LINUX SERVER ADMINISTRATION

DOCUMENTATIE CURS

Securitate si performanta

Incercari de introducere parola la autentificare inainte de deconectare
MaxLoginAttempts 3

Default este none cu sens de unlimited si seteaza nr. clientilor de la up IP care se pot conecta simultan. Atentie la NAT.
Se poate folosi un mesaj indicat clientului la depasire. %m este maximum.
MaxClientsPerHost 2 "Too many (%m) from your IP"

Nr. maxim de clienti conectati cu acelasi username. Default none.
MaxClientsPerUser 1 "Only one such user at a time."

Nr. Maxim de conexiuni noi pe secunda acceptate pt. intreg serverul
MaxConnectionRate 2

Nr. maxim de conexiuni neautentificate per IP
MaxConnectionsPerHost 1 "Sorry, you may not connect !!"

The MaxHostsPerUser directive configures the maximum number of times different hosts, using a given login,
can connect at any given time. The optional argument message may be used which will be displayed to a
client attempting to exceed the maximum value. If message is not supplied, a default message of
"Sorry, the maximum number of hosts (%m) for this user already connected
MaxHostsPerUser 2

The TimeoutNoTransfer directive configures the maximum number of seconds a client is
allowed to spend connected, after authentication, without issuing a command which results in creating
an active or passive data connection (i.e. sending/receiving a file, or receiving a directory listing).
TimeoutNoTransfer 300

Limitarea accesului la un director in functie de IP

Definitie

O clasa reprezinta o serie de IP-uri sau retele carora li se acorda acelasi tratament din punct de vedere al permisiunilor si limitarilor. Un IP poate apartine unei singure clase. In cazul in care un IP apartine mai multor clase, se considera ca facand parte din prima clasa definita in profpd.conf

Exemplu:

```
<Class internal>
   From 192.168.0.0/16
 </Class>
<Class cma>
      From 81.0.0.0/16
      From 61.11.60.46
      From 28.76.0.0/16
 </Class>

<Class foo>
   From *.example.com
   From !bad.example.com
   Satisfy all
 </Class>
```

Optiunea Satisfy all are sensul ca toate "From-urile" dintre clasa trebuie sa fie satisfacute (si logic). Default este any (sau logic) intre "from-uri".

O clasa se foloseste apoi in combinatie cu <Limit> si <Directory> si cu AllowClass sau DenyClass.

<Directory> se foloseste pentru a stabili anumite optiuni de ftp (pt. un anumit director si toate subdirectoarele sale recursiv. Optiunile pt. directorul respectiv se specifica intre <Directory> si </Directory>

Sectiunea de configurare dintre <Limit> si </Limit> permite un control foarte exact asupra comenzilor ftp care pot fi executate de diferiti useri.

Grupurile de comenzi ftp sunt:

- ALL: include toate comenzile FTP mai puti LOGIN
- DIRS: include comenzi referitoare la directoare (mutare in director, listare director etc)
- LOGIN: comenzi referitoare la logarea clientilor
- READ: comenzi referitoare la citire fisiere si directoare
- WRITE: comenzi referitoare la scriere fisiere si directoare

Exemplu:

```
#Directorul /home/crystalmindacademy precum si toate subdirectoarele sale pot fi
accesate (limita ALL - mutare in director, citire continut, scriere continut etc) doar de la retele precizate in clasa numita cma.

#definim clasa cma
<Class cma>
        From 81.0.0.0/16
        From 61.11.60.46
        From 28.76.0.0/16
 </Class>

 #precizam containerul de tip Directory. Optiunile se vor referi doar la directorul respectiv in mod recursiv
<Directory /home/crystalmindacademy>
       #limitam toate comenzile de ftp (fara login)
       <Limit ALL>
              #doar cei de la ip-urile respective au acces, restul nu.
              AllowClass cma
              DenyAll
        </Limit>
</Directory>
```

Limitare useri care se pot autentifica la server

```
<Limit LOGIN>
       AllowUser u1,u2,u3,admin
       DenyAll
</Limit>
```

Se poate folosi si varianta DenyUser/DenyGroup. Cei care nu sunt in lista sunt permisi.

```
<Limit LOGIN>
       DenyUser u1,u2,u3
       DenyAll
</Limit>
```

Limitare grupuri care se pot autentifica la server

```
<Limit LOGIN>
       AllowGroup gr1,gr2
       DenyAll
</Limit>
```

Limitare in functie de director.

```
#Comanda ftp RETR se foloseste pt transfer de pe server pe client
<Directory /home/crystalmind/website>
       <Limit RETR>
              DenyAll
```

```
    </Limit>
</Directory>
```