Syslog i logi systemowe

syslogd - jest programem odpowiedzialnym za zbieranie informacji (logów) o systemie.
Miejscem przeznaczonym na zapisywanie logów systemowych jest katalog /var/log .
Tu w odpowiednich katalogach i plikach można znaleźć interesujące nas dane.

Plikiem konfiguracyjny tego demona jest /etc/syslog.conf .
Każda informacja zawarta w pliku składa się z trzech pól :
źródło_komunikatu.rodzaj_komunikatu wyjście np.:
authpriv.* /var/log/securr

Jeśli kilka rodzajów komunikatów ma te same wyjście to należy oddzielić je średnikiem, np.:
cron.=debug;cron.=info;cron.=notice var/log/cron/info

Źródła komunikatów mogące wystąpić w tym pliku to:
auth - dane związane z autoryzacją
authpriv - inne komunikaty związane z autoryzacją
cron - komunikaty crona
daemon - inne demony
ftp - komunikaty z serwera ftp
kern - komunikaty jądra systemu
local0-local7 - komunikaty lokalne
lpr - system obsługi drukarki
mail - komunikaty związane z pocztą
mark - w regularnych odstępach czasu wysyła datę i czas
news - system wiadomości
syslog - komunikaty demona syslog
user - procesy użytkowników
uucp - komunikaty protokołu uucp

Rodzaje komunikatów to:

alert - wymagające natychmiastowego działania

crit - krytyczne

debug - uruchomieniowe

emerg - sytuacje zagrożenia

err - błędy

info - informacyjne

notice - wymagające zwrócenia szczególnej uwagi

none - po prostu nic

warning - ostrzeżenia

Znaki mogące wystąpić przed rodzajem komunikatów :

* - wszystkie z wyjątkiem mark

! - za wyjątkiem

np.:

mail.*;mail.!=info /var/log/maillog

mail.info /var/log/info

oznacza, że wszystkie rodzaje komunikatów dotyczące usługi mail zostaną zapisane do pliku /var/log/maillog za wyjątkiem komunikatów informacyjnych, które zapisane zostaną do /var/log/info.