova nella cartella **Sistem32**

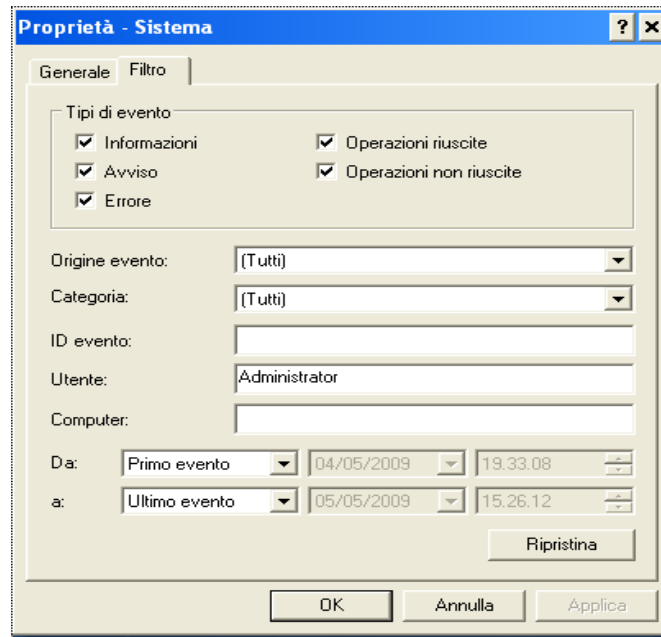
Graficamente l'accesso a tale programma è descritto di seguito:

Start → -impostazioni → Pannello di Controllo → Strumenti di Amministrazione → Visualizzatore eventi

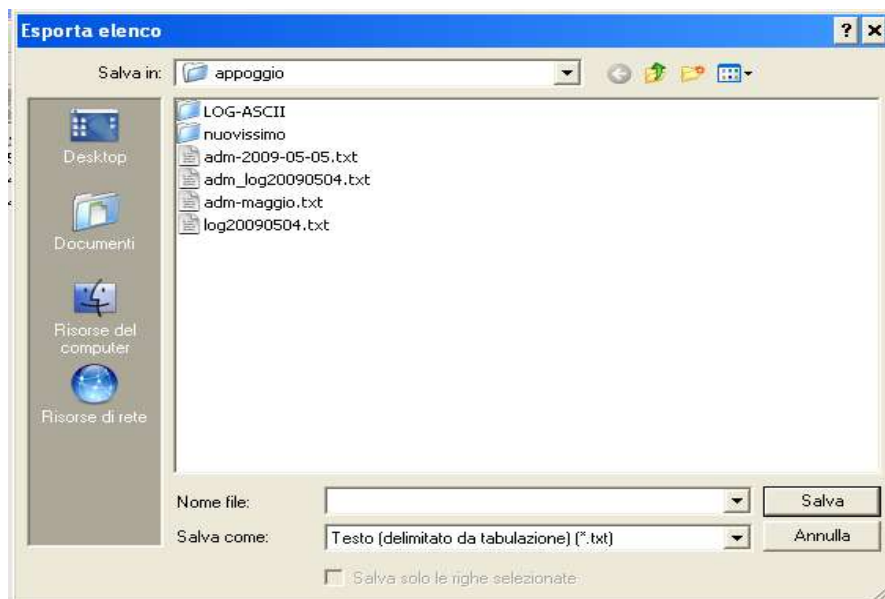


La prima cosa che si nota è l'assenza della descrizione dell'evento che ha generato il LOG

Si possono filtrare gli eventi per utente (Administrator)

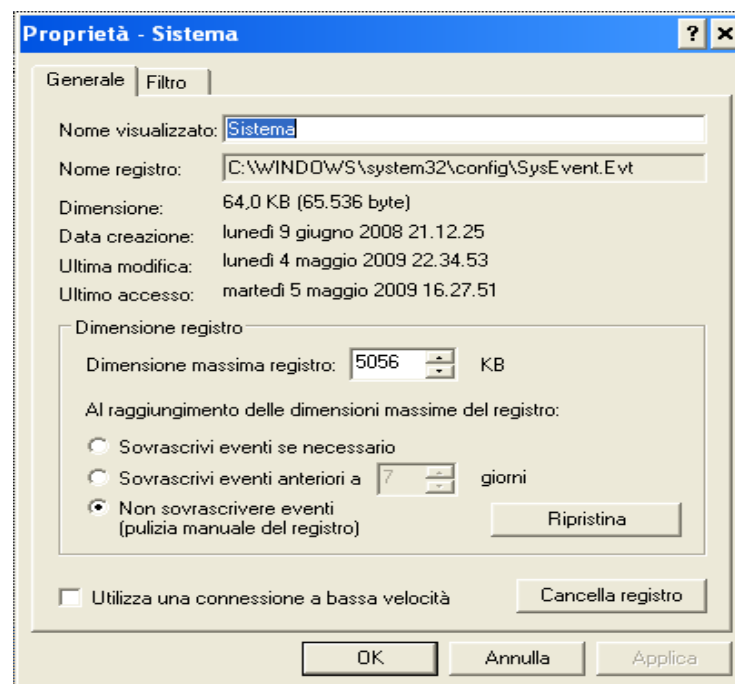


Si può esportare il contenuto in un file ASCII



Nelle proprietà del registro si possono settare vari parametri:

- la dimensione massima del registro in KB
- se sovrascrivere gli eventi o meno, raggiunta la dimensione massima
- se sovrascrivere gli eventi anteriori a X giorni
- se cancellare o meno il registro



Quello che assolutamente non si può fare è cancellare e/o modificare un evento

PROVVEDIMENTO 27 novembre 2008

Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.

omissis

f) Registrazione degli accessi.

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

omissis

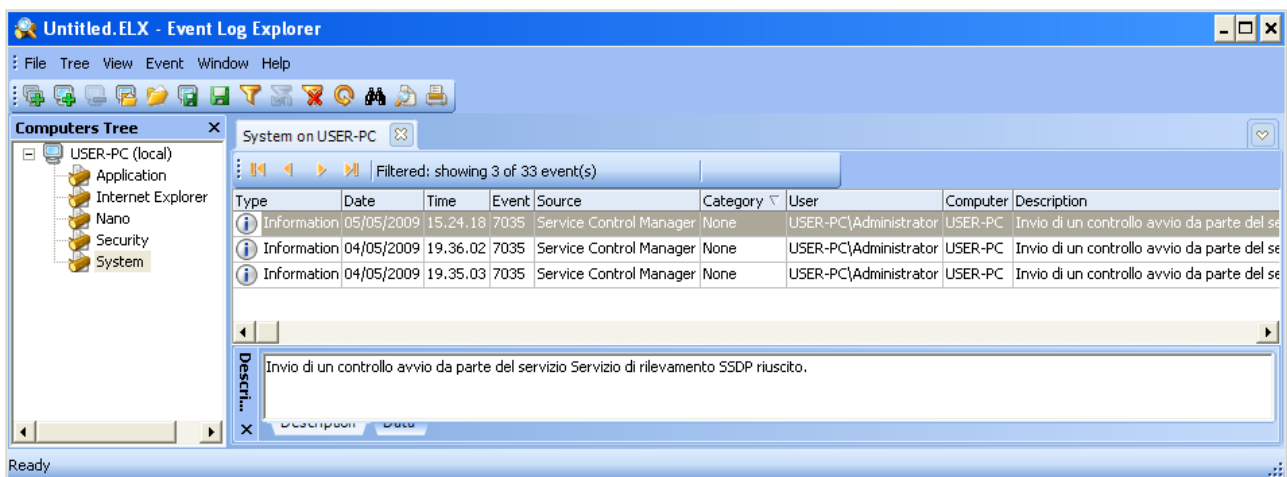
COME (TENTARE DI) OTTEMPERARE ALLE PRESCRIZIONI DEL GARANTE

1° Obiettivo: completezza (descrizione dell'intervento)

2° Obiettivo: filtro (solo i log dell'amministratore)

3° Obiettivo: compressione e inalterabilità

sul sito <http://www.eventlogxp.com/> si può scaricare il programma Event Log Explorer, gratuito con registrazione obbligatoria per ottenere una licenza personale non commerciale.



*** - required fields!**

Full name *

Email address *
(make sure that it's correct)

Street address *

City *

State/province *

Zip/postal code *

Country *

Phone number


Age

Occupation *

Number of computers in your household *

How did you learn of Event Log Explorer which one

Comments and suggestions

 please enter the characters you see in the image *

dopo la registrazione viene inviata all'indirizzo di posta elettronica indicata la chiave di attivazione simile a quella mostrata di seguito

```

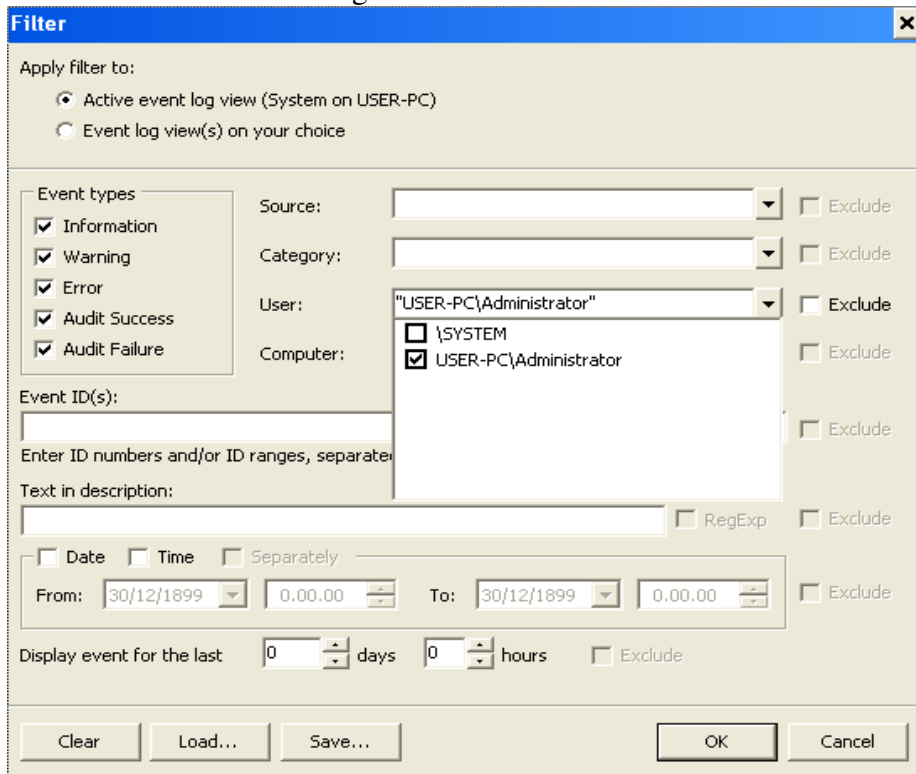
Your registration key is

----- BEGIN KEY -----
0Gh1b+x3XHxYalE6Hcvv8Zi+0+pdL1WBnx2wdaPc
Q8VGhn3nzD2Zoxas9P6n/eRY0ulHOKE1NXW9vgNT
hT+X/lgSzn5kXaseo+iQ4vfFcV4GF7yZ+c9Hxv5e
zJWxFbGNeHU8YsHcl82Xvr98A+BPM8H06xnZQN/B
XuyANIPPr9DnnsEL+u2BqeVSbWCWHQq8LTI4Fxp1
lSpe41BrzxxUxT7IsWAlQYLmoIpgJ1VTVYCxo+Zt
hQByTl5d95v2EemfTCw==
----- END KEY -----
Region

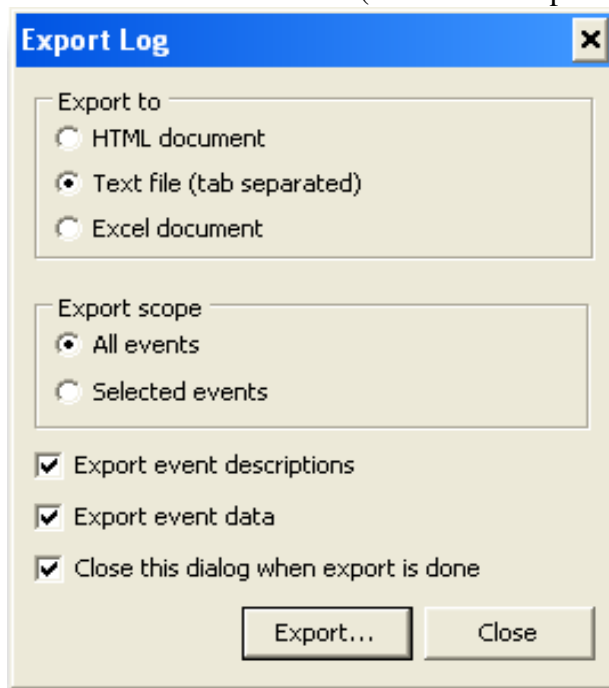
THIS LICENSE IS FOR PERSONAL NONCOMMERCIAL USE ONLY.

```

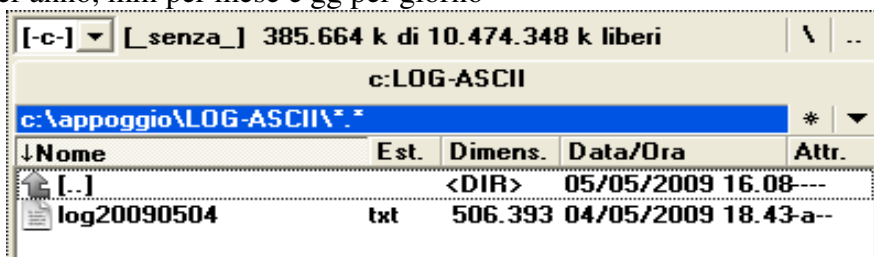
si possono filtrare comodamente tutti i log dell'amministratore



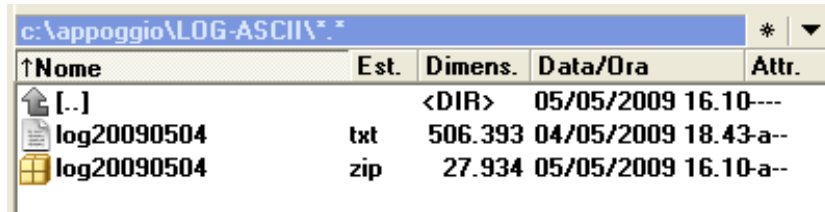
e poi esportare il contenuto filtrato in formato ASCII (text file tab separated)



salvando il file con una convenzione temporale come logaaaammgg.txt dove aaa sta per anno, mm per mese e gg per giorno

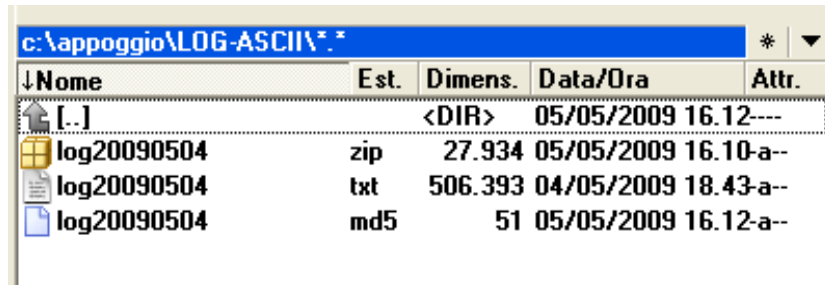


per risparmiare spazio si comprime il file con l'algorithmo zip



↑Nome	Est.	Dimens.	Data/Ora	Attr.
[.]		<DIR>	05/05/2009 16.10---	
log20090504	txt	506.393	04/05/2009 18.43-a--	
log20090504	zip	27.934	05/05/2009 16.10-a--	

per garantire l'integrità del file si calcola l'MD5 del file zippato



↓Nome	Est.	Dimens.	Data/Ora	Attr.
[.]		<DIR>	05/05/2009 16.12---	
log20090504	zip	27.934	05/05/2009 16.10-a--	
log20090504	txt	506.393	04/05/2009 18.43-a--	
log20090504	md5	51	05/05/2009 16.12-a--	

si elimina il file in chiaro (ASCII) e si conserva il file zippato con relativo MD5 per 6 mesi, meglio se su una macchina diversa



Nome	↑Est.	Dimens.	Data/Ora	Attr.
[.]		<DIR>	05/05/2009 16.15---	
log20090504	md5	51	05/05/2009 16.12-a--	
log20090504	zip	27.934	05/05/2009 16.10-a--	

↓Nome	Est.	Dimens.	Data/Ora	Attr.
[.]		<DIR>	05/05/2009 16.15---	
[2009-maggio]		<DIR>	05/05/2009 16.15---	

entro i sei mesi previsti dal Garante sarà possibile verificare l'integrità del file zippato controllando l'MD5 e poi una volta decompresso il file, analizzare riga per riga cosa ha fatto l'amministratore giorno per giorno, ora per ora.

GLI EVENTI DI SISTEMA (LOG) DI GNU/Linux

Gli eventi di Sistema (log) di GNU/Linux vengono registrati automaticamente in file testuali nella directory `/var/log/`



Nome	Dimensione	Tipo	Data di modifica
syslog	116,1 kB	Documento in testo semplice	mar 05 mag 2009
messages	352,0 kB	Documento in testo semplice	mar 05 mag 2009
kern.log	358,3 kB	Log applicazione	mar 05 mag 2009
auth.log	346,6 kB	Log applicazione	mar 05 mag 2009
daemon.log	435,1 kB	Log applicazione	mar 05 mag 2009
dpkg.log	117,4 kB	Log applicazione	mar 05 mag 2009
utmp	14,2 kB	Sconosciuto	mar 05 mag 2009

il contenuto del file `syslog`, quindi è visionabile e modificabile (non potrebbe essere altrimenti su una macchina GNU/Linux) con un editor di testo



File Modifica Visualizza Cerca Strumenti Documenti Ajuto

Nuovo Apri Salva Stampa... Annulla Ripeti Taglia Copia Incolla Trova Sostituisci

! syslog ✕

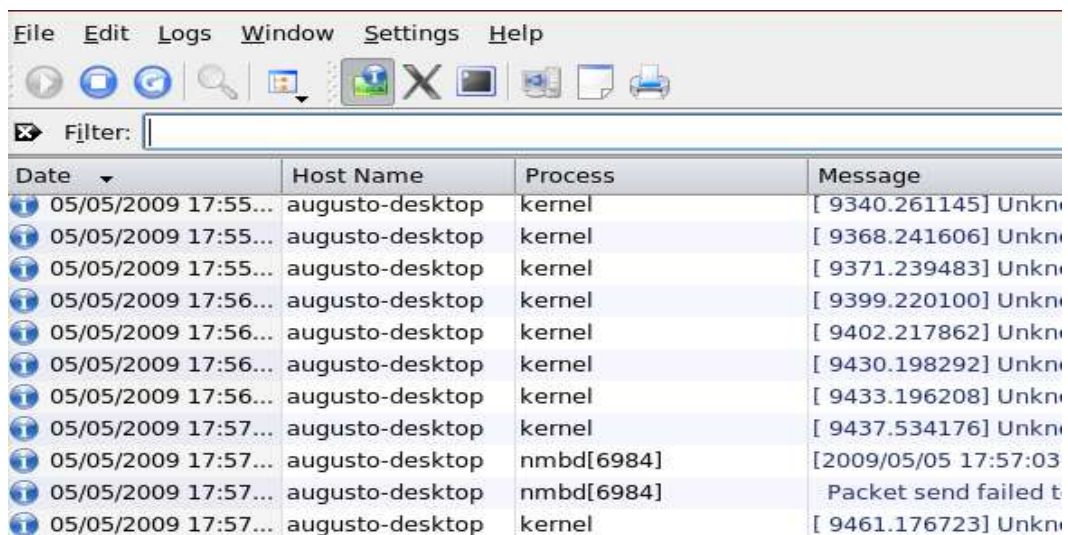
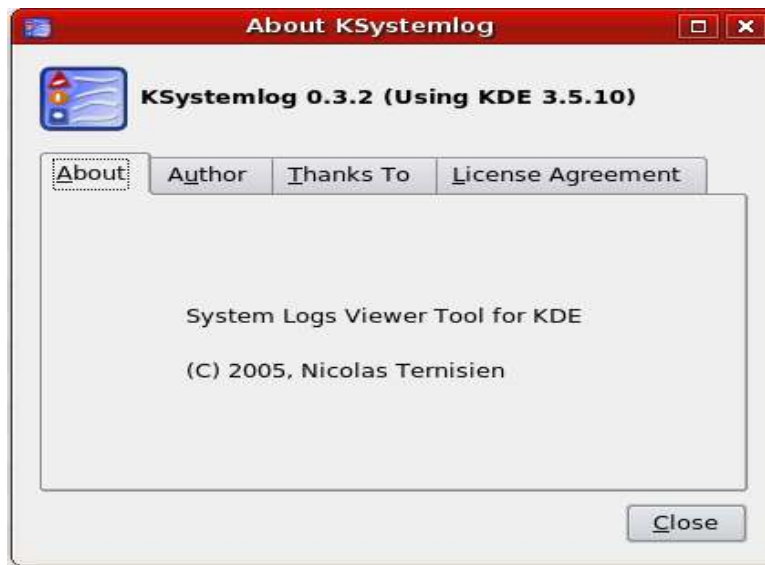
Il file `/var/log/syslog` è stato modificato.

Caricare nuovamente il file?

```
May 5 15:46:34 agosto-desktop syslogd 1.5.0#1ubuntu1: restart.
May 5 15:46:34 agosto-desktop anacron[6939]: Job `cron.daily' terminated (mailing output)
May 5 15:46:34 agosto-desktop anacron[6939]: Can't find sendmail at /usr/sbin/sendmail, no
May 5 15:46:34 agosto-desktop anacron[6939]: Normal exit (1 job run)
May 5 15:46:44 agosto-desktop kernel: [ 1623.781713] Unknown OutputIN= OUT=ham0 SRC=5.239.
ID=0 DF PROTO=UDP SPT=631 DPT=631 LEN=164
May 5 15:46:45 agosto-desktop kernel: [ 1624.781012] Unknown OutputIN= OUT=ham0 SRC=5.239.
ID=0 DF PROTO=UDP SPT=631 DPT=631 LEN=177
May 5 15:47:15 agosto-desktop kernel: [ 1654.760436] Unknown OutputIN= OUT=ham0 SRC=5.239.
ID=0 DF PROTO=UDP SPT=631 DPT=631 LEN=164
May 5 15:47:16 agosto-desktop kernel: [ 1655.759610] Unknown OutputIN= OUT=ham0 SRC=5.239.
ID=0 DF PROTO=UDP SPT=631 DPT=631 LEN=177
May 5 15:47:46 agosto-desktop kernel: [ 1685.739166] Unknown OutputIN= OUT=ham0 SRC=5.239.
ID=0 DF PROTO=UDP SPT=631 DPT=631 LEN=164
May 5 15:47:47 agosto-desktop kernel: [ 1686.737725] Unknown OutputIN= OUT=ham0 SRC=5.239.
ID=0 DF PROTO=UDP SPT=631 DPT=631 LEN=177
May 5 15:48:17 agosto-desktop kernel: [ 1716.716856] Unknown OutputIN= OUT=ham0 SRC=5.239.
ID=0 DF PROTO=UDP SPT=631 DPT=631 LEN=164
```

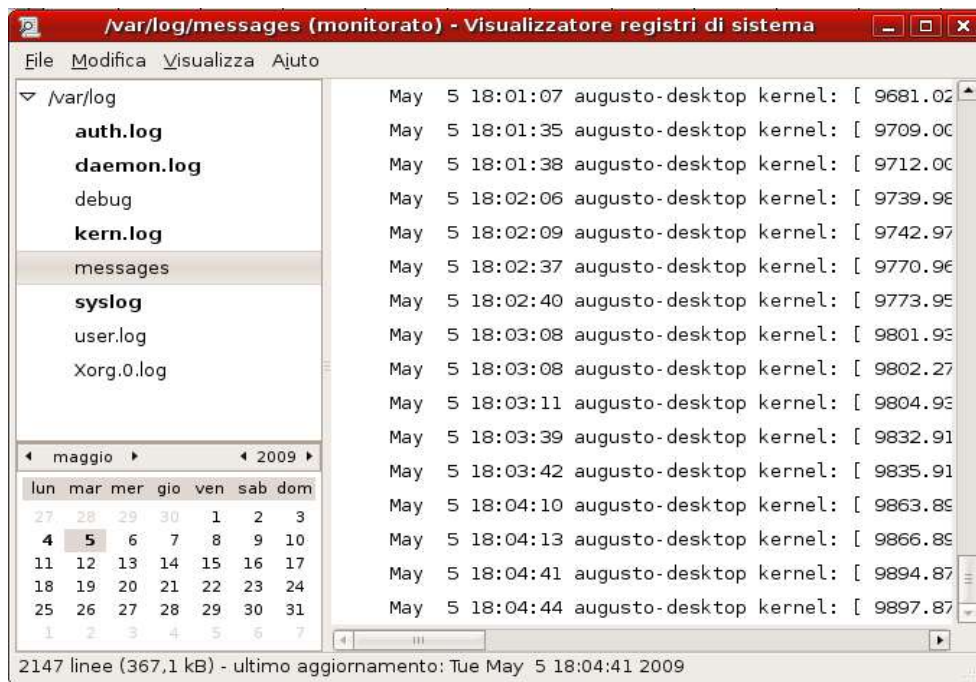
La gestione dei log avviene tramite l'applicazione **Logrotate**, mentre **Logwatch** è uno strumento per analizzare e monitorare i log.

Uno strumento più versatile può essere **KSystemlog** che è uno strumento per **KDE** ma gira anche sotto **GNOME**



o direttamente **gnome-system-log** (nativo per **GNOME**)





In entrambi i casi si può selezionare tutto il contenuto del registro, copiarlo e incollarlo su un file di testo nuovo e vuoto.



Il file può essere **firmato** con la propria firma **GPG GNU PRIVACY GUARD** e conservato per 6 mesi



oppure può essere **cifrato** con la propria chiave **GPG** e conservato per 6 mesi



oppure si può **cifrare il file firmato** e conservato per 6 mesi



Si obietterà che non ha molto senso il fatto che l'amministratore di sistema prelevi il file di log, lo firmi e/o lo cifri con la sua chiave GPG e lo conservi per 6 mesi.

Infatti questo specifico provvedimento del Garante non ha molto senso, relativamente alla gestione dei log.

La tesi del provvedimento è che qualcuno dovrebbe essere in grado di controllare e verificare l'operato dell'amministratore di sistema, questi potrebbe essere un diretto superiore dell'amministratore che usa la propria firma digitale o addirittura una ditta esterna.

Ma, anche se così fosse, si porrebbe il problema di chi controlla il controllore dell'amministratore e così via in un **loop infinito**.

In tale ipotesi, si dice in gergo, che il **sistema andrebbe in crash per buffer overflow**.

FINE

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

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