RSYSLOG

Facilities:

- auth - authentication (login) messages
- cron - messages from the memory-resident scheduler
- daemon - messages from resident daemons
- kern - kernel messages
- lpr - printer messages (used by JetDirect cards)
- mail - messages from Sendmail
- user - messages from user-initiated processes/apps
- local0-local7 - user-defined (see below)
- syslog - messages from the syslog process itself

Severity:

- Emergency (emerg)
- Alerts (alert)
- Critical (crit)
- Errors (err)
- Warnings (warn)
- Notification (notice)
- Information (info)
- Debug (debug)

Arquivo de configuração: "/etc/syslog.conf"

Sintaxe:

facility.severity log-file-name

Exemplo:

auth.emerg *-/var/log/auth.log*
*auth.** *-@logserver.log.com*

Comando para aplicar configurações:

/etc/init.d/rsyslog restart

LOGROTATE

Arquivo de configuração: "/etc/logrotate.conf"

Diretório: "/etc/logrotate.d/"

Comandos :

logrotate -v /etc/logrotate.conf
logrotate -vf /etc/logrotate.conf

Principais parâmetros para scripts:

- daily - Rotacionar diariamente.
- monthly – Rodado no primeiro logrotate do mẽs.
- create – Novos arquivos são criados após a rotação (antes do "postrotate").
- nocreate - Novos arquivos de log não são criados. Isso sobrescreve o "create".
- rotate 1 - Quantos arquivos rotacionados existirão.
- compress - usa o gzip.
- missingok - Caso arquivo de log não exista, vai para o próximo sem apresentar erro.
- postrotate - As linhas entre o "postrotate" e o "endscript" serão executadas depois da rotação do log.

Exemplo:

```
/var/log/jboss/tomcat_access_log*.log {
    daily
    nocreate
    rotate 1
    compress
    missingok
    postrotate
        find /var/log/jboss/ -iname 'tomcat_access_log*.gz' -type f -mtime +4 -exec rm -f \{\} \;
    endscript
}
```