

Administrarea sistemelor Linux

Cursul 12

Configurarea serviciilor sistemului – partea V

Dragoș Acostăchioaie

<http://www.adt.ro>

dragos@adt.ro

Cursul 12

Astazi vom studia:

- **Serviciul de posta electronica – sistemul *postfix***
- **Sistemul numelor de domenii - BIND**

Serviciul de posta electronica - Introducere

- unul dintre primele servicii oferite de Internet
- un sistem de posta electronica este alcatuit din trei componente:
 - agenti utilizator (MUA = *Mail User Agent*) – programe client care permit utilizatorilor sa citeasca, sa emita si sa gestioneze mesajele (exemple: pine, mutt, Kmail, Evolution, Mozilla Mail)
 - agenti de transport (MTA = *Mail Transport Agent*) – programe responsabile cu acceptarea mesajelor primite si livrarea acestora la destinatia finala (exemple: sendmail, postfix, qmail)
 - agenti de distributie (MDA = *Mail Distribution Agent*) – programe care filtreaza si directioneaza mesajele primite catre diferite destinatii (exemplu: procmail)

Serviciul de posta electronica - Introducere

- sistemul numelor de domenii (DNS) are un rol important in cadrul mecanismului de livrare a mesajelor
- pentru a trimite un mesaj de la o masina la alta, agentul de transport va efectua o interogare DNS pentru a determina masina care va receptiona mesajul pentru domeniul din care face parte sistemul destinatie
- inregistrarile MX (*Mail eXchanger*) din cadrul descrierii unui domeniu indica masinile care vor primi mesaje pentru respectivul domeniu

Sistemul *postfix*

- fisierele de configurare se gasesc in /etc/postfix
- mesajele primite sunt stocate in /var/spool/mail (pentru fiecare utilizator cate un fisier avand numele sau)
- cozile de mesaje expediate sunt stocate in /var/spool/postfix
- fisierul jurnal este /var/log/maillog
- coada de asteptare poate fi consultata cu ajutorul comenzii mailq
- gestiunea cozii de mesaje se face prin comanda postsuper
 - postsuper -d *id*
 - sterge din coada mesajul avand identificatorul specificat
 - ALL = toate mesajele

Sistemul *postfix* – fisierul *access*

- fisierul *access* permite controlul accesului la serviciile oferite de server
- are formatul *specificatie actiune*
- *specificatie* poate avea unul dintre formatele:
 - utilizator@domeniu* - specifica dreptul de acces al adresei e-mail
specificate
 - utilizator@* - regula se va referi la numele de cont expeditor specificat
 - .domeniu* – numele domeniului
 - retea* – adresa retelei la care se refera regula de acces
- *actiune* poate lua valorile:
 - REJECT [*cod_eroare text*] - refuza mesajele, returnand codul de eroare si textul mentionate
 - OK – accepta mesajele
 - HOLD [*text*] - pune mesajul intr-o coada de asteptare, trimitand mesajul specificat catre fisierul-jurnal

Sistemul *postfix* – fisierul *access*

DISCARD [*text*] - raspunde ca si cum mesajul ar fi fost acceptat,
trimitand optional un text in fisierul pentru jurnalizare

- dupa modificarea fisierului *access*, va trebui apelata comanda:

`postmap /etc/postfix/access`

- exemplu:

localhost OK

.infoiasi.ro OK

Sistemul *postfix* – fisierul *aliases*

- pseudonimele (*aliases*) reprezinta nume echivalente pentru utilizatorii definiti pe sistem
- pot fi folosite pentru a redirectiona mesajele catre alte adrese (eventual pe alte masini), fisiere sau catre alte programe (mecanismul pipe)
- se configureaza prin `/etc/postfix/aliases` (sau standard `/etc/aliases`):
 - pseudonim: destinatie*
- *destinatie* poate fi:
 - un nume de utilizator
 - o lista de utilizatori, separati prin virgula
 - o adresa de e-mail
 - un fisier (prin specificarea caii complete a acestuia, incepand cu “/”)
 - o comanda a carei intrare va fi constituita de mesaj, trimis prin intermediul mecanismului pipe (prin prefixarea comenzii cu “|”)

Sistemul *postfix* – fisierul *aliases*

- dupa modificarea fisierului *aliases*, trebuie apelata comanda `newaliases`
- pentru activarea mecanismului *aliases*, trebuie ca `main.cf` sa contina:
`aliases_database = hash:/etc/aliases`
- exemplu:
webmaster: dragos
sales: dragos,sabin,bubu
procmail: “/usr/bin/procmail”
- utilizatorii isi pot defini si singuri asemenea pseudonime, prin intermediul fisierului `.forward`, plasat in directorul *home*, in acelasi format cu fisierul *aliases*

Sistemul *postfix* – fisierul *main.cf*

- fisierul principal de configurare al postfix este *main.cf*
- stabilirea valorilor pentru parametrii postfix are formatul:
nume_parametru = valoare
- parametrii pot fi referiti prin *\$nume_parametru*

Nume de masina si domeniu

myhostname – numele masinii

mydomain – numele domeniului

myorigin – numele de origine care urmeaza numele utilizatorului in mesajele expediate (exemplu: *\$mydomain*)

mydestination – lista de masini si domenii pentru care serverul postfix va fi considerat destinatie finala (implicit, nu sunt acceptate decat mesajele adresate masinii)

Sistemul *postfix* – fisierul *main.cf*

Retransmiterea mesajelor

`relay_domains` – specifica spre ce destinatii va fi permisa retransmiterea mesajelor

`relayhost` – masina spre care va fi trimis mesajul, acesta urmand a fi retransmis mai departe de catre aceasta, atunci cand nu exista alta modalitate de transport

`mynetworks` – lista de retele carora li se permite retransmiterea mesajelor, in formatul *adresa_retea/masca_de_retea*

`inet_interfaces` – interfata de retea de pe care vor fi acceptate mesaje

Combaterea spam-ului

`reject_unknown_client` – refuza cererile provenite de pe masini al caror nume nu poate fi rezolvat printr-o interogare DNS

Sistemul *postfix* – fisierul *main.cf*

- `reject_invalid_hostname` – refuza mesajele avand numele masinii expeditoare gresit
- `reject_unknown_hostname` – refuza mesajele avand numele masinii expeditoare fara intregistrare DNS
- `reject_unknown_sender_domain` – refuza mesajele avand domeniul masinii expeditoare fara inregistrare DNS
- exemplu:
 - `myhostname = fenrir.infoiasi.ro`
 - `mydomain = infoiasi.ro`
 - `myorigin = infoiasi.ro`
 - `mydestination = localhost, fenrir.infoiasi.ro, infoiasi.ro`
 - `relay_domains = infoiasi.ro`
 - `aliases_database = hash:/etc/aliases`

Sistemul numelor de domenii - Introducere

- numele de masina permit referirea mai usoara a unui calculator conectat la Internet, in locul adresei IP a acestuia
- rezolvarea (translarea) in ambele sensuri a numelui/adresei se realizeaza prin intermediul sistemului numelor de domenii – DNS
- translarea adresei IP in nume se numeste rezolvarea inversa
- sistemul DNS este o uriasa baza de date distribuita, intinsa pe intreg globul
- sistemul este implementat de catre serverele DNS, care furnizeaza informatii despre unul sau mai multe domenii
- domeniile sunt numite *zone*
- pentru fiecare zona exista cel putin un server de nume care contine informatiile despre masinile din cadrul domeniului
- primul server se numeste server DNS *primar*, care descrie zona numita *master*, si care incarca configurariile dintr-o serie de fisiere de configurare

Sistemul numelor de domenii - Introducere

- celelalte servere se numesc *secundare*, si deservesc zonele denumite *slave*, acestea transferand informatiile despre zone de la serverul primar
- pentru a micsora timpul de rezolvare a adreselor si a reduce traficul, serverele de nume stocheaza informatiile obtinute in urma cererilor intr-o zona-tampon (cache) local
- serverele care gestioneaza informatiile despre masinile din cadrul unei zone se numesc *autoritare* pentru respectiva zona si reprezinta serverele DNS primare
- un server DNS este autoritar doar pentru masina locala, atunci cand este folosit pentru a memora inregistrari DNS in zona tampon, fiind numit *caching-only name server*
- o informatie din baza de date DNS este denumita *inregistrare de resursa*, RR (*Resource Record*)

Sistemul numelor de domenii - Introducere

- fiecare inregistrare are asociat un tip care descrie informatia pe care o reprezinta si o clasa care specifica la ce tip de retea se refera
- serverele DNS pot raspunde la cereri in doua moduri:
 - cererile recursive sunt utilizate atunci cand un client efectueaza o cerere, iar raspunsul nu se gaseste in zona deservita de acesta, serverul fiind nevoit sa parcurga ierarhia DNS pentru a gasi raspunsul
 - cererile nerecursive, utilizate atunci cand un client efectueaza o cerere al carei raspuns nu se afla in zona deservita, serverul fiind nevoit sa trimita o cerere altui server
- pe masinile UNIX, daemonul care ofera servicii DNS se numeste *named*, care face parte din pachetul BIND (*Berkeley Internet Name Domain*)
- serverul BIND se configureaza prin fisierul de configurare `/etc/named.conf` si al fisierelor de definire a zonelor, localizate in `/var/named`

Sistemul BIND – fisierul *named.conf*

- fisierul *named.conf* este alcatuit din mai multe declaratii
- sintaxa declaratiilor este:

```
// comentarii  
cuvant_cheie {  
    ...  
    ... (campuri)  
};
```

- declaratiile pot contine si sub-declaratii
- declaratii:

logging – optiunile privind jurnalizarea

options – optiuni ale serviciului named:

directory – directorul de lucru (contine fisiere de configurare)

forwarders – lista de adrese IP a serverelor DNS catre care vor fi redirectionate cererile (de exemplu, ale ISP-ului)

Sistemul BIND – fisierul *named.conf*

allow-query – specifica masinile carora li se permite efectuarea de cereri DNS; lista este alcatuita din mai multe elemente, separate cu “;”

allow-recursion – masinile carora li se permite sa efectueze cereri recursive

allow-transfer – masinile carora li se permite transferuri de zona

zone – specifica o zona (domeniu); exista cinci tipuri de zone:

- master – serverul detine originalul informatiilor despre zona si furnizeaza raspunsuri autoritare

- slave – detine o copie a zonei; este obligatorie utilizarea directivei *masters*, care specifica adresele masinilor pe care serverul le va contacta pentru a-si actualiza informatiile despre zona

Sistemul BIND – fisierul *named.conf*

- stub – similară cu *slave*, dar se copiază doar înregistrările NS
- forward – utilizată pentru redirectionarea cererilor către alte servere
- hint – folosită atunci când serverul de nume este în regim de *cache*

- exemplu:

```
options {  
    directory “/var/named”;  
    allow-recursion { 10.0.0./0; };  
};
```

Sistemul BIND – fișierul *named.conf*

```
// configuratia pentru server caching-only
```

```
zone "." {  
    type hint;  
    file "named.root";  
};
```

```
// zona infoiasi.ro
```

```
zone "nemesis.ro" {  
    type master;  
    file "nemesis.ro";  
};
```

Sistemul BIND – fișierele de definire a zonelor

- fiecare fișier de definire a unei zone are asociat un domeniu, numit *origine*
- sub-domeniile și numele de masina pot fi specificate relativ la origine
- un nume este considerat absolut dacă se termină cu un punct, altfel este relativ la origine
- originea poate fi referită prin caracterul “@”
- informațiile conținute de un fișier de definire a zonelor sunt structurate în înregistrări de resursă (RR), având formatul:
 [*domeniu*] [*tll*] [*clasa*] *tip data*
- *domeniu* – numele domeniului la care se referă înregistrarea; dacă nu este specificat, este considerat ca fiind cel din înregistrarea precedentă
- *tll* – timpul de expirare a înregistrării, denumit TTL (*Time To Live*) și exprimat în secunde
- *clasa* – clasa de adrese; trebuie să fie IN (*IN*ternet)

Sistemul BIND – fisierele de definire a zonelor

- *tip* – tipul inregistrarii (A, SOA, PTR sau NS)
- *data* – informatiile asociate inregistrarii; formatul acestui camp depinde de tipul inregistrarii
- tipul inregistrarii poate fi:
 - SOA – descrie o zona de autoritate (*Start Of Authority*):
 - origine – numele absolut al masinii care este server DNS primar
 - contact – adresa e-mail a administratorului domeniului
 - serial – un numar care reprezinta versiunea fisierului de descriere a zonei; trebuie incrementat atunci cand sunt modificate informatii
 - interval_actualizare – intervalul de timp la care se face verificarea zonei de catre serverele secundare (in secunde)
 - interval_reincercare – intervalul de timp la care se reincearca verificarea zonei de catre serverele secundare, in caz de eroare

Sistemul BIND – fișierele de definire a zonelor

- timp_expirare – timpul după care serverele secundare trebuie să renunțe la informațiile despre zonă, dacă nu au reușit contactarea serverului primar
- minim – valoarea TTL implicată pentru înregistrările care nu o specifică
- A – asociază o adresă IP cu un nume de mașină (*Address*); pentru fiecare nume de mașină trebuie să existe doar o înregistrare de tip A
- NS – specifică serverul primar și cele secundare ale zonei (*Name Server*)
- CNAME – asociază un pseudonim numelui autorizat al unei mașini (*Canonical Name*)
- PTR – utilizat pentru asocierea inversă (reverse mapping) a adreselor IP cu nume de mașină (*Pointer*)
- MX – stabilește un agent de transport al poștei electronice (*Mail eXchanger*)

Sistemul BIND – fisierele de definire a zonelor

Exemplu:

```
$TTL 1D
```

```
@          IN SOA   infoiasi.ro. root.infoiasi.ro. (  
          2004083001      ; numarul serial  
          1D              ; interval actualizare  
          2H              ; interval reincercare  
          1W              ; timp expirare  
          1D )            ; minim  
          IN NS   ns.infoiasi.ro.  
          IN MX   10      mail.infoiasi.ro  
infoiasi.ro. IN A   193.231.30.131  
thor         IN A   193.231.30.131  
www         IN A   193.231.30.131  
fenrir      IN A   193.231.30.197
```