

Domēna vārdu serveris (DVS) lokālajam datortīklam uz BIND 9 bāzes

Dokumenta oriģināls: <http://ru-board.com/new/article.php?sid=161>

Šis dokuments apraksta sākotnējo programmas BIND uzstādīšanas un konfigurēšanas procesu, lai izveidotu to par domēna vārdu buferserveri lokālā datortīkla vajadzībām. BIND 9 uztur piekļuves tiesību pārvaldes, zonu pārraides un dinamisku jauninājumu sarakstus. Pie tam, šīs versijas programma uztur dinamisko jauninājumu un zonu izmaiņu paziņojumu standartu; tā izmanto speciālu zonu pārraides veidu, kas sekundāriem DVS ļauj pieprasīt zonas primārajiem DVS tikai datu izmaiņu gadījumā. Tas ļauj paātrināt zonu pārraides procesu.

Kā operētājsistēma izmantota Slackware Linux 10.1.

BIND uzstādīšana

Raksta tapšanas laikā pēdējā stabilā BIND 9 versija bija 9.3.0. Instalācijas fails atrodams adresē: <ftp://ftp.linux.ee/pub/slackware/slackware-10.1/slackware/n/bind-9.3.0-i486-3.tgz>

Ar root tiesībām veicam sekojošas darbības:

1. `# cd /usr/local/src`

2. Lejupielādējam programmas instalāciju no FTP servera ftp.linux.ee:

```
# wget -v --passive-ftp ftp://ftp.linux.ee/pub/slackware/slackware-10.1/slackware/n/bind-9.3.0-i486-3.tgz
```

3. Uzstādām ielādēto programmu:

```
# installpkg bind-9.3.0-i486-3.tgz
```

Sākotnējā BIND 9 konfigurēšana un startēšana

Slackware Linux 10.1 konfigurācijas faili atrodas katalogā `/etc`. Esiet uzmanīgi, veicot tajos izmaiņas, bet īpaši uzmanieties, ja rakstiet tos "no nulles". Vispirms mums jātiek galā ar galveno BIND 9 konfigurācijas failu `named.conf`. Tā saturs pēc konfigurēšanas būs apmēram šāds:

```
# cat /etc/named.conf
```

```
// Pirmajā rindā nosakām tīklu (-us), no kuriem būs atļauts sūtīt pieprasījumus
```

```
// caur mūsu DVS:
```

```
acl "musu_tikls" { 192.168.5.0/24; 127.0.0.1; };
```

```
options {
```

```
// Darba katalogs:
```

```
directory "/var/named";
```

```
// Atļaujam sūtīt pieprasījumus tikai no tiem tīkliem, kurus mēs norādījām:
```

```
allow-query { "musu_tikls"; };
```

```
};
```

```
zone "." IN {
```

```
type hint;
```

```
file "/etc/named.root";
```

```
};
```

```
zone "0.0.127.in-addr.arpa" IN {
```

```
type master;
```

```
file "/etc/localhost.rev";
```

```
notify no; };
```

Tagad jāizveido faili, uz kuriem atsaucamies failā `named.conf`. `named.root` un `localhost.rev`.

Lejupielādējam failu `named.root`:

```
# wget -v --passive-ftp ftp://ftp.internic.net/domain/named.root -P /etc
```

Vēlams regulāri šo procedūru atkārtot vai arī izveidot automātisku jaunināšanu ar programmas `cron` palīdzību. Failu `localhost.rev` var rakstīt ar roku. Tā saturs ir apmēram šāds:

```
# cat /etc/localhost.rev
$TTL 3600
@ IN SOA serveris.domens.lv. (
20040603 ; Serial
3600 ; Refresh
900 ; Retry
3600000 ; Expire
3600 ) ; Minimum
IN NS serveris.domens.lv.
1 IN PTR localhost.domens.lv.
```

Tagad vajadzētu startēt un pārbaudīt mūsu bind:

```
# chmod 755 /etc/rc.d/rc.bind
# /etc/rc.d/rc.bind start
# ps ax | grep bind
```

Ieraudzīsim apmēram sekojošo:

```
29232 pts/1 S+ 0:00 grep bind
```

Mēģināsim nosūtīt pieprasījumu caur mūsu DVS:

```
# dig @127.0.0.1 slackers.lv
```

Atbildei mēs saņemsim apmēram sekojošo:

```
; <<> DiG 9.3.1 <<> @127.0.0.1 slackers.lv
; (1 server found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59323
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; QUESTION SECTION:
;slackers.lv. IN A
;; ANSWER SECTION:
slackers.lv. 86400 IN A 213.21.215.139
;; AUTHORITY SECTION:
slackers.lv. 3600 IN NS ns.datateks.lv.
;; ADDITIONAL SECTION:
ns.datateks.lv. 86319 IN A 213.21.215.139
;; Query time: 38 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Jul 20 19:46:03 2005
;; MSG SIZE rcvd: 87
```

Ja atbildes nav, jāskatās fails /var/log/messages, un jālasa, ko mūsu BIND raksta un mēģinām saprast, ar ko tas ir saistīts :). Jāatgādina, ka attiecīgi jānokonfigurē arī ugunssiena, lai tīkla klienti varētu izmantot mūsu DVS:

```
# iptables -A INPUT -p tcp -s 192.168.5.0/24 -dport 53 -j ACCEPT
# iptables -A INPUT -p udp -s 192.168.5.0/24 -dport 53 -j ACCEPT
```

Ja saņemta pozitīva atbilde, tad mūsu DVS darbojas un var apkalpot mūsu datortīklu :) Tagad mūsu dators ir jānokonfigurē darbam ar mūsu DVS. Labojam failu /etc/resolv.conf. Tagad failam jāizskatās sekojoši:

```
# cat /etc/resolv.conf
# mūsu domens
domain slackers.lv
# IP adrese vai nu 127.0.0.1, vai datora adrese
nameserver 127.0.0.1
```

Pārbaudām, vai mūsu dators griežas pie uzstādītā DVS:

```
# nslookup slackers.lv
Server: 127.0.0.1
Address: 127.0.0.1#53
Non-authoritative answer:
Name: slackers.lv
Address: 213.21.215.139
```

Ja saņemta apmēram šāda atbilde, tas nozīmē, ka DVS darbojas. Lai samazinātu

mūsu DVS trafiku, tam var norādīt mūsu interneta pakalpojumu sniedzēja (IPS) DVS adresi. Šai gadījumā pieprasījuma laikā mūsu DVS vispirms griezīsies pie IPS DVS bufera. Lai to panāktu, DVS konfigurācijas failam */etc/named.conf* jāpievieno parametrs *forwarders*.

Sekcijai *options* pievienojam rindu:

```
forwarders { x.x.x.x; };
```

Neaizmirstiet x vietā ierakstīt jūsu IPS DVS adresi. Pēc izmaiņu veikšanas dodam komandu:

```
# /etc/rc.d/rc.bind restart
```

Šajā dokumentā netiek apskatīti DVS drošības līmeņa paaugstināšanas jautājumi.

Tulkoja un pielāgoja:
swami@slackers.lv