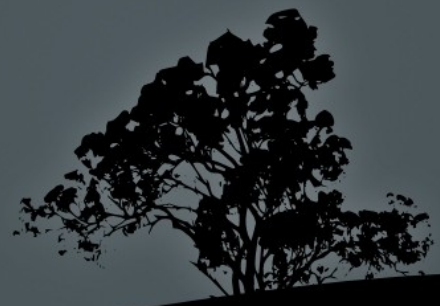
Εξέταση 102 – Μάθημα 11

108.2 Καταγραφή συστήματος



Αρχεία Καταγραφής – Log Files

- Τα αρχεία καταγραφής είναι από τις πιο σημαντικές υπηρεσίες που παρέχει ένα σύστημα Linux γιατί μας επιτρέπει να ανατρέχουμε στο παρελθόν και να βλέπουμε πως συμπεριφέρεται το σύστημα μας
- Το κύριο πρότυπο για διαχείριση των αρχείων καταγραφής είναι το **Syslog** με ραχοκοκαλιά το δαίμονα **syslogd**. Χρησιμοποιεί το μοντέλο Πελάτη – Διακομιστή (Client – Server) όπου μπορεί να υπάρχει ένας κεντρικός διακομιστής Syslog και όλα τα υπόλοιπα συστήματα να χρησιμοποιούν αυτόν.
- Υπάρχουν υπηρεσίες οι οποίες χρησιμοποιούν τα κεντρικά αρχεία καταγραφής (/var/log/messages, /var/log/syslog) ενώ άλλες χρησιμοποιούν δικά τους αρχεία καταγραφής (/var/log/apache/*)
- Τα σύγχρονα συστήματα έχουν νεότερες υλοποιήσεις του Syslog με περισσότερες δυνατότητες πχ **rsyslog** και **syslog-ng**. Όλα όμως δουλεύουν με παρόμοια λογική

Το αρχείο ρυθμίσεων */etc/syslog.conf*

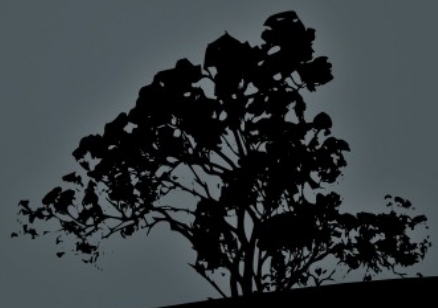
- Το αρχείο **/etc/syslog.conf** παρέχει τις ρυθμίσεις στον δαίμονα **syslogd**. Η μορφή του αρχείου είναι ως εξής:
- **facility.priority action (υπηρεσία.προτεραιότητα δράση)**
- **facility (υπηρεσία)**: καθορίζει την πηγή των μηνυμάτων η οποία μπορεί να είναι: **auth**, **authpriv**, **cron**, **daemon**, **kern**, **lpr**, **mail**, **ftp**, **mark**, **news**, **syslog**, **user**, **uucp**, και **local0** εώς **local7**
- **priority (προτεραιότητα)**: παρέχει το επίπεδο σοβαρότητας των μηνυμάτων και μπορεί να είναι ένα από αυτά (ταξινομημένα από το σοβαρότερο στο ηπιότερο): **emerg**, **alert**, **crit**, **err**, **warning, notice**, **info, debug**.
- **action (δράση)**: εδώ καθορίζεται ο προορισμός των μηνυμάτων. Συνήθως είναι κάποιο αρχείο αλλά μπορεί και να είναι κάποιο τερματικό, κάποιος διακομιστής syslog ή ακόμη και χρήστης

Λίστα facilities (υπηρεσιών)

facility	Περιγραφή
authpriv (auth,security)	Μηνύματα πιστοποίησης, εξουσιοδότησης και ασφάλειας. Συστήνεται η χρήση του authpriv έναντι των auth και security
cron	Μηνύματα από το χρονοπρόγραμμα cron
daemon	Μηνύματα δαιμόνων που δεν έχουν δικό τους facility
ftp	Μηνύματα από σύστημα ftp
kern	Μηνύματα που προέρχονται από τον πυρήνα
lpr	Μηνύματα από το σύστημα εκτύπωσης
mail	Μηνύματα από το σύστημα ηλεκτρονικού ταχυδρομείου
mark	Για εσωτερική χρήση του syslog
news	Μηνύματα από δαίμονα nntp (newsgroups)
syslog	Μηνύματα από το ίδιο το syslog
user	Μηνύματα από διεργασίες χρηστών
uucp	Μηνήματα από σύστημα UUCP (Unix-to-Unix Copy)
local0,local1,...,local7	Αυτές οι υπηρεσίες προορίζονται για τοπική χρήση και μπορούν να καθοριστούν από τους διαχειριστές

Λίστα priorites (προτεραιοτήτων)

priority	Περιγραφή
emerg (panic)	Άκρως επείγοντα μηνύματα που αφορούν την σταθερότητα του συστήματος και έχουν την υψηλότερη προτεραιότητα. Συστήνεται το emerg έναντι του panic
alert	Μηνύματα που χρειάζονται επείγουσες ενέργειες. Δεύτερη υψηλότερη προτεραιότητα.
crit	Κρίσιμες συνθήκες. Τρίτη ψηλότερη προτεραιότητα
err (error)	Σφάλματα συστήματος ή δαιμόνων. Προτιμάται το err
warning (warn)	Σοβαρές προειδοποιήσεις. Προτιμάται το warning
notice	Σημαντικές επισημάνσεις
info	Χρήσιμες πληροφορίες
debug	Μηνύματα για απασφαλμάτωση ή επίλυση προβλημάτων



Παραδείγματα ρυθμίσεων σε syslog.conf

- **mail.*** **/var/log/maillog** # αποστολή όλων των μηνυμάτων (ανεξαρτήτως προτεραιότητας), προερχόμενα από το σύστημα email, στο αρχείο καταγραφής **/var/log/maillog**
- ***.emerg** * # αποστολή όλων των μηνυμάτων με προτεραιότητα **emerg** (ανεξαρτήτως υπηρεσίας) σε όλες τις κονσόλες όλων των χρηστών
- ***.*** **@syslog.server.dom** # αποστολή (δικτυακά) όλων των μηνυμάτων του συστήματος στο διακομιστή **syslog.server.dom**. Δέχεται και διευθύνσεις IP
- **auth,authpriv.*** **/var/log/auth** # αποστολή όλων των μηνυμάτων ασφαλείας στο αρχείο καταγραφής **/var/log/auth**

Παραδείγματα ρυθμίσεων σε syslog.conf

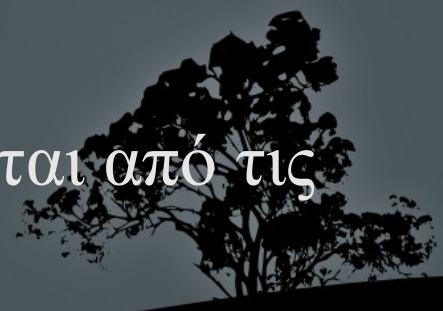
- **kern.crit /dev/console** # αποστολή κρίσιμων μηνυμάτων και υψηλότερων προτεραιοτήτων (crit, alert, emerg) πυρήνα σε κονσόλα (συνήθως /dev/tty1)
- **kern.=info;kern.=notice /dev/tty8** # αποστολή μόνο πληροφοριακών μηνυμάτων και επισημάνσεων πυρήνα στο τερματικό **/dev/tty8** (**Ctrl-Alt-F8**)
- **kern.info;daemon.!debug @10.0.0.10** # αποστολή πληροφοριών και άνω που αφορούν τον πυρήνα και οτιδήποτε μηνυμάτων που αφορούν δαίμονες (πλην το debug) στο διακομιστή **10.0.0.10**
- ***.info;mail.none;cron.none;news.none;authpriv.none \ /var/log/messages** # όλα τα πληροφοριακά και άνω, μηνύματα του συστήματος θα καταλήγουν στο **/var/log/messages** εκτός από τις υπηρεσίες **mail**, **cron**, **news**, και **authpriv**

Οι δαίμονες *syslogd* και *klogd*

- Το σύστημα Syslog αποτελείται από δύο δαίμονες, το **syslogd** και το **klogd**.
- Το **syslogd** ασχολείται με οτιδήποτε καταγραφές, πλην όσες αφορούν το πυρήνα. Για τις καταγραφές του πυρήνα υπάρχει το **klogd**
- Έχουν κοινό αρχείο ρυθμίσεων, το **/etc/syslog.conf**
- Για να ξεκινήσουν/σταματήσουν/επανεκκινήσουν κτλ, υπάρχει το σενάριο εκκίνησης:
  /etc/rc.d/init.d/syslog start|stop|restart|reload # σε RedHat
- Σε Debian δεν υπάρχουν δύο ξεχωριστοί δαίμονες αλλά ένα αναβαθμισμένο Syslog, το **rsyslog**:
  /etc/init.d/rsyslog start|stop|restart|reload # σε Debian

Χειροκίνητη καταγραφή μηνυμάτων με *logger*

- Η εντολή **logger** χρησιμοποιείται για την καταγραφή μηνυμάτων χειροκίνητα από κάποιο χρήστη ή κάποιο σενάριο
- **$ logger -p user.info "Strange behavior on console"**
  # αποστολή του μηνύματος εντός εισαγωγικών στο facility **user** με προτεραιότητα **info**
- **$ logger -t bug -p user.info "Strange behavior on \ console"** # αντικατάσταση του ονόματος του χρήστη στη αρχή του μηνύματος με **bug:**
- Το που θα καταλήξει το μήνυμα εξαρτάται από τις ρυθμίσεις στο **/etc/syslog.conf**

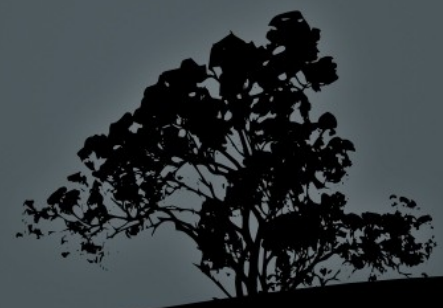


Ανανέωση/αρχειοθέτηση παλαιών αρχείων καταγραφής με *logrotate*

- Το **logrotate** έχει σχεδιαστεί για να εμποδίζει τα αρχεία καταγραφής να μεγαλώνουν ανεξέλεγκτα και να προκαλούν προβλήματα
- Μπορεί να αρχειοθετεί τα παλιά αρχεία, να τα συμπιέζει και να τα διαγράφει εφόσον ξεπεράσουν κάποια προκαθορισμένη διάρκεια ζωής. Μπορεί επίσης να στέλνει ως email κάποια αρχεία καταγραφής. Στη θέση των παλιών αρχείων δημιουργούνται καινούργια για να μπουν οι νέες πληροφορίες
- Η συμπεριφορά του ρυθμίζεται από το αρχείο **/etc/logrotate.conf** και τα επιμέρους αρχεία ρυθμίσεων κάτω από το κατάλογο **/etc/logrotate.d/***
- Τα παλιά αρχεία παίρνουν αριθμητικές τιμές στο όνομα τους και τα ακόμα πιο παλιά ενδεχομένων να συμπιέζονται με gzip, πχ **logfile**, **logfile.1**, **logfile.2.gz**, **logfile.3.gz**

Παράδειγμα /etc/logrotate.conf

weekly # προκαθορισμένη εβδομαδιαία αρχειοθέτηση
rotate 4 # προκαθορισμένη διατήρηση αρχείων μέχρι 4 εβδομάδες
create # δημιουργία καινούργιου αρχείου μετά την αρχειοθέτηση
include /etc/logrotate.d # συμπερίληψη των αρχείων κάτω από **/etc/logrotate.d**
/var/log/wtmp { # παραμετροποιημένες ρυθμίσεις για **wtmp**
    missingok # αν δεν υπάρχει το αρχείο μην παράξεις μήνυμα σφάλματος
    monthly # μηνιαία αρχειοθέτηση
    create 0664 root utmp # δημιουργία καινούργιου αρχείου με άδειες χρήσης
                                0664 και κυριότητα χρήστη root και ομάδας utmp
    rotate 1 # διαγραφή αρχείων παλαιότερα του ενός μηνός
}
/var/log/btmp { # παραμετροποιημένες ρυθμίσεις για **btmp**
    missingok #
    monthly #
    create 0660 root utmp #
    rotate 1 #
} #



Εργαλεία προβολής αρχείων καταγραφής

- Οποιοσδήποτε κειμενογράφος μπορεί να προβάλει τα αρχεία καταγραφής που είναι σε μορφή κειμένου. Για δυαδικά αρχεία υπάρχουν εργαλεία ανάλογα με την περίπτωση πχ last (wtmp)
- **# less /var/log/messages** # ο βασικός προβολέας αρχείων
- **# view /var/log/syslog** # η «μόνο για ανάγνωση» εκδοχή του vi
- **# zless /var/log/user.2.gz** # για προβολή συμπιεσμένων αρχείων κειμένου
- **# grep <string> -r /var/log** # αναδρομική αναζήτηση όρων αν δεν ξέρουμε που βρίσκεται κάτι
- **# zgrep <string> /var/log/auth.log.*.gz** # αναζήτηση σε συμπιεσμένα αρχεία κειμένου
- **# tail -f -n30 /var/log/secure** # προβολή των τελευταίων γραμμών ενός κειμένου και παρακολούθηση του αρχείου καθώς μεγαλώνει με καινούργια γεγονότα

Εργαστήριο 11

Ξεκινήστε και τις δύο εικονικές μηχανές και συνδεθείτε σαν ”root”

- **# ps aux | egrep -i "(syslog|klogd)"**
- **# /etc/rc.d/init.d/syslog restart** # σε RedHat
- **# /etc/init.d/rsyslog restart** # σε Debian
- **# view /etc/syslog.conf** # σε RedHat
- **# view /etc/rsyslog.conf** # σε Debian
- **# ls -la /etc/rsyslog.d** # σε Debian
- **# vi /etc/syslog.conf** # σε RedHat
  daemon.* /dev/tty8
  :wq
- **# service syslog restart**
- **Ctrl-F8**
- **Ctrl-F1**
- **# logger -p daemon.info "mysql dying \ painfully"**
- **# logger -p daemon.info -t mysql "mysql \ still dying painfully"**
- **Ctrl-F8**
- **Ctrl-F1**
- **# logger -p user.info "Testing by root"**
- **# su - user**
- **$ logger -p user.info "Testing by user"**
- **$ logger -t bug -p user.info "Testing by \ user"**
- **$ exit**

Εργαστήριο 11

- **# grep Testing -r /var/log**
- **# grep user -r /etc/rsyslog.*** # σε Debian
- **# grep user /etc/syslog.conf** # σε RedHat
- **# cd /var/log**
- **# find . -type f -exec ls -l {} \; | sort -k8 | less**
- **# vi /etc/logrotate.conf**
- **# tail -f /var/log.messages** # σε άλλο τερματικό
- **# logger -p lpr.notice -t printer "Printer is \ no more"less**
- **# less /var/log/auth.log.3.gz** # σε Debian
- **# zless /var/log/auth.log.3.gz** # σε Debian
- **# view /var/log/auth.log.3.gz** # σε Debian
- **# grep cron.daily /var/log/syslog*** # σε Debian
- **# zgrep cron.daily /var/log/syslog*** # σε Debian
- **# head -n20 /var/log/syslog** # σε Debian
- **# tail -n20 /var/log/syslog** # σε Debian
- **# tail -n20 /var/log/syslog** # σε Debian
- **# file /var/log/[bw]tmp**
- **# last**
- **# lastb**