

# Gestione dei Log e Normativa Italiana: Come Dormire Tranquilli Con Soluzioni Open Source

*<http://joind.in/event/view/468>*

Ing. Stefano Maraspin  
Studio Associato S. Maraspin - S. Valle  
Ingegneri dell'Informazione

[www.twitter.com/maraspin](http://www.twitter.com/maraspin)  
[s.maraspin@mvassociati.it](mailto:s.maraspin@mvassociati.it)

Avv. Luca Zenarolla  
Studio Legale D'Agostini

<http://it.linkedin.com/pub/luca-zenarolla/26/454/57b>  
[lucazenarolla@alice.it](mailto:lucazenarolla@alice.it)



- Fondatore e Managing Partner M.V. Associati
  - Progettazione e Sviluppo Sistemi Software
    - E-Commerce (UX, IA, Progettazione, Sviluppo)
    - Sistemi per la Diagnostica (Architettura, Design)
- “Seguace” dell'Open Source; in realtà piuttosto neutrale sulle tecnologie; ma pur sempre con qualche simpatia... ;-)
  - Sviluppo in PHP
  - Sistemi Server basati su RHEL, CentOS e FreeBSD



[www.mvassociati.it](http://www.mvassociati.it) <http://it.linkedin.com/in/maraspin> [www.twitter.com/maraspin](http://www.twitter.com/maraspin)

# Parte 1: Introduzione



- Definizioni
- Impieghi dei Log
- Modalità di Logging
- Tipologie di Gestione
- Gestione Centralizzata
- Compliance

- Logging: *“insieme delle procedure attraverso le quali un sistema operativo o un'applicazione registrano gli eventi e li memorizzano per successivi riutilizzi”*

Maximum Linux Security – SAMS – 1999

- File di Log: file nei quali sono raccolti gli eventi relativi ad un sistema operativo o un'applicazione, attraverso attività di Logging



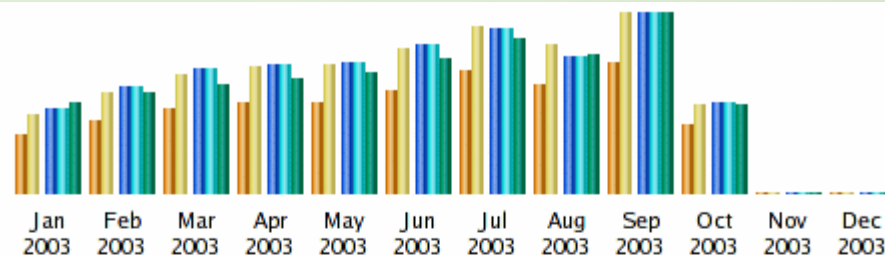
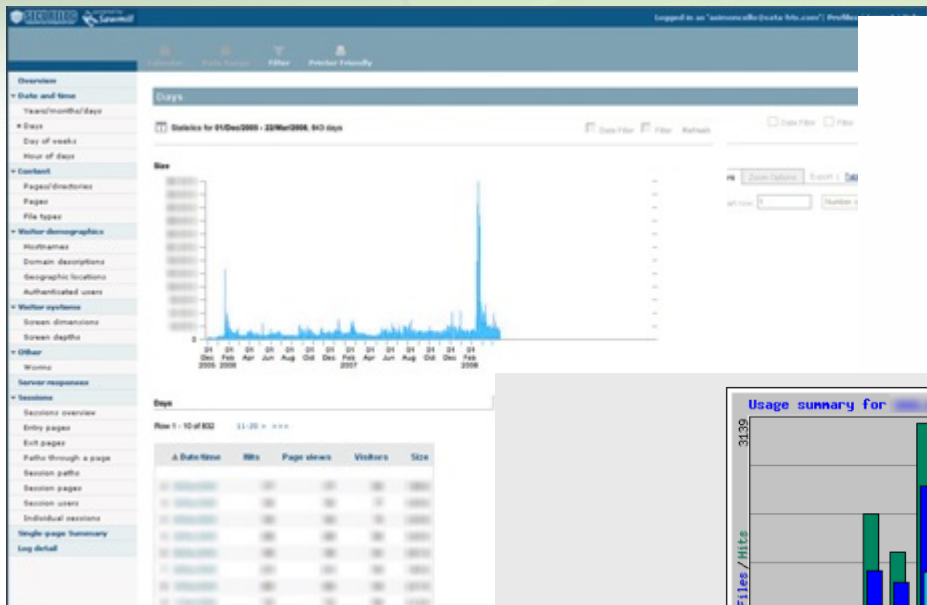
[http://pijournal.blogspot.com/2008\\_10\\_01\\_archive.html](http://pijournal.blogspot.com/2008_10_01_archive.html)

<http://mayang.com/textures/> - [http://mayang.com/textures/Wood/images/Other%20Wood/log\\_pile\\_4210098.JPG](http://mayang.com/textures/Wood/images/Other%20Wood/log_pile_4210098.JPG)

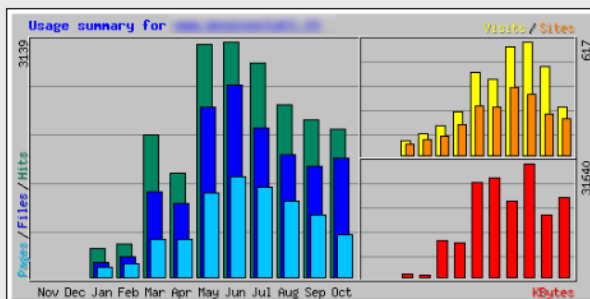
<http://en.wikipedia.org/wiki/File:Logkit.jpg>

[http://en.wikipedia.org/wiki/File:Grand\\_Turk%2834%29.jpg](http://en.wikipedia.org/wiki/File:Grand_Turk%2834%29.jpg)



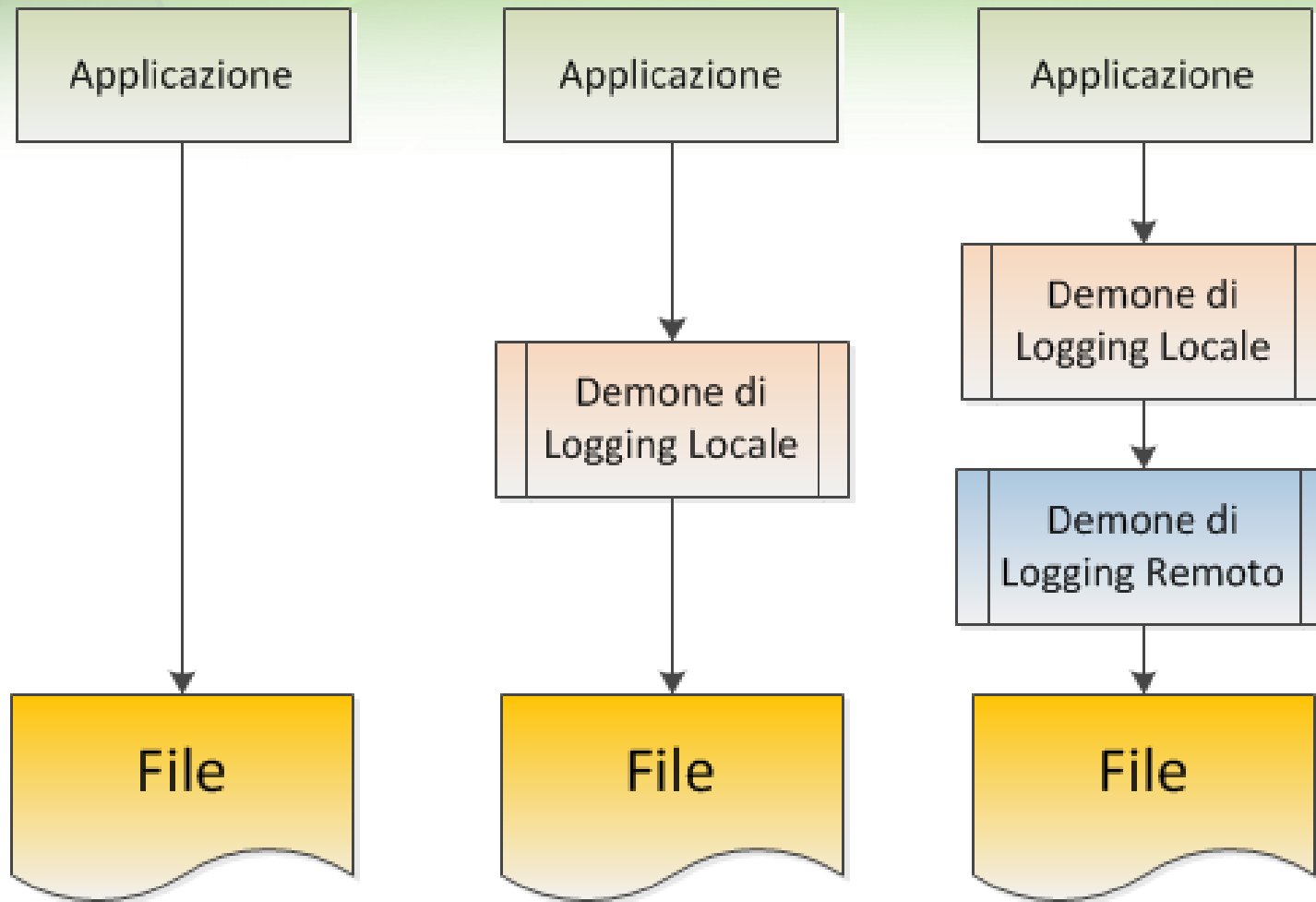


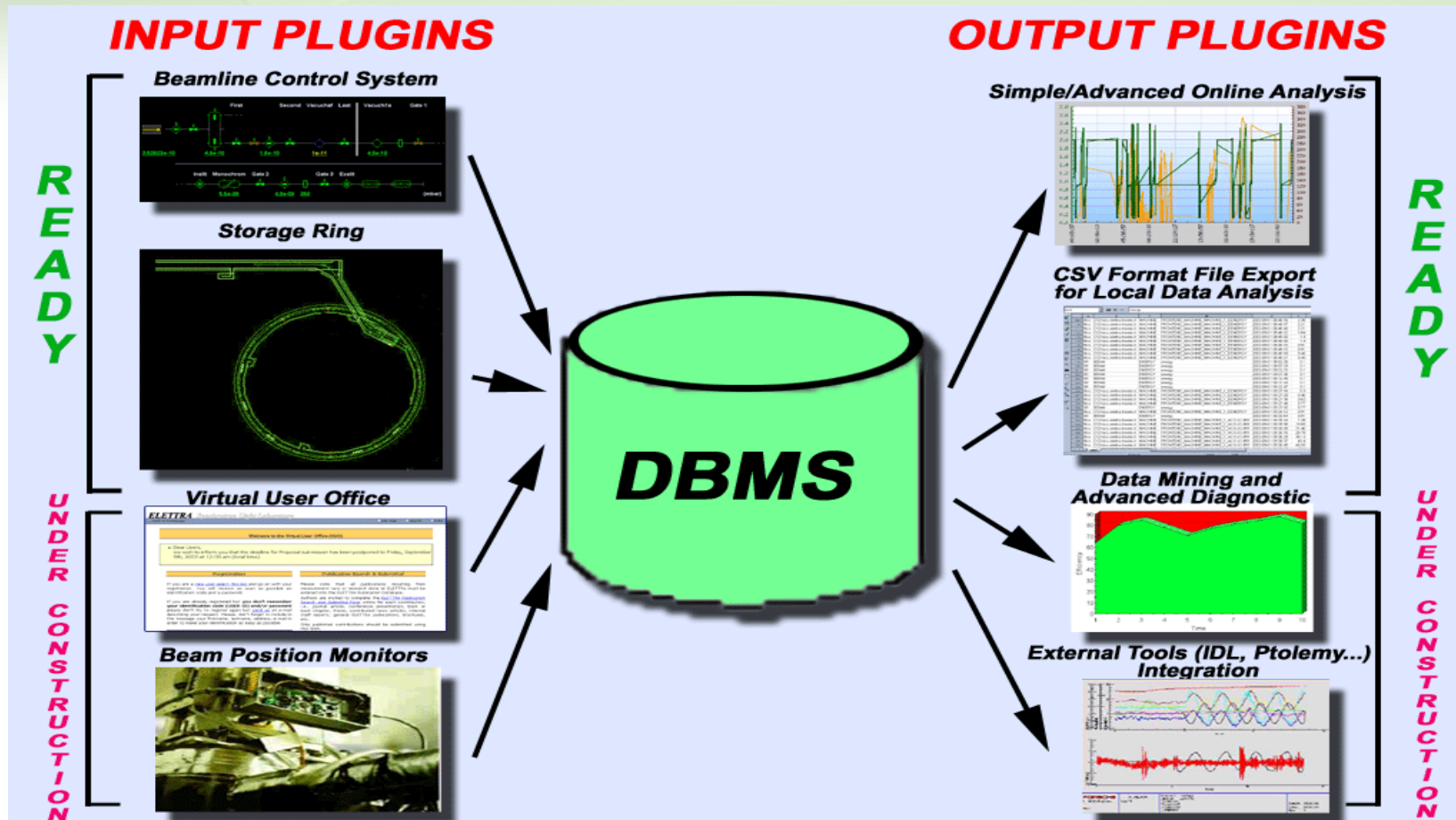
Month	Unique visitors	Number of visits	Pages	Hits	Bandwidth
Jan 2003	21060	28083	44398	44398	1.51 GB
Feb 2003				56627	1.66 GB
Mar 2003				65518	1.79 GB
Apr 2003				68114	1.90 GB
May 2003				69093	2.01 GB
Jun 2003				78585	2.23 GB
Jul 2003				87366	2.55 GB
Aug 2003				72458	2.30 GB
Sep 2003				95095	2.97 GB
Oct 2003				48147	1.48 GB
Nov 2003				0	0
Dec 2003				0	0
<b>Totals</b>	<b>685401</b>	<b>20.39 GB</b>			



Month	Summary by Month									
	Daily Avg					Monthly Totals				
	Hits	Files	Pages	Visits	Sites	KBytes	Visits	Pages	Files	Hits
Oct 2010	104	83	29	13	201	22008	264	567	1588	1976
Sep 2010	69	49	27	16	222	17399	484	826	1480	2092
Aug 2010	74	52	32	19	333	31640	617	1015	1638	2299
Jul 2010	92	64	38	19	366	21047	591	1206	1994	2856
Jun 2010	104	85	44	13	264	27559	414	1332	2561	3139
May 2010	100	73	36	14	266	26356	450	1124	2269	3106
Apr 2010	46	32	16	7	164	9460	235	496	989	1386
Mar 2010	61	36	15	5	105	10049	161	495	1136	1892
Feb 2010	15	9	6	4	84	640	118	175	268	444
Jan 2010	14	7	4	2	57	676	78	132	200	379
<b>Totals</b>						<b>166834</b>	<b>3412</b>	<b>7368</b>	<b>14123</b>	<b>19569</b>







- **SIM, SEM, SIEM:** raccolta unicamente orientata alla sicurezza, con filtraggio e analisi dei dati in tempo reale
  - Applicazione di Euristiche per individuare e segnalare pattern di utilizzo anomalo, anche su diversi sistemi
  - Possibilità di decentralizzare alcune attività (es. aggregazione e filtraggio degli eventi alla sorgente)
- **Log Management:** raccolta a lungo termine di tutti i dati, per tutti gli utenti di tutti i sistemi

- Sarbanes-Oxley (SOX)
- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability & Accounting Act (HIPAA)
- Gramm-Leach-Bliley (GLBA)
- ISO 27001
- Basilea II
- Normativa nazionale italiana

# Parte 2: Riferimenti Normativi



# Avv. Luca Zenarolla



Laureato presso la Facoltà di Giurisprudenza dell'Università degli Studi di Trieste nel 2004 con una tesi intitolata "La tutela della riservatezza e della sicurezza negli uffici giudiziari alla luce del decreto legislativo 196/2003".

Dal 2009 é iscritto all'albo degli Avvocati dell'Ordine di Udine con cui collabora come membro della Commissione informatica.

Relatore e docente a numerosi seminari e corsi di formazione in tema di diritto delle nuove tecnologie, é autore di diversi contributi e pubblicazioni in materia di diritto dell'informatica e privacy.

Dal 2004 svolge attività consulenziale in materia di privacy e sicurezza informatica, e-procurement, archiviazione elettronica e conservazione sostitutiva.

- Log nell'ordinamento giuridico nazionale
- Il decreto Pisanu
- Il Provvedimento del Garante sulla Privacy

# I Log nell'Ordinamento nazionale

- **D.Lgs. 196/03 Codice privacy (art. 132)**
- **D.L. 27 luglio 2005, n. 144 (D.Pisanu), e Decreto Ministero Interno del 16 agosto 2005**
- **Provvedimenti a carattere generale Garante Privacy - 27 novembre 2008**



# Il Decreto Pisanu

## Legge 155/2005

## D.M. 16 agosto 2005

Misure urgenti per il contrasto del terrorismo internazionale: misure **straordinarie** e in linea di massima **temporanee**.



# Il Decreto Pisanu

Vengono, eliminati per fornitori di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico, i limiti previsti per la conservazione dei dati del traffico telefonico o telematico.

Modifica dell'articolo 132 del D.Lgs. 196/03



# Il Decreto Pisanu e decreto attuativo

## Nuove regole per i c.d Internet Point:

- chi apre un pubblico esercizio o un circolo privato di qualsiasi specie, in cui sono a disposizione apparecchi terminali utilizzabili per le comunicazioni, anche telematiche, deve chiederne la licenza al questore.
- Sono esclusi i telefoni pubblici a pagamento, abilitati esclusivamente alla telefonia vocale.



# Il Decreto Pisanu e decreto attuativo

## Nuove regole per i c.d Internet Point:

- l'acquisizione dei dati riportati su un documento di identità, "nonché il tipo, il numero e la riproduzione del documento presentato dall'utente";
- la raccolta e l'archiviazione di tali dati "con modalita' informatiche" (l'archiviazione cartacea è possibile solo con non più di tre terminali);
- la conservazione dei dati stessi fino alla vigenza del D.Pisanu



# Il Decreto Pisanu e decreto attuativo

## Nuove regole per i c.d Internet Point:

- memorizzazione dei "dati relativi alla **data ed ora della comunicazione** e alla **tipologia del servizio utilizzato**, abbinabili univocamente al **terminale utilizzato** dall'utente, esclusi comunque i contenuti delle comunicazioni".
- Estensione obblighi a chi offre accesso alle reti telematiche utilizzando **tecnologia senza fili** in aree messe a disposizione del pubblico.



# IL PROV. DEL GARANTE PRIVACY

**Prov. 27 novembre 2008**, Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema

**Prov. 12 febbraio 2009**, Proroga delle misure e accorgimenti prescritti relativamente alle attribuzioni delle funzioni di amministratore di sistema

**Prov. 25 giugno 2009**, Modifiche del provvedimento del 27 novembre 2008 e proroga dei termini.



# IL PROVVEDIMENTO

## L'AMMINISTRATORE DI SISTEMA:

Figura professionale finalizzata alla gestione e alla manutenzione di un sistema informatico o di sue componenti.

Ai fini del provvedimento vengono considerati tali gli amministratori di data-base, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi



# IL PROVVEDIMENTO

## I COMPITI DELL'AMMINISTRATORE DI SISTEMA:

- Autenticazione informatica;
- Gestione sicurezza (firewall, antivirus, ...);
- Salvataggio e ripristino dei dati;
- Gestione supporti rimovibili;
- Manutenzione hardware;
- Altre attività All. B.

**NB: TUTTI TRATTAMENTI DI DATI PERSONALI!**



# IL PROVVEDIMENTO

## LE SINGOLE MISURE:

### 1. VALUTAZIONE DELLE CARATTERISTICHE PERSONALI

Caratteristiche equivalenti a quelle del responsabile del trattamento.

### 2. DESIGNAZIONE INDIVIDUALE

Divieto di nomina della classe omogenea d'incarico

### 3. ELENCO DEGLI A.d.S.



# IL PROVVEDIMENTO

## LE SINGOLE MISURE:

### 4. VERIFICA DELL'ATTIVITA' DELL'A.d.S

Controllo almeno annuale da parte del titolare del trattamento

### 5. REGISTRAZIONE DEGLI ACCESSI

Registrazione degli accessi al sistema informatico da parte degli A.d.S. Le registrazioni (conservate almeno 6 mesi) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

# La Registrazione degli accessi

**Access Log:** registrazione degli eventi generati dal sistema di autenticazione informatica all'atto dell'**accesso** o **tentativo di accesso** da parte di un AdS o all'atto della sua disconnessione



# La Registrazione degli accessi

## Contenuto Access Log:

- account utilizzato
- data e ora dell'evento (timestamp),
- descrizione dell'evento (sistema di elaborazione o software utilizzato, se si tratti di un evento di log-in, di log-out, ecc.)

**NO ATTIVITA' INTERATTIVA! (Es:  
comandi impartiti.)**



# La Registrazione degli accessi

INALTERABILITA' DEI LOG:  
CARATTERISTICA DA VALUTARE  
SULLA BASE DEL “**CONTESTO  
OPERATIVO**” ...



# IL PROVVEDIMENTO

## QUESITI DI FONDO

QUESTI ADEMPIMENTI SONO OBBLIGATORI  
PER TUTTI?

• L'AMMINISTRATORE DI SISTEMA E'  
NECESSARIO?



# IL PROVVEDIMENTO

## E SE NON OTTEMPERO?

### **Art. 162, c. 2-ter**

In caso di inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieto di cui, rispettivamente, all'articolo **154, comma 1, lettere c)** e d), è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma **da 30.000 euro a 180.000 euro**.

# Parte 3: Considerazioni Tecniche



- Quanto é problematico implementare quanto é stato richiesto dalla normativa?
- Siamo sicuri circa Integrità e Riferimenti Temporalì?
- Successivi chiarimenti del Garante

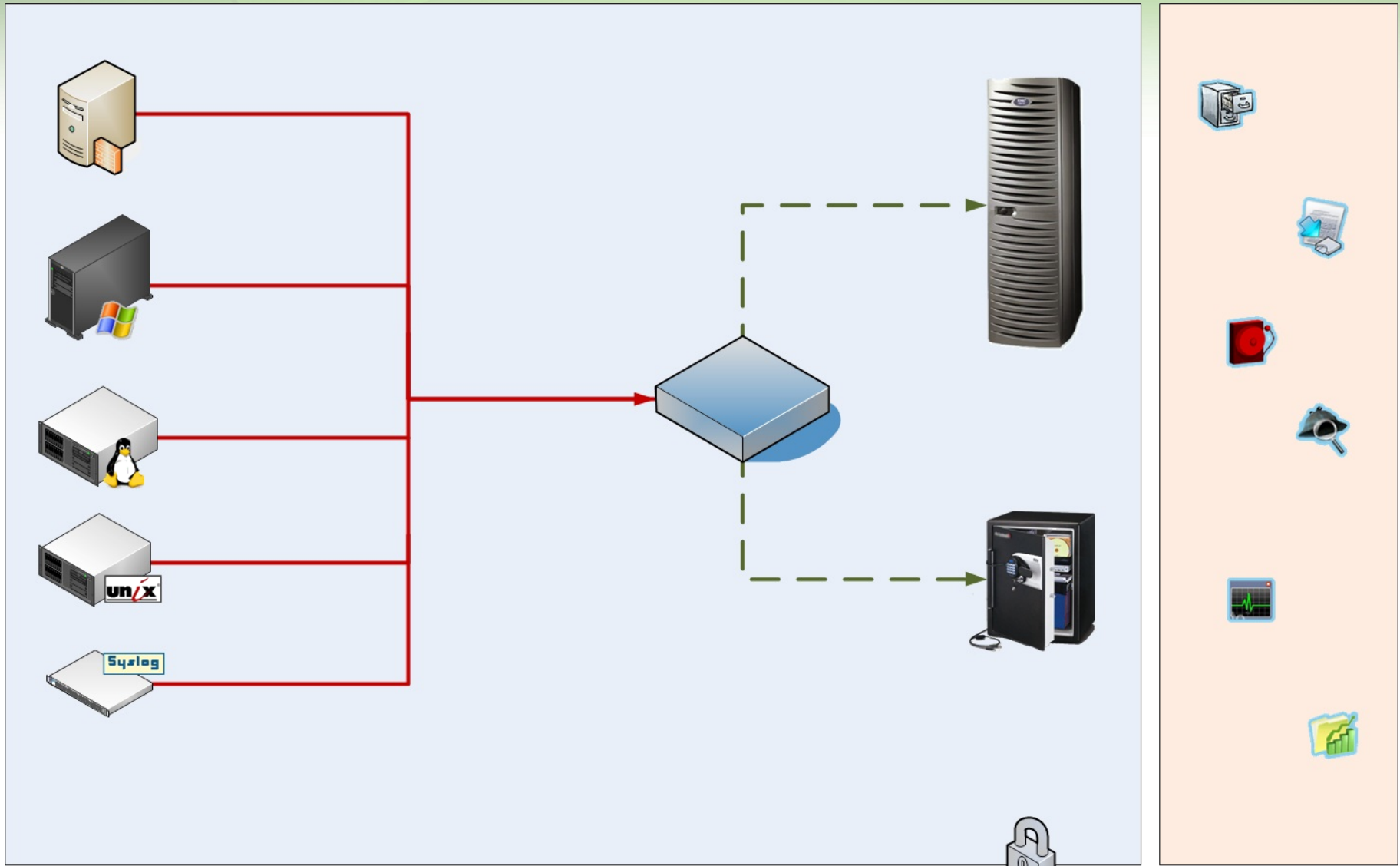
Collezione

Trasporto

Centralizzazione

Memorizzazione

Applicazioni





- Per garantire integrità, è necessario garantire sicurezza **in tutto il data path** del sistema, non solo nel layer di trasporto o in quello di memorizzazione
- La **raccolta** deve perciò avvenire in **real time** (tramite syscall, handles, modifiche di bassissimo livello, etc)
  - Raccogliere i dati a posteriori, in batch, ha poco senso
- In ogni caso, vi devono essere continui periodici **controlli lato server** (ovvero unità di raccolta) sullo stato di salute delle connessioni con i client – altrimenti basta “staccare il cavo”

- Il **protocollo di trasporto** deve anch'esso essere **affidabile** (controllo di sequenza anche a livello applicativo; TCP non basta) e **sicuro** (autenticazione/validazione del mittente)
- Anche la memorizzazione deve avvenire in ambienti protetti (es. dispositivi **WORM** o unità comunque non accessibili dagli intrusi)
- E ci dev'essere ovviamente **protezione fisica!**
- Inoltre la **marca temporale** (o qualsiasi altra azione atta ad indicare data ed ora di un evento) dev'essere **immediata**; se apposta a posteriori, perde il proprio significato

- L'**amministratore** di sistema ha, per definizione, il **controllo completo** sui sistemi amministrati; é perciò pressoché impossibile essere certi di poter controllare tutte le sue attività;
- In ogni caso, come minimo, almeno la macchina su cui i Log vengono raccolti dev'essere al di **fuori di qualsiasi possibilità d'intervento** da parte sua; e comunque questa deve anche attivamente preoccuparsi dello stato di salute dei client connessi.
- Se d'altronde non mi posso fidare del mio amministratore di sistema, probabilmente ho anche problemi che superano, per gravità, quelli legati alla privacy...

- Fortunatamente il Garante ha profondamente rivisto le proprie disposizioni; l'“**adeguatezza** (di una soluzione per la gestione dei log) è *da valutare in rapporto alle **condizioni organizzative e operative dell'organizzazione**”*”
- Per enti e grandi aziende, la cosa più conveniente é probabilmente quella di adottare una **soluzione enterprise**. Sviluppare in casa una soluzione che rispetti tutto quanto visto (e riesca ad integrare fonti eterogenee) é tutt'altro che banale!

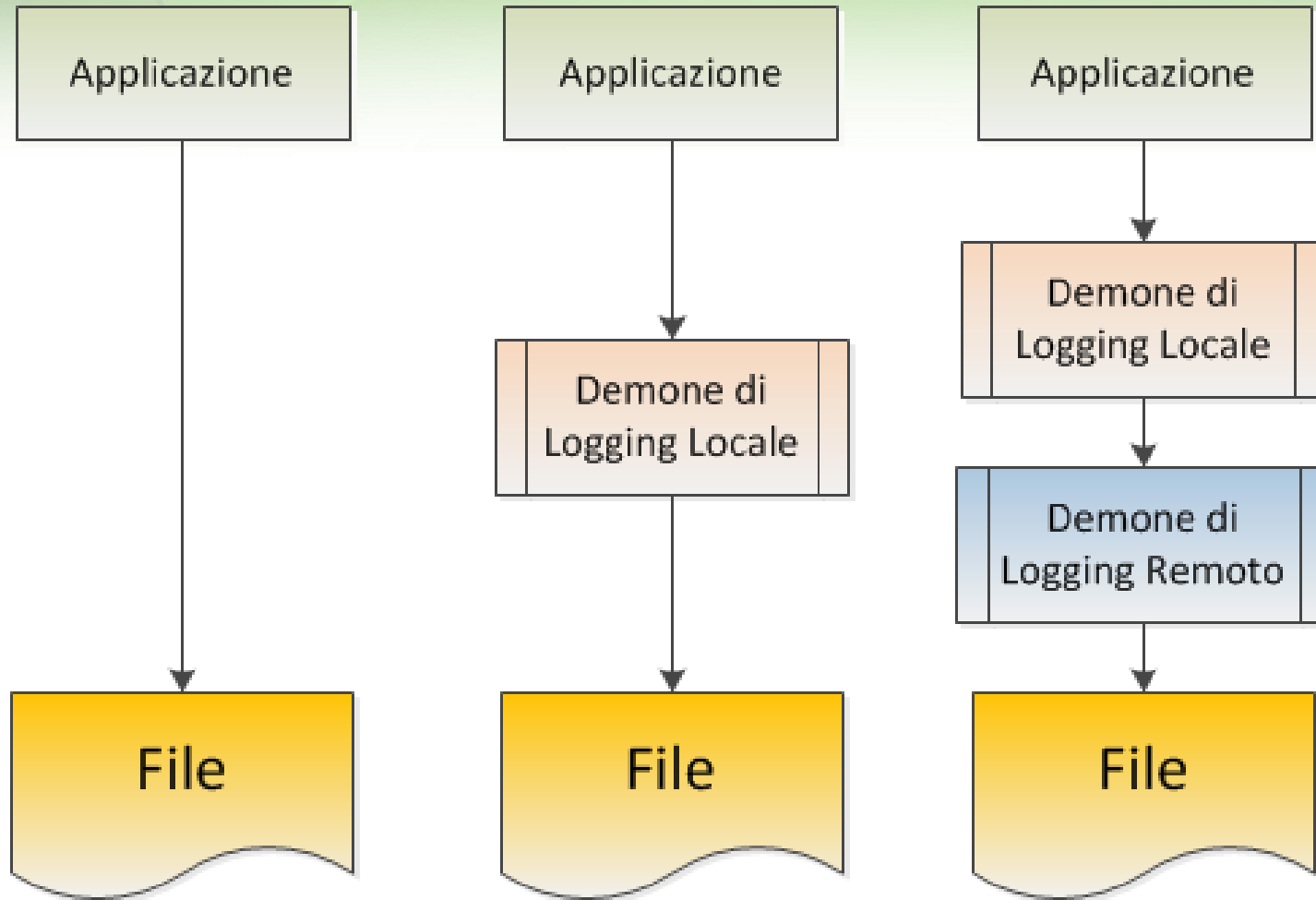
- Per le **PMI**, invece, le soluzioni **Open Source** sono tipicamente sufficienti per far fronte alle disposizioni normative sul controllo dell'operato degli **amministratori di sistema**
  - anche se non possono ovviamente garantire la sicurezza nella maniera in cui questa veniva richiesta al momento in cui i provvedimenti erano stati originariamente emanati
- Per quanto riguarda invece il Decreto **Pisanu**, essendo limitato l'ambito d'applicazione ad un particolare settore e contenuti i costi di acquisto, anche per le PMI é spesso conveniente, in questo caso ricorrere ad una **soluzione chiavi in mano**.

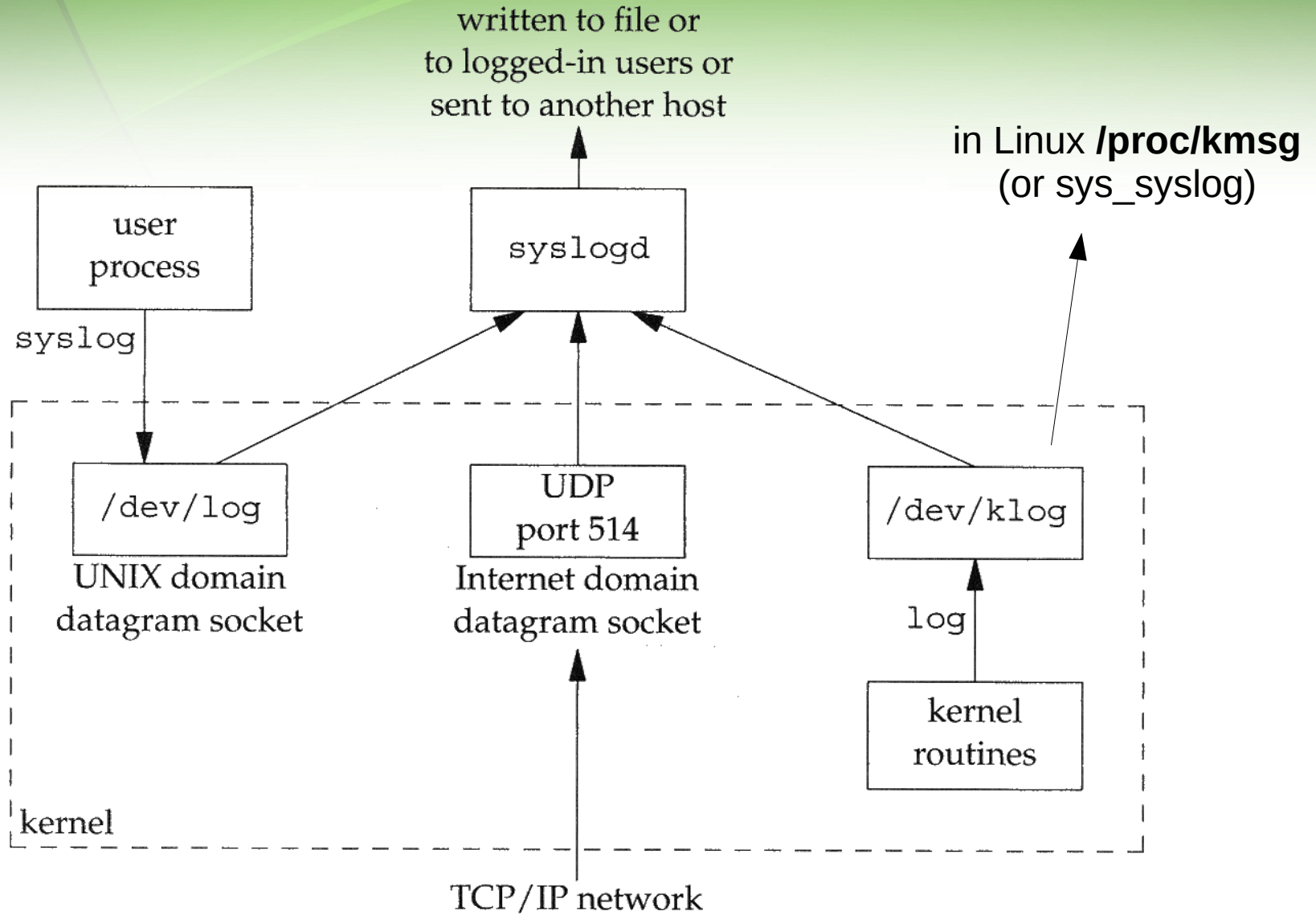
# Parte 4: Soluzioni Open Source



- Il demone syslogd
- Il protocollo syslog
- Rsyslog
- Log da Sistemi Microsoft
- Inserimento dei Dati su DB (cenni)

- Originariamente proposto da Eric Allman come componente di Sendmail e diffuso su sistemi 4.2BSD; in seguito diffusione anche su derivati da System V e incluso nelle specifiche UNIX (Single Unix Specifications)
- Specifiche del protocollo formalizzate nel RFC 3164 (2001)
- Attuali specifiche descritte da RFC 5424 e relative integrazioni - RFC 5425, 5426: (2009)





- Syslog impiega lo **User Datagram Protocol** (UDP), tipicamente sulla porta di destinazione **514**;
- Essendo un protocollo “**best-effort**” non orientato alla connessione, non ci sono “*acknowledgments*”; ciò neppure a livello applicativo, alla ricezione di dati da parte del server.
- Di conseguenza il dispositivo che invia messaggi conformemente con lo standard syslog non sa se questi hanno raggiunto il ricevente; anzi, non sa neppure se il ricevente esiste oppure no!

- La dimensione di un pacchetto syslog é limitata a 1024 byte e si compone delle seguenti informazioni:
  - Facility
  - Severity
  - Hostname
  - Timestamp
  - Message

<i>facility</i>	XSI	Description
LOG_AUTH		authorization programs: login, su, getty, ...
LOG_AUTHPRIV		same as LOG_AUTH, but logged to file with restricted permissions
LOG_CRON		cron and at
LOG_DAEMON		system daemons: inetd, routed, ...
LOG_FTP		the FTP daemon (ftpd)
LOG_KERN		messages generated by the kernel
LOG_LOCAL0	•	reserved for local use
LOG_LOCAL1	•	reserved for local use
LOG_LOCAL2	•	reserved for local use
LOG_LOCAL3	•	reserved for local use
LOG_LOCAL4	•	reserved for local use
LOG_LOCAL5	•	reserved for local use
LOG_LOCAL6	•	reserved for local use
LOG_LOCAL7	•	reserved for local use
LOG_LPR		line printer system: lpd, lpc, ...
LOG_MAIL		the mail system
LOG_NEWS		the Usenet network news system
LOG_SYSLOG		the syslogd daemon itself
LOG_USER	•	messages from other user processes (default)
LOG_UUCP		the UUCP system

<i>level</i>	Description
LOG_EMERG	emergency (system is unusable) (highest priority)
LOG_ALERT	condition that must be fixed immediately
LOG_CRIT	critical condition (e.g., hard device error)
LOG_ERR	error condition
LOG_WARNING	warning condition
LOG_NOTICE	normal, but significant condition
LOG_INFO	informational message
LOG_DEBUG	debug message (lowest priority)

- Il demone `syslogd` riceve i messaggi relativi agli eventi e confronta gli stessi con quanto presente in `/etc/syslog.conf`
- Alcuni esempi di regole di confronto sono le seguenti:

```
mail.info          /var/log/maillog
mail.*             /var/log/verbosemaillog
*. *              |/var/log/useless.log
kern.debug         root, steve
*. *; authpriv.none /myProgram
Local0.*          @192.168.0.1
```

**NB: Usare TAB, non spazi; se utenti non loggati, info perse!**



- Dopo aver effettuato le modifiche:
  - `/etc/init.d/syslog reload`
  - `Kill -HUP PID`
- Spesso anche necessità di impostare appositi switch per il logging in remoto:
  - Su Red Hat e derivate:  
`SYSLOGD_OPTIONS="-r -m 0" → /etc/sysconfig/syslog`
  - Su Debian e derivate:  
`SYSLOGD="-r" → /etc/default/syslogd`
  - Su FreeBSD:  
`syslogd_flags="-a client.example.it -vv" → /etc/rc.conf`

- Mio consiglio é comunque quello di di testare sempre in locale; poi provare il trasferimento remoto
- Per fare ciò é possibile utilizzare l'utility `logger(1)`\*  

```
logger -p local0.warning "Messaggio di Prova"
```
- Dopo aver verificato che tutto funzioni come deve con una redirectione su file, se ci sono problemi nella trasmissione in rete, ricordarsi di controllare il Firewall; utility come `tcpdump(8)` possono ritornare parecchio utili in questi casi.

\* Semplicità arma a doppio taglio: così chiunque può, in pratica, inviare contenuti al demone `syslog!`

- Usa UDP
- Non cifra
- Meccanismo di filtering scarno
- Nessun supporto per inserimento in db
- Nessun supporto per la bufferizzazione

Funzionalità	Syslogd	Syslog-NG	Rsyslog
Open Source	O	“Quasi”	O
Cifratura	-	TLS	TLS* / GSSAPI /Tunnel
Affidabilità	-	TCP	RELP
Buffering	-	-	O
Database	-	O	O

\* Non (ancora) compatibile con RELP

- Implementazione estesa dello standard Syslog
- Progetto avviato nel 2004 da Rainer Gerhards
- Disponibile per Linux e BSD, oltre che per Solaris
- Sta diventando lo standard per il logging su diversi sistemi
  - es. Debian → a partire da Lenny
- Supporto per Template (formati e filtri)
- Possibilità di trasferimento asincrono dei Log (ad esempio quando la macchina é scarica)

[http://wiki.rsyslog.com/index.php/Configuration\\_Samples](http://wiki.rsyslog.com/index.php/Configuration_Samples)



- Per Sistemi Operativi Microsoft ci sono Snare e Ntsyslog
- **Disclaimer:** Non testati da chi vi parla; sono comunque entrambi sotto GPL...

The image shows two overlapping windows. The background window is a web browser displaying the 'SNARE for Windows' interface. The foreground window is the 'NTSYSLOG Service Control Manager'.

**NTSYSLOG Service Control Manager**

Service status on computer <Local Machine>...  
Service is running.

Select Computer Start Service Stop Service

Configuration...  
Syslog Daemons Select Syslog Daemon servers for forwarded events.  
Use the drop down menu below to select which EventLog to forward.

System Application Security System EventLog

Close About

**Intersect Alliance - Information Technology Security - Microsoft Internet Explorer**

Address http://localhost:6161/eventlog

**INTERSECT ALLIANCE SNARE for Windows**

Latest Events  
Network Configuration  
Active Configuration  
Audit Service Status  
Latest Audit Configuration

**Current Events**

Date	System	Event Count	EventID	Source	UserName	UserType	ReturnCode	Strings
Tue Aug 08 11:41:03 2006	flash.InterSect.local	92	643 (Account Management)	Security	SYSTEM	User	Success Audit	Domain Policy Changed: Password Policy modified Domain Name: INTERSECT Domain ID: %{S-1-5-21-4225700407-1522440742-3458925109} Caller User Name: FLASH\$ Caller Domain: INTERSECT Caller Logon ID: (0x0,0x3E7) Privileges: - Changed Attributes: Min. Password Age: - Max. Password Age: - Force Logoff: - Lockout Threshold: - Lockout Observation Window: - Lockout Duration: - Password Properties: - Min. Password Length: 6 Password History Length: - Machine Account Quota: - Mixed Domain Mode: - Domain Behavior Version: - OEM Information: -
Tue Aug 08 11:41:03 2006	flash.InterSect.local	91	1704 (None)	SecCli	Unknown User	N/A	Information	Security policy in the Group policy objects has been applied successfully.
Tue Aug 08 11:41:00 2006	flash.InterSect.local	90	538 (Logon/Logoff)	Security	SYSTEM	User	Success Audit	User Logoff: User Name: FLASH\$ Domain: INTERSECT Logon ID: (0x0,0x939E2) Logon Type: 3
Tue Aug 08 11:40:48 2006	flash.InterSect.local	89	538 (Logon/Logoff)	Security	SYSTEM	User	Success Audit	User Logoff: User Name: FLASH\$ Domain: INTERSECT Logon ID: (0x0,0x93938) Logon Type: 3

Done Local intranet

- Con rsyslog possibilità d'inserimento diretto su **DB**, per facilità di consultazione, **analisi**, report, etc
- Volendo ulteriormente raffinare la raccolta dei dati, soprattutto per quanto riguarda sistemi distribuiti sviluppati ad hoc, ovvero sistemi sui quali si ha completo controllo, é possibile definire ulteriormente **formati per il payload** syslog, usando formati come JSON, oppure Google Protocol Buffers (comodi, efficienti).
- Un possibile approccio di quanto sopra é attraverso l'impiego d'inserimento direttamente su Postgres e poi impiego di **Stored Procedure** (Python - Protocol Buffers Disponibili - o PERL)

# Parte 5: Implementazioni



- Preparazione
- Configurazione Lato Client
- Configurazione Lato Server
- Log di Accessi Postgres
- Log di Accessi Mysql
- Rotazione dei Log
- API per le applicazioni

- Se gli amministratori di sistema sono più di uno, é bene innanzitutto notare che le operazioni di amministrazione non possono essere effettuate tutte tramite l'utente root, ma devono poter essere effettuate dagli utenti appositamente designati e tracciati (**sudo**, sudoers)
- Analogamente, anche per l'accesso ai database bisognerebbe istituire regole ben precise, con **credenziali** d'accesso per **manutenzione** diverse da quelle impiegate in esercizio
- Prepariamo un server **NTP**; il nostro server di centralizzazione e i nostri client dovranno farvi riferimento

- Installazione

Red Hat: `yum install rsyslog`

Debian: `apt-get install rsyslog (relp su backports)`

FreeBSD: `/usr/ports/sysutils/rsyslog5`

- Configurazione (base) di `/etc/rsyslog.conf`

```
# abilita il supporto per RELP, UNIX socket e klog
$ModLoad omrelp
$ModLoad imuxsock
$ModLoad imklog
```

```
# invia tutto a "servercentrale" sulla porta (TCP) 2514
*. * :omrelp:servercentrale:2514;RSYSLOG_ForwardFormat
```



- Esempio (base) di /etc/rsyslog.conf

```
$ModLoad imudp
$UDPServerRun 514
$ModLoad imrelp
$InputRELPServerRun 9999
$ModLoad imuxsock
$ModLoad imklog
# $ModLoad omrelp

# Uncomment this to see kernel messages on the console.
#kern.* /dev/console

# Log anything 'info' or higher, but lower than 'warn'.
# Exclude cron, and mail. These are logged elsewhere.
*.info,*.!warn,cron.none,mail.none /var/log/messages

[...]

# Private authentication message logging:
auth,authpriv.* /var/log/access_log
```



- Postgres supporta nativamente il logging su syslog
  - Modificare postgresql.conf (che su CentOS, ad esempio, si trova in /var/lib/pgsql/data/ - in altre distro può trovarsi ad esempio in /usr/local/pgsql/data):

```
log_destination = 'syslog'  
syslog_facility = 'auth'  
syslog_ident = 'postgres'  
log_connections = true  
log_disconnections = true  
log_duration = true  
log_hostname = true
```

- Meno immediato, dato che MySQL non supporta il Logging diretto su syslog
- Faccio ricorso a named pipe, in concerto con logger
- Creo una pipe:

```
mkfifo /path/to/namedpipe
```

- poi modifico /etc/my.cnf, aggiungendo:

```
log=/path/to/namedpipe
```

- Infine faccio uso di qualcosa tipo:

```
while [ true ]; do  
cat /path/to/namedpipe | egrep 'Connect|Quit' | logger -p  
auth.info -t mysql  
done
```

- Impiego congiunto di RELP e TLS non ancora supportato; facciamo uso di **stunnel**, realizzando qualcosa tipo:

```
client_rsyslog_send(127.0.0.1:4444)
<-client-> client_accept_from(127.0.0.1:4444) |
client_connect_to(<server_address>:5555)
<-network->
server_accept_from(:5555) | server_connect_to(127.0.0.1:6666)
<-server->
server_rsyslog_listen(127.0.0.1:6666)
```

<http://www.debian-administration.org/users/openjaf/weblog/1>

```
openssl req -new -x509 -days 3650 -nodes -out stunnel.pem -keyout stunnel.pem
```

- A questo punto non dobbiamo dimenticarci di modificare il file di configurazione di rsyslog (e il firewall!) per tenere in considerazione quanto sopra.

- Su Linux: `logrotate(8)`
  - Rotazione sulla base di dimensione/data; compressione; rimozione; invio attraverso E-Mail; azioni di *postrotate* (ad esempio riavvio di un demone)
- Su FreeBSD: `newsyslog(8)`
  - Rotazione sulla base di dimensione/data; compressione; riavvio dei demoni (`kill -HUP`)
- Per masterizzare posso infine usare utilities come:  
`mkisofs(8)`, `cdrecord(1)`

```
#include <syslog.h>

main() {

    setlogmask (LOG_UPTO (LOG_NOTICE));

    openlog ("presentazione",
            LOG_CONS | LOG_PID | LOG_NDELAY,
            LOG_LOCAL1);

    syslog (LOG_NOTICE,
            "La presentazione di %d sta volgendo al termine",
            getuid ());

    syslog (LOG_INFO,
            "Grazie a tutti per la Vostra attenzione");

    closelog ();

}
```



# Parte 6: Conclusioni



- Istituire un sistema di gestione dei Log offre in ogni caso anche altri **vantaggi**, oltre a soddisfare le disposizioni normative;
- per minimizzare l'impatto organizzativo é comunque possibile ricorrere ad **intervento esterno** per la sola gestione dei sistemi in cui avviene la centralizzazione dei Log; o adottare soluzioni **SAAS**; **tutto dipende dal contesto!**
- altrimenti (dopo le FAQ del Garante), anche con conoscenze minime é in realtà abbastanza semplice essere compliant; non si sarà sicuri al 100%... ma si possono dormire sonni tranquilli dal punto di vista normativo. ;-)

**Grazie per l'attenzione**

*<http://joind.in/event/view/468>*

Ing. Stefano Maraspin  
Studio Associato S. Maraspin - S. Valle  
Ingegneri dell'Informazione

[www.twitter.com/maraspin](http://www.twitter.com/maraspin)  
[s.maraspin@mvassociati.it](mailto:s.maraspin@mvassociati.it)

Avv. Luca Zenarolla  
Studio Legale D'Agostini

<http://it.linkedin.com/pub/luca-zenarolla/26/454/57b>  
[lucazenarolla@alice.it](mailto:lucazenarolla@alice.it)

