LINUX SERVER ADMINISTRATION

DOCUMENTATIE CURS

Prezentare generala

In Linux una dintre sarcinile cele mai frecvente ale unui administrator de sistem este de-a verifica logurile serverelor care ruleaza. Fiecare serviciu salveaza informatii despre modul de operare, avertismente sau erori generate in fisiere text numite loguri. Acestea se gasesc in directorul /var/log

Pentru a putea urmari eficient intrega activitate de pe Server, Router sau Firewall trebuie configurat in detaliu modul (cantitatea si tipul de mesaje) de logare pentru fiecare server care prezinta interes.

Din punct de vedere al securitatii sistemului, logurile reprezinta modalitatea prin care adminul poate identifica incercarile de logare neautorizate sau modul prin care a fost compromis un server sau intreg sistemul.

Syslog reprezinta standardul de forwardare si salvare a mesajelor de tip log intr-o retea IP.
Termenul Syslog se refera atat la librariile folosite de servere pentru salvarea de mesaje in fisiere de tip log cat si la protocolul/standardul de logare din sistem.

Syslog ruleaza client server. syslogd numit daemonul syslog sau serverul syslog reprezinta aplicatia care receptioneaza si proceseaza mesajele si ruleaza default pe orice distributie de Linux. Este pornit la butarea sistemului de catre un script de initializare din /etc/init.d

Din punct de vedere istoric Syslog a fost dezvoltat in anul 1980 de catre Eric Allman, creatorul primului server de e-mail numit Sendmail. Scopul acestuia era de a fi folosit ca parte integranta a serverului pentru logarea mesajelor generate de acesta.

IETF a standardizat in 2001 protocolul syslog in RFC 3164. In prezent syslog reprezinta standardul "de facto" si "de jure" de logare folosit atat pe Unix/Linux cat si pe alte sisteme de operare sau echipamente dedicate precum Routere sau Switch-uri Cisco.

syslogd ruleaza impreuna cu klogd (Kernel Log Daemon) pentru logarea de mesaje.

Fisierul de configurare al daemonului syslogd este /etc/syslog.conf

Nota

Pe distributiile recente de Linux (Exemplu: Fedora Core 9) syslogd a fost inlocuit cu rsyslogd - Reliable and Extended syslogd. Acesta reprezinta o versiune imbunatatia dar compatibila cu syslogd. Fisierul sau de configurare este /etc/rsyslog.conf

Resurse

- System Logging using Syslog