

## Provvedimento amministratori di sistema del 27 novembre 2008

# Come risolvere con una soluzione free?

Metto giù giusto qualche riga per spiegare i test effettuati per adeguarsi al provvedimento relativo agli amministratori di sistema che richiede (entro il 15 dicembre 2009) la registrazione e la conservazione per almeno sei mesi dei log di accesso di ogni account degli amministratori di sistema. Esistono molti software commerciali a pagamento che consentono di mettersi in regola con il provvedimento, ma perchè spendere soldi se con un poche righe di configurazione possiamo adeguare i nostri sistemi? Ecco dunque una breve panoramica sui software che è possibile utilizzare e sulla loro configurazione.

I software che andremo ad utilizzare sono:

**syslog:** più che un software è uno standard, un protocollo, che viene utilizzato per trasmettere attraverso una rete semplici informazioni di log. Generalmente il traffico syslog viene inviato utilizzando il protocollo udp (dunque ad assenza di controllo della connessione, ecco perchè più avanti vedremo che per gestire i log di molti host è preferibile utilizzare un protocollo con controllo della connessione come tcp).

**Snare:** è un agent open source, che installa un servizio per il log degli eventi su Windows. E' amministrabile via interfaccia web. Snare non fa altro che inviare remotamente i log desiderati alla macchina che ha il demone syslog in ascolto.

**Splunk (facoltativo):** è un software commerciale ma con una licenza free per un volume massimo di 500MB giornalieri. Splunk è prima di tutto un motore di ricerca, che ci consente di visualizzare in modo più presentabile i log collezionati dal syslog e ci dà la possibilità di eseguire sui log stessi analisi e report.

Iniziamo dunque...

Per essere compliant alla normativa, ogni utente e quindi ogni amministratore di sistema deve avere il proprio account personale. Per abilitare utenti diversi ad effettuare operazioni che richiedono i poteri di root si può abilitare sui server nix\* il comando *sudo*, creando un gruppo apposito (su Ubuntu esiste già, è il gruppo *admin*) e modificando opportunamente con *visudo* i diritti di root per tale gruppo. Ad esempio:

```
$ sudo visudo

# User privilege specification root ALL=(ALL) ALL

# Members of the admin group may gain root privileges

%admin ALL=(ALL) ALL
```

Ovviamente il nome del gruppo di utenti abilitati può essere scelto liberamente. In alcuni sistemi il nome di default è *wheel*. Quello che resta da fare è aggiungere gli utenti al gruppo admin usando *useradd* se l'utente deve essere creato da zero oppure *usermod* se l'utente esiste già.

```
# useradd -G admin nomeutente

# usermod -G admin nomeutente
```

Sui sistemi sarebbe necessario impedire l'utilizzo dell'accesso come amministratore (in quanto il Garante

dice che è necessario poter risalire dall'utente logico all'utente fisico che ha materialmente eseguito il logon e il logoff, cosa per cui gli utenti "Administrator" o "root" sono troppo generici e potenzialmente utilizzati da più persone [amministratori]) per il normale uso.

E' il caso di ricordare che il log degli accessi amministrativi va registrato non solo per i server ma anche per i sistemi client se su queste macchine si gestiscono dati personali.

Syslog è il demone installato di default per gestire i log di sistema . A far bene dovremmo sostituire *syslog* con un software che abbia delle funzioni in più. Su Debian 5 (lenny) rsyslog è il demone di log installato di default. Un'alternativa potrebbe essere syslog-ng. Entrambi i software permettono di ricevere i log da server remoti anche via ssl e registrarli su un db come Mysql o Postgres o altro.

Su Ubuntu, ad esempio, l'installazione si effettua così:

```
# apt-get install rsyslog
```

Per abilitare la ricezione dei log da remoto va modificato sul log server (la macchina dove abbiamo installato rsyslog) il file di configurazione **/etc/rsyslog.conf**.

Invece il file **/etc/default/rsyslog** va modificato solo in caso vada mantenuta la compatibilità con vecchi sistemi, altrimenti non è necessario editarlo.

Nel file **/etc/rsyslog.conf** del log server va tolto il commento alle righe sotto riportate per mettere il demone in ascolto sulla porta 514 UDP. Attenzione, se il traffico fosse molto elevato, si rischia di perdere delle righe di log (per il motivo sopra descritto che il protocollo UD è ad assenza di controllo della connessione). In questo caso va usato il protocollo TCP o RELP.

```
# provides UDP syslog reception

$ModLoad imudp

$UDPServerRun 514
```

Fatte queste modifiche è necessario riavviare il demone con:

```
# /etc/init.d/rsyslogd restart
```

Verificare poi che il demone rsyslogd sia effettivamente in ascolto sulla porta 514 UDP:

```
netstat -lpu | grep rsyslogd
```

che dovrebbe restituire in output qualcosa di simile a:

```
udp          0          0  0.0.0.0:514          0.0.0.0:*
3393/rsyslogd
udp6         0          0  :::514              :::*
3393/rsyslogd
```

Per attivare l'invio del log al rsyslog remoto su ogni macchina linux che deve essere loggata va modificato il file **/etc/rsyslog.conf** (o **/etc/syslog.conf** nel caso in cui il gestore di log sia **syslog** anziché **rsyslog**) modificando la riga

```
auth, authpriv.* /var/log/auth.log
```

in

```
auth, authpriv.* @10.133.0.142 (mettere l'ip del server rsyslog centralizzato)
```

La @ davanti all'indirizzo IP indica a quale host deve essere inviato il log.

Per Windows ho testato Snare Agent for Windows (scaricabile all'indirizzo <http://www.intersectalliance.com/projects/SnareWindows/index.html>), un pacchetto open source che installa un servizio per il log degli eventi su Windows ed è amministrabile tramite una pagina web. L'installazione si limita al solito doppio click sull'eseguibile, all'impostazione della password ed alla scelta se permettere o meno l'accesso remoto alla pagina di configurazione del servizio. Per effettuare la configurazione è sufficiente far puntare il browser all'indirizzo **http://localhost:6161**. Utente e password di default sono snare/snare, da cambiare immediatamente.

La configurazione da impostare per avere il log remoto è sulla pagina network. Basta impostare *Destination Snare Server address* con l'indirizzo ip del server di log (nel mio caso 10.133.0.142) e come destination port 514. Attivare *Enable Syslog Header* e selezionare come syslog facility **auth**, con livello **notice**.

The screenshot shows the 'SNARE for Windows' web interface. The main heading is 'SNARE Network Configuration'. Below this, it states: 'The following network configuration parameters of the SNARE unit is set to the following values:'. The configuration parameters are as follows:

Override detected DNS Name with:	
Destination Snare Server address	10.133.0.142
Destination Port	514
Perform a scan of ALL objectives, and display the maximum criticality?	<input type="checkbox"/>
Allow SNARE to automatically set audit configuration?	<input checked="" type="checkbox"/>
Allow SNARE to automatically set file audit configuration?	<input checked="" type="checkbox"/>
Export Snare Log data to a file?	<input type="checkbox"/>
Enable active USB auditing? (This option requires the service to be fully restarted)	<input type="checkbox"/>
Enable SYSLOG Header?	<input type="checkbox"/>
SYSLOG Facility	User
SYSLOG Priority	Notice

At the bottom of the configuration area, there are two buttons: 'Change Configuration' and 'Reset Form'.

Se tutto è andato bene, adesso nel file **/var/log/auth.log** del server dove abbiamo installato rsyslog (o syslog) verranno registrati login, logout ed errori di login delle macchine configurate.

Tenete presente che i log sistemi Windows contengono molte informazioni che non ci servono assolutamente per il provvedimento e che quindi bisogna saperli leggere per recuperare le informazioni necessarie. Gli eventi vengono identificati tramite un codice (ID Event) che assume il valore 528 per il login e 538 per il logout e distinguono gli accessi locali dagli accessi remoti tramite la variabile "Type" che ha valore 2 per accesso locale e valore 3 per accesso effettuato via rete. Vi sono inoltre vari altri ID e Type legati ad altre situazioni (ad esempio errori di login) ed eventuali problemi (quale il mancato log degli eventi con ID 538 al momento della disconnessione).

Se vogliamo fare un passo in più e utilizzare uno strumento che ci permetta di svolgere un'analisi dei log e soprattutto di avere la possibilità di fornire dei report eleganti ed esaustivi, possiamo installare il potentissimo Splunk, un software commerciale che viene però fornito con una licenza free per un volume di dati non maggiore ai 500MB giornalieri (comunque più che sufficiente per i log che andremo a gestire).

Per scaricare Splunk, è necessario registrarsi al sito <http://www.splunk.com/>, quindi scaricare l'eseguibile (per Linux, Mac o Windows, ma essendo stato il software scritto in ambiente Unix consiglio la versione per Linux o Mac, che è decisamente più performante) dalla pagina <http://www.splunk.com/download> (nel momento in cui scrivo siamo alla versione 4.0.7). In Ubuntu per eseguire l'installazione (che va effettuata

ovviamente sulla stessa macchina sulla quale abbiamo installato rsyslog) è sufficiente il seguente comando:

```
dpkg -i splunk-4.0.7-72459-linux-2.6-intel.deb
```

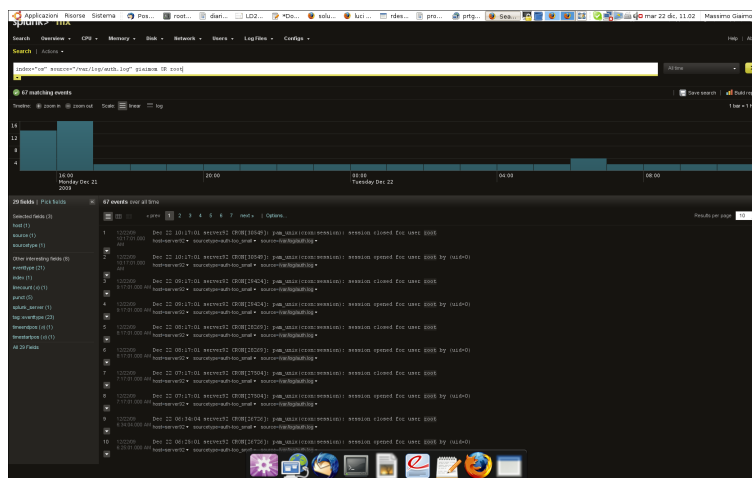
Il software viene installato di default nella directory /opt/splunk

La versione per Windows è altrettanto semplice da eseguire; basta infatti un doppio clic sull'eseguibile ed è sufficiente confermare ciò che viene visualizzato a video.

Al termine dell'installazione, in Ubuntu dobbiamo far partire il servizio Spluk:

```
/etc/init.d/splunk start
```

Possiamo quindi collegarci con il browser all'indirizzo <http://serversplunk:8000> ed accedere (le credenziali iniziali sono "admin" e "changeme"). Il software è molto complesso se utilizzato in tutte le sue innumerevoli funzioni ma molto semplice se utilizzato esclusivamente per ciò che il provvedimento richiede.



Dobbiamo innanzitutto dire a Splunk di presentarci i log che ci vengono inviati da syslog remoti o da agent Snare. Per fare questo, clicchiamo su "Manager" (il terzo link in altro da destra), quindi su "Data inputs". Facciamo clic sulla Actions "Add new" relativo alla riga UDP, quindi in UDP port digitiamo "514" (la porta dove sia i syslog remoti che gli agenti Snare ci inviano i log) e confermiamo. Torniamo dunque alla pagina iniziale di Splunk e attiviamo le apps "Splunk for Windows" e "Splunk for Unix e Linux" (che non sono altro che delle dashboard già configurate per visualizzare i log rispettivamente di sistemi Windows e nix\*). Ora non ci rimane altro che avviare l'una o l'altra apps per visualizzare i log desiderati.

Altri elementi da valutare riguardo al provvedimento sono relativi alla gestione e al ciclo di vita dei log, una volta memorizzati sul nostro server. Secondo il Garante, i log devono essere immutabili e quindi un suggerimento potrebbe essere quello di copiare periodicamente i log su un supporto non riscrivibile, validando i file con un hash. Ovviamente i file e gli hash devono essere tenuti in posti distinti. La soluzione ottimale sarebbe quella di utilizzare come log server una macchina alla quale l'amministratore di sistema non ha accesso né logico né fisico, anche se come scenario è difficile da attuare.

In ogni caso questo è solo un contributo e non la soluzione ottimale al problema sollevato dal Garante. Poi credo sia logico che ogni soluzione deve essere adattata al contesto aziendale nel quale si va operare e quindi non esiste un metodo standard che vada bene per tutti.