Intro

logwatch è un insieme di script Perl che permette il monitoraggio a scadenze regolari (per es. giornaliero) dei log di sistemi e dei log degli applicativi.

Configurazione per invio mail

ssmtp

È necessario configurare un server SMTP per l'invio dei messaggi di posta, altrimenti questi vengono normalmente inoltrati alla mail dell'utente root locale alla macchina.

A tale scopo è spesso sufficiente installare ssmtp, che permette di inoltrare qualsiasi mail indirizzata ad un utente locale (come root) ad un account esterno specificando il server SMTP da utilizzare.

Nel nostro caso, per tutte le macchine interne è possibile specificare come server il nostro vecchio server di posta dns3.bo.priv, che è a disposizione per il solo inoltro di mail mediante SMTP non autenticato su porta 25.

Si riporta un esempio di file di configurazione per Ubuntu:

/etc/ssmpt/ssmpt.conf

```
#
# Config file for sSMTP sendmail
#
# The person who gets all mail for userids < 1000
# Make this empty to disable rewriting.
root=system-admin@3di.it

# The place where the mail goes. The actual machine name is required no
# MX records are consulted. Commonly mailhosts are named mail.domain.com
mailhub=dns3.bo.priv

# Where will the mail seem to come from?
rewriteDomain=3di.it

# The full hostname
hostname=tomcat-test.bo.priv

# Are users allowed to set their own From: address?
# YES - Allow the user to specify their own From: address
# NO - Use the system generated From: address
#FromLineOverride=YES
```

logwatch

Per poter funzionare correttamente, è specificare a logwatch che quando viene eseguito dal daily cron job (sito normalmente in /etc/cron.daily/00-logwatch o /etc/cron.daily/0logwatch, a seconda della distro utilizzata) la mail che crea deve essere inoltrata ad un utente ben specifico, ovvero l'utente specificato per l'inoltro della mail nella configurazione di ssmtp.

Nel nostro caso, tale utente è root, per cui il file eseguito dal cron.daily assumerà un aspetto simile a questo (possono esserci differenze triviali da una distro all'altra anche qua):

/etc/cron.daily/00-logwatch

```
#!/bin/bash

#Check if removed-but-not-purged
test -x /usr/share/logwatch/scripts/logwatch.pl || exit 0

#execute
/usr/sbin/logwatch --output mail --mailto root

#Note: It's possible to force the recipient in above command
#Just pass --mailto address@a.com instead of --output mail
```