

Syslog

Il "registro di sistema" (*system log*, o anche *syslog*) e' la procedura di registrazione degli eventi importanti all'interno di un cosiddetto file di *log*, ovvero un file di registrazione.

Questa procedura è gestita principalmente dal demone **'syslogd'**, che viene configurato attraverso `/etc/syslog.conf`. Altri programmi o demoni possono aggiungere annotazioni al registro inviando messaggi a **'syslogd'**.

Anche se potrebbe sembrare che la conoscenza di questo sistema di registrazione sia uno strumento utile principalmente per chi ha già esperienza di GNU/Linux o dei sistemi Unix in generale, la consultazione dei file delle registrazioni può essere di aiuto al principiante che si trova in difficoltà e non sa quale sia la causa del mancato funzionamento di qualcosa.

Syslog

`/etc/syslog.conf`

Le righe sono composte da record di due campi: il primo definisce la selezione dell'evento, il secondo l'azione.

Il campo che definisce la selezione, serve a indicare per quali eventi effettuare un'annotazione attraverso l'azione indicata nel secondo campo.

Questo primo campo si divide in due sottocampi, uniti da un punto singolo ('.'), e questi si riferiscono ai servizi e alle priorità. I servizi sono rappresentati da una serie di parole chiave che rappresentano una possibile origine di messaggi, mentre le priorità sono altre parole chiave che identificano il livello di gravità dell'informazione.

Le parole chiave riferite ai servizi possono essere:

'auth'; **'authpriv'**; **'cron'**; **'daemon'**; **'kern'**; **'lpr'**; **'mail'**; **'news'**; **'syslog'**; **'user'**; **'uucp'**; e da **'local0'** a **'local7'**.

Syslog

Volendo identificare tutti i servizi si può usare l'asterisco (**), mentre per indicare un gruppo se ne può inserire un elenco separato da virgole (',').

Le parole chiave riferite alle priorità possono essere quelle seguenti, elencate in ordine di importanza crescente, per cui l'ultima è quella che rappresenta un evento più importante.

• **'debug'**; • **'info'**; • **'notice'**; • **'warning'**; • **'err'**; • **'crit'**; • **'alert'**; • **'emerg'**.

In linea di massima, l'indicazione di una parola chiave che rappresenta una priorità implica l'inclusione dei messaggi che si riferiscono a quel livello, insieme a tutti quelli dei livelli superiori. Per indicare esclusivamente un livello di priorità, occorre fare precedere la parola chiave corrispondente dal simbolo '='. Si possono indicare assieme più gruppi di servizi e priorità, in un solo campo, unendoli attraverso un punto e virgola (;).

Syslog

Si possono escludere delle priorità ponendo anteriormente un punto esclamativo (!).

Il secondo campo, quello che definisce l'azione, serve a indicare la destinazione dei messaggi riferiti a un certo gruppo di servizi e priorità definiti dal primo campo. Può trattarsi di un file o di altro, a seconda del primo carattere utilizzato per identificarlo. Segue l'elenco.

• **'/'**

Se il primo carattere è una barra obliqua normale, si intende che si tratti dell'indicazione di un percorso assoluto di un file destinatario dei messaggi. Può trattarsi anche di un file di dispositivo opportuno, come quello di una console virtuale.

• **'|'**

Se il primo carattere è una barra verticale, si intende che la parte restante sia l'indicazione del percorso assoluto di una pipe con nome, ovvero di un file FIFO, generata attraverso **'mkfifo'**

Syslog

- '@'

Se il primo carattere è il simbolo '@', si intende che la parte restante sia l'indicazione di un elaboratore remoto, che ricevendo tali messaggi li inserirà nel proprio sistema di registrazione.

- Elenco di utenti

Se il primo carattere non è scelto tra quelli elencati fino a questo punto, si intende che si tratti di un elenco di utenti (separati da virgole) a cui inviare i messaggi sullo schermo del terminale, se questi stanno accedendo in quel momento.

Syslog

- '*'

Se il primo e unico carattere è un asterisco (*), si intende che i messaggi debbano essere inviati sullo schermo del terminale di tutti gli utenti connessi in quel momento.

È importante osservare che gli stessi messaggi possono essere inviati anche a destinazioni differenti, attraverso più record in cui si definiscono le stesse coppie di servizi e priorità, oppure coppie differenti che però si sovrappongono.

Esempi

```
# Salva tutti i messaggi in un file unico: /var/log/syslog
```

```
*.* /var/log/syslog
```

```
Invia tutti i messaggi nel file '/var/log/syslog'.
```

Syslog

```
# Invia tutti i messaggi del kernel sulla console  
kern.* /dev/console
```

I messaggi del servizio 'kern', a qualunque livello di priorità appartengano, vengono inviati al dispositivo corrispondente alla console. In pratica vengono scritti sullo schermo della console.

```
mail.* /var/log/maillog
```

I messaggi riferiti alla gestione della posta elettronica sono memorizzati nel file '/var/log/maillog'.

```
# Invia tutti i messaggi da warning in su, all'elaboratore  
elios.disi.unige.it  
*.warning @elios.disi.unige.it
```

Syslog

Il file '/var/log/wtmp' è il registro storico degli accessi al sistema. Al suo interno vengono indicate le informazioni della data e dell'ora di accesso di ogni utente, assieme all'indicazione della provenienza degli accessi. I dati contenuti in questo file hanno valore solo se sono completi, nel senso che per ogni accesso si deve trovare anche la registrazione della conclusione della sessione di lavoro, altrimenti non possono essere calcolati i tempi di utilizzo.

Purtroppo, questo file non offre le garanzie di una base di dati vera e propria, e le registrazioni che vengono fatte al suo interno non sono mai sicure. Pertanto, i dati che si riescono a estrapolare sono da considerare approssimativi in generale.

Questo file tende a ingrandirsi rapidamente, tanto che periodicamente conviene fare pulizia. Di solito, le distribuzioni GNU/Linux provvedono a fornire degli script necessari per gestire in modo elegante, attraverso il sistema Cron, l'archiviazione e rotazione dei file delle registrazioni, compreso '/var/log/wtmp'.

La stampa

Tradizionalmente, il dispositivo di stampa permette solo la scrittura, cioè si comporta come un file al quale si possono solo aggiungere dati.

In questa situazione, la stampa si ottiene semplicemente trasferendo (copiando) un file alla stampante. Naturalmente, il file deve essere stato predisposto in modo da poter essere interpretato correttamente dalla stampante che si utilizza.

Il sistema di stampa in stile BSD si avvale del programma **'lpr'** per accodare le stampe, e del demone **'lpd'** per gestire la stampa di ciò che è stato accodato, oltre che per ricevere le richieste attraverso la rete.

La stampa

La configurazione di un sistema di stampa in stile BSD avviene principalmente attraverso il file **'/etc/printcap'**, con il quale si definiscono le code di stampa e il loro componentamento.

Il suo contenuto è organizzato in record, dove ognuno di questi contiene le informazioni relative a una coda.

Il primo campo di ogni record identifica tutti gli pseudonimi possibili di una certa coda di stampa, e questo serve di solito per identificare anche la stampante a cui questa coda è abbinata.

Questi sono separati da una barra verticale.

Gli altri campi contengono tutti una sigla identificativa composta da due caratteri, seguita eventualmente da un valore che gli viene attribuito.

La stampa

Il sistema di stampa BSD tradizionale prevede una quantità molto grande di campi nei record di **'/etc/printcap'**. Le esigenze attuali sono tali per cui i campi che si utilizzano in pratica sono molto pochi:

if	<i>Input Filter</i>	filtro di ingresso.
lf	<i>Log File</i>	file per la registrazione degli errori.
lp	<i>Line Printer</i>	file di dispositivo di stampa.
mx	<i>MaX</i>	dimensione massima di una stampa.
rm	<i>Remote Machine</i>	nodo di stampa remota.
rp	<i>Remote Printer</i>	coda di stampa remota.
sd	<i>Spool Directory</i>	directory usata per la coda.
sf	<i>Suppress Feed</i>	soppressione dell'avanzamento di separazione.
sh	<i>Suppress Header</i>	soppressione dell'intestazione.

La stampa

Esempio

```
lp|laserjet|HP Laserjet:\
:sd=/var/spool/lpd/lp:\
:sh:\
:lp=/dev/lp0:\
:if=/var/spool/lpd/lp/filtro:
```

Per prima cosa si nota che è possibile fare riferimento a questo utilizzando tre nomi possibili: **'lp'**, **'laserjet'** o **'HP Laserjet'**. A parte questo, si nota l'inserimento di un filtro di ingresso. Il file **'/var/spool/lpd/lp/filtro'** potrebbe essere sia un programma che uno script che esegue un qualche tipo di trasformazione sui dati ricevuti.

La stampa

Il servizio di stampa è gestito dal demone 'lpd'. Questo si occupa principalmente di scandire le code e di mettere in stampa ciò che vi dovesse trovare.

E' anche in grado di ricevere richieste di stampa attraverso la rete, e in tal caso si occupa di metterle in coda; infine, è anche capace di inviare una richiesta di stampa a un nodo remoto.

Ogni sistema di stampa utilizza le proprie tecniche di autorizzazione per concedere l'accesso al servizio di stampa.

In generale, un sistema di stampa installato attraverso i pacchetti della propria distribuzione GNU/Linux dovrebbe consentire la stampa quando questa è richiesta a partire dallo stesso elaboratore locale; mentre per consentire l'accesso dall'esterno, occorre predisporre altri file di configurazione che non sono standard

La stampa

Dal momento che la stampa è controllata da un demone, quando si modifica il file di configurazione '/etc/printcap', bisogna fare in modo che 'lpd' lo rilegga. Questo lo si può ottenere arrestando e riavviando il servizio, oppure inviando al processo del demone un segnale di aggancio ('SIGHUP'):

kill -HUP *pid_di_lpd*

Il cliente del sistema di stampa è un programma in grado di accodare una stampa. In generale, nei sistemi di stampa derivati da quello di BSD, si utilizza il programma 'lpr', e in alcuni casi il programma 'lp':

`lpr [opzioni] [file...]`
`lp [opzioni] [file...]`

La stampa

In condizioni normali, questi programmi sono in grado di mettere in stampa i file indicati alla fine della riga di comando, oppure, in loro mancanza, utilizzano per questo lo standard input.

Sono molto poche le opzioni standard di questi programmi e in generale, la cosa più importante è la definizione della coda di stampa a cui si vuole inviare il file.

Ad esempio `lpr -Pcoda file` permette di specificare una coda di stampa particolare, tra quelle previste all'interno di '/etc/printcap'. Se non viene utilizzata questa opzione, si fa riferimento alla stampante predefinita

-m

Al termine della stampa, invia un messaggio attraverso 'mail' all'utente che ha avviato il programma

-#n copie

Permette di specificare il numero di copie che si vuole siano stampate. Il numero di copie è indicato da un numero che segue il simbolo '#'

La stampa

> `lpr lettera` oppure `lp lettera`

Accoda la stampa del file 'lettera' utilizzando la coda predefinita.

> `lpr -P laser lettera` oppure `lp -d laser lettera`

Per conoscere la situazione delle code di stampa si utilizza il comando 'lpq':

`lpq [opzioni] [numero_processo_di_stampa...] [utente...]`

'lpq' esamina le code di stampa e restituisce lo stato di una o di tutte le stampe accodate dall'utente specificato.

Se 'lpq' viene eseguito senza alcun argomento, restituisce lo stato di tutte le stampe accodate.

Alcune opzioni

-P *coda*

Permette di specificare una coda particolare. Se non viene specificato, si fa riferimento a quella predefinita.

-l

Restituisce maggiori informazioni su ogni processo di stampa.

La stampa

I processi di stampa che risultano ancora visibili nelle code, possono essere rimossi dall'utente che li ha generati, o dall'utente **'root'** tramite il comando `lprm`

Il nome dell'utente può essere specificato solo se il comando viene utilizzato dall'utente **'root'**, nel senso che solo lui può interrompere la stampa di altri utenti.

Se non viene specificato il nome dell'utente, si intende che si tratti dello stesso che ha eseguito `'lprm'`. Se non vengono specificati argomenti, l'esecuzione del comando `'lprm'` implica l'eliminazione della stampa in corso per l'utente che lo ha richiesto.

Se l'utente **'root'** utilizza `'lprm'` senza specificare un utente a cui fare riferimento, ottiene l'eliminazione di tutti i processi di stampa nelle code, attivi o meno che siano.