Εργαστήριο 3

Ασκήσεις: Διαχείριση συστήματος (αρχεία με σημαντικές πληροφορίες)

Πιο κάτω θα δούμε κάποια σημαντικά αρχεία που βρίσκονται σε συστήματα UNIX και περιέχουν διάφορες πληροφορίες χρήσιμες για το διαχειριστή του συστήματος

Αρχείο /etc/passwd

Το αρχείο /etc/passwd σε συστήματα τύπου Unix περιέχει πληροφορίες για τους χρήστες του συστήματος. Κάθε γραμμή του αρχείου αντιστοιχεί σε έναν χρήστη και περιέχει διάφορες πληροφορίες διαχωρισμένες με άνω-κάτω τελείες :. Παρόλο που το αρχείο ονομάζεται "passwd" (password), δεν περιέχει τους κωδικούς πρόσβασης των χρηστών σε σύγχρονα συστήματα, καθώς αυτοί αποθηκεύονται στο αρχείο /etc/shadow.

Δομή του /etc/passwd
Κάθε γραμμή έχει 7 πεδία, τα οποία είναι:

```
username:x:UID:GID:comment:home_directory:shell
```

Επεξήγηση των πεδίων:

username: Το όνομα χρήστη (login name). Χρησιμοποιείται για την ταυτοποίηση του χρήστη κατά την είσοδο στο σύστημα.

x: Αυτό το πεδίο παλιότερα περιείχε τον κρυπτογραφημένο κωδικό πρόσβασης (password). Σε σύγχρονα συστήματα, αυτό το πεδίο περιέχει απλά το γράμμα x, που δείχνει ότι ο κωδικός πρόσβασης αποθηκεύεται στο αρχείο /etc/shadow.

UID: Το User ID. Αυτός είναι ο αριθμητικός αναγνωριστικός αριθμός χρήστη (User Identifier). Κάθε χρήστης έχει ένα μοναδικό UID στο σύστημα. Οι τυπικοί χρήστες έχουν UID συνήθως από 1000 και πάνω, ενώ οι συστημικοί χρήστες και οι υπηρεσίες έχουν μικρότερα UID.

GID: Το Group ID. Είναι το αναγνωριστικό αριθμός της ομάδας στην οποία ανήκει ο χρήστης (Group Identifier). Αυτή η τιμή καθορίζει την κύρια ομάδα του χρήστη.

comment: Μια προαιρετική περιγραφή ή σχόλιο για τον χρήστη. Συχνά χρησιμοποιείται για το πραγματικό όνομα του χρήστη ή άλλες πληροφορίες όπως email ή το τμήμα της εταιρείας όπου εργάζεται.

home_directory: Ο απόλυτος φάκελος στον οποίο βρίσκεται ο προσωπικός κατάλογος (home directory) του χρήστη. Αυτός ο κατάλογος είναι ο χώρος όπου ο χρήστης μπορεί να αποθηκεύει τα προσωπικά του αρχεία.

shell: Το πρόγραμμα που εκτελείται όταν ο χρήστης συνδέεται στο σύστημα. Συνήθως είναι το bash ή κάποιο άλλο κέλυφος (shell), αλλά μπορεί επίσης να είναι προγράμματα που εμποδίζουν την πρόσβαση (π.χ. /bin/false).

Παράδειγμα μιας γραμμής από το /etc/passwd:

```
john:x:1001:1001:John Doe:/home/john:/bin/bash
```

Ανάλυση του παραδείγματος:
john: Το όνομα χρήστη είναι "john".
x: Ο κωδικός πρόσβασης δεν αποθηκεύεται στο /etc/passwd.
1001: Το UID του χρήστη είναι 1001.
1001: Το GID της κύριας ομάδας του χρήστη είναι επίσης 1001.
John Doe: Αυτό είναι το σχόλιο που περιγράφει τον χρήστη.
/home/john: Ο προσωπικός κατάλογος του χρήστη είναι /home/john.
/bin/bash: Το κέλυφος (shell) που εκτελείται κατά την είσοδο στο σύστημα είναι το bash.

Το αρχείο /etc/passwd είναι σημαντικό για την ταυτοποίηση των χρηστών στο σύστημα και τη διαχείριση των πληροφοριών τους.

Αρχείο /var/log/lastlog και εντολή lastlog

Το αρχείο /var/log/lastlog είναι ένα δυαδικό αρχείο σε συστήματα τύπου Unix που περιέχει πληροφορίες σχετικά με την τελευταία επιτυχημένη σύνδεση κάθε χρήστη. Κάθε χρήστης έχει μία εγγραφή στο αρχείο αυτό, και οι πληροφορίες που περιλαμβάνονται περιγράφουν:

Την ημερομηνία και ώρα της τελευταίας σύνδεσης.
Τη διεύθυνση IP ή το όνομα του host από όπου έγινε η σύνδεση.
Το τερματικό (TTY) που χρησιμοποιήθηκε για τη σύνδεση.

Το αρχείο lastlog δεν είναι ένα απλό αρχείο κειμένου, αλλά δυαδικό (binary), γι' αυτό δεν μπορεί να διαβαστεί απευθείας με έναν επεξεργαστή κειμένου. Αντ' αυτού, υπάρχει η εντολή lastlog που επιτρέπει την ανάγνωση και την εμφάνιση των δεδομένων του.

Παράδειγμα χρήσης της εντολής lastlog:

```
lastlog
```

Αυτό θα εμφανίσει μια λίστα με τους χρήστες του συστήματος και πληροφορίες για την τελευταία τους σύνδεση, σε μορφή πίνακα που περιλαμβάνει:

Username: Το όνομα χρήστη.
Port/TTY: Το τερματικό (port/TTY) που χρησιμοποιήθηκε.
From: Η διεύθυνση IP ή το όνομα του host από όπου έγινε η σύνδεση.
Last Login: Η ημερομηνία και η ώρα της τελευταίας σύνδεσης.

Παράδειγμα εξόδου:

```
Username      Port     From             Latest
root          pts/0    192.168.1.2      Wed Sep 12 14:23:45 +0200 2024
john          pts/1    192.168.1.3      Mon Sep 10 09:17:12 +0200 2024
avahi                                   **Never logged in**
```

Σημειώσεις:
Αν κάποιος χρήστης δεν έχει συνδεθεί ποτέ, το πεδίο της τελευταίας σύνδεσης θα εμφανίζει "**Never logged in**".

Το αρχείο /var/log/lastlog ενημερώνεται αυτόματα κάθε φορά που ένας χρήστης συνδέεται στο σύστημα.
Το lastlog είναι χρήσιμο για να παρακολουθούμε τις τελευταίες επιτυχημένες συνδέσεις των χρηστών, να εντοπίζουμε τυχόν μη εξουσιοδοτημένη πρόσβαση ή να ελέγχουμε αν κάποιοι χρήστες δεν έχουν συνδεθεί ποτέ.

Αρχείο /var/log/dnf.log

Το αρχείο /var/log/dnf.log είναι το αρχείο καταγραφής (log) του DNF package manager σε συστήματα Linux που χρησιμοποιούν το DNF (Dandified YUM) για τη διαχείριση πακέτων λογισμικού, όπως το Fedora, το RHEL (Red Hat Enterprise Linux), και το CentOS.

Το αρχείο /var/log/dnf.log περιέχει αναλυτικές καταγραφές σχετικά με τις ενέργειες που γίνονται κατά τη διαχείριση των πακέτων λογισμικού, όπως:

Εγκαταστάσεις πακέτων.
Αναβαθμίσεις πακέτων.
Απεγκαταστάσεις πακέτων.
Αναζητήσεις ή άλλα αιτήματα που γίνονται μέσω της εντολής dnf.

Κάθε ενέργεια που πραγματοποιείται μέσω του DNF καταγράφεται στο αρχείο με λεπτομέρειες όπως:

Ημερομηνία και ώρα της ενέργειας.
Χρήστης που εκτέλεσε την εντολή.
Ονόματα πακέτων που επηρεάστηκαν (εγκαταστάθηκαν, αφαιρέθηκαν, αναβαθμίστηκαν).
Ενέργειες που πραγματοποιήθηκαν (install, remove, update).
Πηγές από όπου λήφθηκαν τα πακέτα.

Παράδειγμα περιεχομένου:

```
2024-09-13T15:45:41+0300 INFO --- logging initialized ---
2024-09-13T18:32:01+0300 INFO DNF version: 4.7.0
2024-09-13T20:19:01+0300 INFO Command line: dnf install httpd
2024-09-13T22:22:01+0300 INFO Installed: httpd-2.4.51-1.fc3.x86_64
```

Χρήση:

- Αναζήτηση προβλημάτων: Αν παρουσιαστούν προβλήματα κατά την εγκατάσταση ή την αναβάθμιση πακέτων, το αρχείο αυτό μπορεί να χρησιμοποιηθεί για να εντοπιστεί το σφάλμα.
- Ιστορικό ενεργειών: Παρέχει ένα πλήρες ιστορικό όλων των ενεργειών που έχουν πραγματοποιηθεί με το DNF, διευκολύνοντας την παρακολούθηση αλλαγών στο σύστημα.
- Ασφάλεια: Μπορεί να χρησιμοποιηθεί για την ανίχνευση μη εξουσιοδοτημένων ή ύποπτων αλλαγών στο σύστημα λογισμικού.

Το dnf.log είναι ένα από τα βασικά αρχεία καταγραφής που βοηθούν τους διαχειριστές συστήματος να διατηρούν τον έλεγχο στις ενέργειες διαχείρισης πακέτων.

Ερωτήσεις

Με βάση τις πιο πάνω πληροφορίες απαντήστε τις ερωτήσεις:

1) Από το αρχείο /etc/passwd εκτυπώστε όλα τα login shells αλλά να εμφανίζεται μια φορά το καθένα.

2) Από το αρχείο /etc/passwd εκτυπώστε ποιο login shells χρησιμοποιείται από τους περισσότερους χρήστες και πόσους.

3) Από το αρχείο /etc/passwd εκτυπώστε τους προσωπικούς καταλόγους των χρηστών που δεν περιέχουν μέσα το var.

4) Από το αρχείο /etc/passwd μετατρέψετε όλα τα usernames σε κεφαλαία γράμματα και εκτυπώστε τα.

5) Εκτυπώστε τους χρήστες που ενώθηκαν στη μηχανή που είστε συνδεδεμένοι τον τρέχοντα μήνα Να εμφανίζονται όλες οι πληροφορίες (Username, Port, From, Latest). Μην γράψετε τον τρέχοντα μήνα ρητά μέσα στην εντολή π.χ. Sep αλλά διαβάστε τον από την εντολή date.

6) Εκτυπώστε μόνο τα usernames των χρηστών που ενώθηκαν στη μηχανή που είστε συνδεδεμένοι τον τρέχοντα μήνα, μέρα Παρασκευή από τις 10:00 μέχρι και τις 10:59 και αποθηκεύσετε τα το ένα δίπλα στο άλλο (χωρισμένα με space) σε αρχείο με το όνομα users.txt.

7) Βρείτε και εκτυπώστε πιθανά λάθη (γραμμές που περιέχουν τη λέξη error) που προέκυψαν κατά την εγκατάσταση, αναβάθμιση ή απεγκατάσταση πακέτων στη μηχανή σας.

8) Βρείτε όλα τα αρχεία (όχι καταλόγους) που βρίσκονται μέσα στον κατάλογο /var μέχρι και 3 επίπεδα βάθος τα οποία έχουν την κατάληξη .log Αν υπάρχουν κάποιες γραμμές στα αποτελέσματα που έχουν το "Permission denied" να τις απορρίψετέ (επειδή αυτά τυπώνονται στο stderr, η απόρριψη των γραμμών αυτών μπορεί να γίνει με εκτροπή του stderr στο /dev/null).

9) Συνεχίστε την πιο πάνω εντολή έτσι ώστε να δείτε στη συνέχεια και τα permissions των αρχείων αυτών.