

# LINUX SERVER ADMINISTRATION

## DOCUMENTATIE CURS

DOCUMENTATIE

INTREABA PROFESORUL

CURSURILE MELE

7 Serverul Apache » 7.5 Configurare Apache » 7.5.5 Controlul accesului la resurse

- 1. Shell Scripts
- 2. Linux Kernel
- 3. Serverul DHCP
- 4. Serverul FTP
- 5. NFS - Network File System
- 6. Serverul DNS
- 7. Serverul Apache
  - 7.1 Protocolul HTTP
  - 7.2 Prezentare generala server
  - 7.3 Compilare si instalare
  - 7.4 Structura Apache
  - 7.5 Configurare Apache
    - 7.5.1 Sectiuni de configurare
    - 7.5.2 Configurare Minimala
    - 7.5.3 Directive principale
    - 7.5.4 Virtual Hosting
    - 7.5.5 Controlul accesului la resurse
      - 7.5.5.1 Acces in functie de IP
      - 7.5.5.2 Acces in functie de user si parola
      - 7.5.5.3 Autorizare acces (Apache 2.4)
  - 7.6 PHP
    - 7.7 Securitate Web
- 8. Serverul MySql
- 9. NETFILTER
- 10. Sistemul de e-Mail
- 11. Serverul Postfix
- 12. Serverul POP/IMAP
- 13. Managementul Logurilor
- 14. Exemple practice (Ubuntu 14.04 LTS)
- 15. Webmin

## Controlul accesului la resurse

- 7.5.5.1 Acces in functie de IP
- 7.5.5.2 Acces in functie de user si parola
- 7.5.5.3 Autorizare acces (Apache 2.4)

Modul default de functionare al serverului Apache presupune ca acesta serveste orice fisier din orice director de sub directorul definit de **DocumentRoot** clientilor.

Pentru un site de prezentare acest comportament este acceptabil, dar pentru un sistem informatic, pentru o sectiune de administrare, pentru un Intranet sau pentru un site care contine informatii sensibile sau confidentiale, Apache trebuie sa limiteze accesul la resurse doar pentru clientii autorizati.

Exista 2 moduri in care Apache poate limita accesul la resurse:

1. In functie de IP-ul de la care se conecteaza clientul

Aceasta varianta este optima in momentul in care accesul la informatiile confidentiale se realizeaza de la un IP sau grup de IP-uri cunoscute dinainte.

In cazul in care conexiunea are loc de pe Internet limitarea accesului in functie de IP este considerata foarte sigura. IP-ul public este furnizat de un ISP, iar un posibil Cracker nu poate sub nicio forma folosi un IP care nu i-a fost setat de provider.

2. In functie de username si parola

Aceasta varianta este optima in momentul in care accesul la informatiile confidentiale se realizeaza de la IP-uri dinamice, necunoscute apriori cum ar fi cazul utilizatorilor mobili care doresc accesarea informatiei de oriunde s-ar afla.

### Nota



Pentru o securitate crescuta serverul web poate fi configurat pentru ambele moduri de restrictionare a accesului.