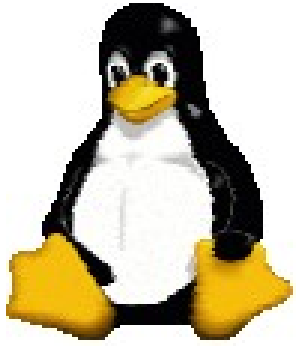
www.uom.gr
ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΟΙΚΟΝΟΜΙΚΩΝ ΚΑΙ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
τμήμα Εφαρμοσμένης Πληροφορικής

Προγραμματισμός Διαχείρισης Συστημάτων ΙΙ

Μάθημα 6ο

Καταγραφή συστήματος και Αρχεία καταγραφής



Μιχαηλίδης Παναγιώτης

Περιεχόμενα

- Καταγραφή συστήματος και αρχεία καταγραφής
  - Πολιτικές καταγραφής
  - Αρχεία καταγραφής Linux
  - Logrotate: Διαχείριση αρχείων καταγραφής
  - Syslog: Καταγραφή συστήματος
  - Παραμετροποίηση Syslog
  - Συμπύκνωση αρχείων καταγραφής

Πολιτικές καταγραφής

- Τι κάνουμε με τα αρχεία καταγραφής; Μερικές επιλογές:
  - Να κοιτάξουμε όλα τα δεδομένα άμεσα
  - Να διαγράφουμε τα αρχεία καταγραφής περιοδικά
  - Να "μετακινήσουμε" τα αρχεία καταγραφής, κρατώντας τα δεδομένα για ένα σταθερό διάστημα
  - Να συμπιέσουμε και να αρχειοθετήσουμε τα αρχεία καταγραφής σε μόνιμα μέσα αποθήκευσης

Κοιτάζουμε στα αρχεία καταγραφής

- Δεν συστήνεται!
- Χρειάζεται ένδειξη (ή απόδειξη) για προβλήματα ασφάλειας
- Ειδοποιήσεις για προβλήματα υλικού και λογισμικού
- Ιδανικά, κρατάμε τα δεδομένα για ένα μήνα
  - Ίσως πάρει μεγάλο διάστημα για ανακοίνωση ενός προβλήματος!
- Διαγραφή των αρχείων όταν ο δίσκος είναι πλήρες

Μετακίνηση αρχείων καταγραφής

- Κρατάμε ένα σύνολο προηγουμένων αρχείων καταγραφής
  - Μετακίνηση του τρέχοντος αρχείου μέσα στο σύνολο πάνω σε μια τακτική φάση (καθημερινά, εβδομαδιαία, κλπ)
  - Παράδειγμα

```
#!/bin/sh
cd /var/log
mv logfile.2 logfile.3
mv logfile.1 logfile.2
mv logfile logfile.1
touch logfile
chmod 600 logfile
```

  - Ίσως θέλουμε να προσθέσουμε συμπίεση, επαναφορά διακομιστή

Αρχειοθέτηση αρχείων καταγραφής

- Ίσως χρειαστεί να αρχειοθετήσουμε τα δεδομένα και αρχεία καταγραφής για πολιτική, ελέγχους κλπ
- Πρώτα μετακινούμε στο δίσκο
  - ταχύτερη πρόσβαση σε πρόσφατα δεδομένα
- Τότε γράφουμε σε μια ταινία ή σε άλλα μέσα
- Τα αρχεία καταγραφής πρέπει να είναι μέρος της ακολουθίας εφεδρικού αντίγραφου
  - Οι χάκερ έχουν τη τάση ή τη πρόθεση να τα διαγράφουν!

Αρχεία καταγραφής Linux

- Τα περισσότερα αρχεία καταγραφής εγγράφονται στην θέση /var/log
  - /var/adm ίσως επίσης να περιέχουν μερικά αρχεία (εξαρτάται από την διανομή)
- Τα περισσότερα προγράμματα στέλνουν εγγραφές καταγραφής στο syslog
  - /etc/syslog.conf συνήθως βάζει τις εγγραφές στο /var/log
- Αρχεία καταγραφής:
  - messages – κύριο αρχείο καταγραφής συστήματος
  - maillog – καταγραφή της δραστηριότητας sendmail
  - boot.log – έξοδος των αρχείων εκκίνησης συστήματος

Ειδικά αρχεία καταγραφής

- /var/log/wtmp
  - Καταγράφει τις συνδέσεις και αποσυνδέσεις των χρηστών
  - Δυαδική μορφή – χρησιμοποιούμε την last για ανάγνωση
  - Αποκοπή και παρακολούθηση
- /var/log/lastlog
  - Καταγραφή του χρόνου της τελευταίας σύνδεσης
  - Δυαδική μορφή
  - Σταθερό μέγεθος και δεν χρειάζεται μετακίνηση
- /var/log/dmesg
  - Απεικόνιση ενταμιευτή μηνυμάτων του πυρήνα στο τέλος της εκκίνησης

Logrotate

- Χρήσιμο εργαλείο για την διαχείριση των αρχείων καταγραφής
- Για την διαχείριση αναφερόμαστε σε ομάδες αρχείων καταγραφής

```
# Example log rotation
rotate 5
weekly
/var/log/messages {
    postrotate
        /bin/kill -HUP `cat /var/run/syslogd.pid`
    endscript
}
var/log/samba/*.log {
   notifempty
   copytruncate
   postrotate
       /bin/kill -HUP `cat /var/lock/samba/*.pid`
   endscript
```

Syslog

- Κατανοητό σύστημα καταγραφής
  - Ελευθερία στους προγραμματιστές από το να γράφουν δικά τους αρχεία
  - Επιτρέπει στους διαχειριστές συστημάτων να ελέγχουν την καταγραφή
- Ευελιξία
  - Μπορεί να ταξινομηθεί κατά προέλευση ή επίπεδο
  - Έξοδος σε μια ποικιλία περιφερειακών - αρχεία, τερματικά, άλλες μηχανές
- Μπορεί να είναι κεντρική η καταγραφή σε ένα βασικό υπολογιστή ελέγχου

Syslog (συνέχεια)

- Το syslog αποτελείται από τρία μέρη:
  - syslogd - δαίμονας καταγραφής (χρησιμοποιεί /etc/syslog.conf)
  - openlog – συναρτήσεις βιβλιοθήκης
  - logger - εντολή του φλοιού για υποβολή εγγραφών καταγραφής
- Οι εφαρμογές χρησιμοποιούν την βιβλιοθήκη για εγγραφή μηνυμάτων στην θέση /dev/log
- Syslogd διαβάζει τα μηνύματα από την /dev/log
  - Η έξοδος των μηνυμάτων εξαρτάται από το αρχείο /etc/syslog.conf

Παραμετροποίηση syslogd

- /etc/syslog.conf
  - Ελέγχει πως η syslog θα χειρίζεται τα μηνύματα
  - Απλό αρχείο κειμένου με κάθε γραμμή να έχει την εξής μορφή:
    - selector <tab> action
  - Ο selector επιλέγει ποια μηνύματα θα καταγραφούν
    - Ο selector είναι της μορφής facility.priority
    - Facility είναι το πρόγραμμα που στέλνει το μήνυμα
    - Priority είναι το επίπεδο του μηνύματος
  - Η action περιγράφει πως θα καταγράφονται τα μηνύματα

Παραμετροποίηση syslogd (συνέχεια)

- Selector
  - Οι ειδικές τιμές που χρησιμοποιούνται στο selector είναι οι εξής:
    - * - όλες οι πιθανές τιμές
    - none – χωρίς τιμές
  - Πολλαπλά facilities με την ίδια τιμή priority μπορούν να διαχωριστούν με κόμμα
  - Πολλαπλά selectors μπορούν να συνδυαστούν με ελ. ερωτηματικό
  - Το Linux επιτρέπει να προσθέσουν μπροστά στο επίπεδο priority τους χαρακτήρες:
    - = - Μόνο αυτή η προτεραιότητα
    - ! - Εκτός αυτής της προτεραιότητας και άνω
    - != - Όλα εκτός της προτεραιότητας που ορίζεται

Παραμετροποίηση syslogd (συνέχεια)

Facility	Messages from
• kern	The kernel
• user	user processes
• mail	The sendmail daemon and other mail software
• cron	The cron daemon
• auth	Security and authorization commands
• lpr	The printing system
• ftp	The ftp daemon
• daemon	Other system daemons
• local0 -local7	Local messages
• syslog	Internal messages from syslogd

Παραμετροποίηση syslogd (συνέχεια)

- Priority
  - Οκτώ επίπεδα προτεραιτότητας, από υψηλό προς χαμηλό

Priority	Description	Priority
emerg	Panic situations	0 – Highest
alert	Urgent situtations	1
crit	Critical conditions	2
err	Other error conditions	3
warning	Warning messages	4
notice	Attention messages	5
info	Informational messages	6
debug	For debugging only	7 - Lowest

Παραμετροποίηση syslogd (συνέχεια)

- Action
  - Syslogd εγγράφει μηνύματα στην θέση που προσδιορίζεται από την action
  - Μόνο μια action προσδιορίζεται σε κάθε γραμμή

Action	Description
filename	Writes the message to a file on the local machine
@hostname	Forwards the message to the syslogd on hostname
@ipaddress	Forwards the message to the host at IP add
|fifo	Writes the message to a FIFO (named pipe)
User1, user2	Writes the message to users' screens
*	Writes the messages to all logged in users

Δείγμα syslog.conf

```
# Emergencies: tell everyone who is logged in
*.emerg;user.none                       *
*.warning;daemon,auth.info,user.none var/log/messages

# Forward important messages to the central logger
*.warning;daemon,auth.info      @netloghost

# printer errors
lpr.debug                               /var/log/lpd-errs
```

Δείγμα εξόδου syslog

```
Apr 22 04:04:21 wume1 named[2826]: lame server resolving '211.68.246.64.in-addr.arpa' (in '68.246.64.inaddr.arpa'?): 160.79.6.130#53
Apr 22 13:22:41 wume1 sshd(pam_unix)[16776]: session opened for user panosm by (uid=0)
Apr 22 13:22:44 wume1 su(pam_unix)[16802]: session opened for user root by panosm (uid=501)
Apr 25 20:31:57 wume1 sshd(pam_unix)[28375]: check pass; user unknown
Apr 25 20:32:00 wume1 sshd(pam_unix)[28375]: 1 more authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=
```

Συμπύκωση αρχείων καταγραφής

- Το syslog (και άλλα προγράμματα καταγραφής) δημιουργεί πάρα πολλά αρχεία καταγραφής
- Χρειάζεται εργαλεία για την σάρωση των αρχείων καταγραφής και να εντοπίζουμε σημαντικές εγγραφές:
  - Εγγραφές που έχουν σχέση με την ασφάλεια
  - Μηνύματα σχετικά με το χώρο του δίσκου
  - Μηνύματα που επαναλαμβάνονται πολλές φορές