LINUX SERVER ADMINISTRATION

DOCUMENTATIE CURS

Acces in functie de IP

Modulul care introduce directivele ce realizeaza accesul la resursele serverului in functie de IP-ul clientului este mod_authz_host pentru Apache 2.4

Directivele folosite pentru restrictionara accesului sunt: Order, Allow si Deny si se folosesc in interiorul unui container <Directory> pentru stabilirea accesului la un intreg director, <Location>, <Files> sau <FilesMatch> pentru stabilirea accesului doar la anumite fisiere.

Directiva Allow specifica IP-urile de la care se permit conexiuni. Se pot folosi atat IP-uri cat si clase de IP-uri sau nume de domenii.

Exemplu

1. Permite conexiuni la server de la un singur IP

```
Allow from 192.168.0.1
Allow from 88.0.0.1
```

2. Permite un intreg domeniu (com sau www.crystalmind.ro). Serverul realizeaza un reverse DNS pentru translatarea IP-ului in nume de domeniu care ulterior este folosit pentru evaluare

```
Allow from .com
Allow from www.crystalmind.ro
```

3. Permite un intreg range de IP-uri folosind un prefix (/8)

```
Allow from 10.0.0.0/8
```

4. Verifica doar partial (sa inceapa cu 10 sau 172.16)

```
Allow from 10 172.16
```

5. Permite pentru un IPv6

```
Allow from 2001:db8::a00:20ff:fea7:ccea
```

6. Permite toate IP-urile

```
Allow from all
```

Directiva Deny specifica IP-urile de unde nu se permit conexiuni. Modul de folosire este identic cu cel al directivei Allow

Exemplu

1. Blocheaza un singur IP

```
Deny from 192.168.0.90
```

2. Blocheaza un intreg range de IP-uri

```
Deny from 88.0.0.0/16
```

3. Blocheaza in functie de domeniu. Serverul Apache realizeaza reverse DNS

```
Deny from evil.linux.com
```

4. Blocheaza conexiuni de la toate IP-urile

```
Deny from all
```

A 3-a directiva necesara, Order poate avea 2 forme si stabileste ordinea de evaluare.

Cele 2 forme sunt:

1. Order Allow,Deny
Prima data sunt evaluate toate directivele Allow. Daca nici una nu este adevarata requestul clientului este rejectat.
Deny este policy: ce nu este permis de un Allow este rejectat

```
<Directory /opt/apache/htdocs/crystalmind.ro/website/cursuri>
Order Allow,Deny
Allow from crystalmind.ro
Deny from 88.0.0.1
</Directory>
```

Pentru directorul /opt/apache/htdocs/crystalmind.ro/website/cursuri sunt permise doar requesturile de la IP-urile care se rezolva invers in DNS in crystalmind.ro. Requesturile de la 88.0.0.1 precum si restul requesturilor sunt rejectate.

2. Order Deny, Allow
Prima data sunt evaluate toate directivele Deny. Daca vreuna este adevarata FARA ca IP-ul clientului sa fie "prins" si de o directiva Allow, requestul este rejectat. Requesturile care nu corespund cu nicio directiva Deny sau Allow sunt permise.
Allow este Policy: ce nu este rejectat de un Deny este permis

```
<Directory /opt/apache/htdocs/crystalmind.ro/website>
Order Deny,Allow
Deny from 88.0.0.1
Deny from 192.168.0.0/24
</Directory>
```

Pentru directorul /opt/apache/htdocs/crystalmind.ro/website requesturile de la IP-ul 88.0.0.1 sau din subnetul 192.168.0.0/24 sunt rejectate. Restul requesturilor sunt permise din cauza ordinei de evaluare Deny, Allow

Orice fisier cu terminatia sau extensia xls este servit doar daca clientul se conecteaza de la 88.0.0.1

```
<FilesMatch "\.xls$">
    Order Allow,Deny
    Allow from 88.0.0.1
</FilesMatch>
```

Important

Modulul de evaluare al directivelor Allow si Deny este diferit de modul de evaluare a regulilor unui Firewall. Regulile unui firewall sunt evaluate pana cand o regula 'prinde' pachetul caz in care se executa o actiune fara a se mai evalua restul regulilor.
In cazul directivelor Allow si Deny toate regulile se evalueaza pana la final ceea ce determina ca ordinea in care acestea apar sa nu fie importanta ceea ce este in contrast cu un firewall.

Resurse:

- IP-based Access Control
- mod_authz_host, Allow, Deny si Order - Documentatia oficiala

Accesul la resurse in functie de IP

Durata: 5.40 min
Marime: 10.04MB