

Dinamički DNS pomoću naredbe nsupdate



Ako ste imali potrebu pristupati izvana svom računalu kod kuće, tada znate da to zbog promjenljive IP adrese nije jednostavno. U tu svrhu koristimo dinamičke DNS servise. Oni mapiraju stalno ime računala iz svojih domena na promjenjive IP adrese koje vam daje vaš pružatelj usluga. Kućni DSL routeri čak imaju mogućnost rada s nekim od takvih servisa, što nam olakšava posao.

No, stvari se na mreži brzo mijenjaju, pa je tako popularni DynDNS je od 8. svibnja 2014. ukinuo besplatni pristup svom servisu. Drugi takav servis, no-ip.com, traži potvrdu svakih mjesec dana i ne nudi nikakvu podršku za korisnike besplatne usluge. U svakom slučaju i on može uskoro početi naplaćivati uslugu.

Kolege čitatelji portala obično imaju pod kontrolom (svoj) vlastiti DNS server, pa se postavlja pitanje da li je moguće upotrijebiti "svoj" server da bi osigurali stalnu adresu za kućna računala? Mogućeje, i to uz pomoć naredbe *nsupdate*.

Dinamički DNS ste sigurno upoznali prvi puta kada su Windows klijenti pokušavali prijaviti svoje adrese vašem DNS serveru na Linuxu. Sada možete isti sustav upotrijebiti da omogućite sebi i svojim korisnicima pristup računalima kod kuće. Za to moraju biti ispunjeni određeni uvjeti.

Mi ćemo se u ovom članku ograničiti na Linux računala i servere, ali isti alati postoje i za Windowse, a vjerojatno je moguće koristiti i neke nativne Windows mehanizme.

KLIJENT

Na klijentu treba instalirati paket *dnsutils*, koji sadržava program *dnssec-keygen*. Nije potrebno instalirati potpuni BIND9 paket, čak nije potrebno imati pokrenut *daemon* "named".

Najprije moramo generirati ključeve, i to ovako:

```
# dnssec-keygen -a HMAC-MD5 -b 512 -n USER at.home.domena.hr.  
-a algorithm  
-b keysize (izme?u 512 i 1024)  
-n nametype (ZONE, USER, HOST)
```

Za poddomenu *at.home.domena.hr* vrijediti će sljedeće:

```
domena.hr      - vaša domena  
home.         - poddomena koju ?emo koristiti za ku?ne korisnike  
at.           - jedan od zapisa korisnika u poddomeni home
```

U tom direktoriju pojavit će se dvije datoteke, jedna s privatnim, druga s javnim ključem. Generirane datoteke imaju prilično čudna imena, a ključ treba prekopirati na vaš udaljeni DNS server:

```
# ls Kat.home*  
Kat.home.domena.hr.+157+26848.key
```

```
Kat.home.domena.hr.+157+26848.private
```

```
# cat Kat.home.domena.hr.+157+26848.key
at.home.domena.hr. IN KEY 0 3 157 kHLKjliz...a58z5S9ORdCLterN3UZUY9JjfPgZzSepA==
```

Ključ je dugački niz znakova (mi smo ga ovdje skratili). Ove dvije datoteke držite zajedno u istom direktoriju gdje pokrećete naredbu *nsupdate*.

SERVER

Na serveru, u direktoriju `/etc/bind/`, kreirajte datoteku **keys.conf** i uključite je s *include* unutar datoteke `/etc/bind/named.conf.local`:

```
include "/etc/bind/keys.conf";
```

Datoteka `keys.conf` izgleda ovako:

```
key at.home.domena.hr. {
  algorithm HMAC-MD5;
  secret "kHLKjliz...a58z5S9ORdCLterN3UZUY9JjfPgZzSepA== ";
};
```

Važno: Obratite pažnju na točku iza "hr", obvezna je!

Nakon toga treba kreirati novu zonu. Odlučili smo koristiti zonu "home" jer u slučaju greške vaše ostale zone neće biti "oštećene". Zonu smo dodali kao poddomenu (home.) već postojećoj domeni na vašoj instituciji (domena.hr).

Unutar datoteke `/etc/bind/named.conf.local` dodajete zapis za novu zonu:

```
zone "home.domena.hr" {
  type master;
  file "/etc/bind/home.domena.hr.db";
  allow-update {
    key at.home.domena.hr.; // ovdje ?e te dodavati ?iji sve 'key
' smije raditi update.
  };
};
```

Naravno, umjesto kreiranja nove zone, možete direktivu "allow-update" upisati u postojeću zonu i dodati samo jedan adresni (A) zapis (*record*) za vlastito kućno računalo.

Zatim, treba napraviti datoteku `/etc/bind/home.domena.hr.db`, koju možete iskopirati iz neke postojeće, pa je preoblikovati da odgovara novoj zoni i domeni:

```
-----/etc/bind/home.domena.hr.db-----
$TTL 3600 ; 1 sat
@ IN SOA dns.domena.hr. root.domena.hr. (
      2014121501 ; serial
      1800 ; refresh (30 minutes)
      600 ; retry (10 minutes)
      604800 ; expire (1 week)
      3600 ; minimum (1 hour)
```

)

```
NS      dns.domena.hr.      ; dns.domena.hr je FQDN zapis naseg DNS servera
-----/etc/bind/home.domena.hr.db-----
```

Kako bi *named daemon* mogao pisati *journal* datoteku (koja se pojavljuje s nastavkom **.jnl**, te služi sličnoj svrsi kao i *journaling* na ext3 datotečnom sustavu), potrebno je *daemonu* omogućiti pisanje unutar */etc/bind*:

```
# chmod 2755 /etc/bind
# chown root:bind /etc/bind
# ls -ld /etc/bind
drwxrwsr-x 12 root bind 4096 May 16 00:06 /etc/bind
```

Možda bi bilo bolje jednostavno zonsku datoteku i *journal* staviti unutar */var/lib/bind* ili */var/cache/bind*, ali na internetu se nalaze svakakve upute, koje ne moraju odgovarati Debianovim standardima. Sami odlučite što vam je jednostavnije, a ukoliko se pojave neke greške u logovima, gotovo sigurno je to zbog toga što *daemon* ne može pisati i brisati *journal* unutar zadanog direktorija.

Što je još potrebno napraviti? Prvo, *reload* dns servisa na serveru:

```
# rndc reload
```

ili

```
# /etc/init.d/bind9 reload
```

ili

```
# service bind9 reload
```

Pregledajte logove u potrazi za greškama, koje su kod DNS-a uvijek moguće. Jedna točka manje ili više vašu konfiguraciju čini neispravnom. Ali ne brinite, jer kako smo naveli, to će se odnositi samo na vašu novu zonu.

Nakon toga na klijentu pokrenemo naredbu *nsupdate*:

```
# nsupdate -v -k Kat.home.domena.hr.+157+26848.private /tmp/nsupdate
-k putanja do ključa
-v komunikacija ide TCP-om a ne UDP-om
```

Naredba je prilično jasna, definira koji ćemo privatni ključ koristiti, datoteku koja sadrži naredbe za udaljeni DNS server. Za izradu ove datoteke upotrijebit ćemo skriptu koju pokrećemo iz *crona*. Ovu skriptu možete snimiti u neki svoj direktorij gdje i inače smještate slične stvari (*/root/bin?* */usr/local/sbin?* Nama je svejedno). Skriptu za dinamički update ćemo napraviti u direktoriju */tmp* (iako može i negdje drugdje). Primjer cron skripte izgleda ovako:

```
#!/bin/bash
IP=$(wget -q -O - checkip.dyndns.org|sed -e 's/.*Current IP Address: //' -e 's/<.*$//')
SERVER="vas.dns.server.hr"
```

```
ZONA=home.domena.hr.  
LOC=/etc/bind  
cat > /tmp/nsupdate <<END  
server $SERVER  
debug yes  
zone $ZONA  
update delete $ZONA  
update add $ZONA 600 A $IP  
send  
END  
cd $LOC && nsupdate -v -k Kat.home.domena.hr.+157+26848.private /tmp/nsupdate 2>&1
```

Skriptu treba staviti u cron da se izvršava svakih 10 minuta ili koliko mislite da vam je dovoljno (provideri mijenjaju adresu najčešće svaka 24 sata). Naravno, uvijek možete ručno pokrenuti skriptu ukoliko se adresa promijenila.

Dodatne izmene je moguće izvesti, poput modifikacije da se se nsupdate pokrene odmah po dobivanju adrese preko DHCP-a ili pokretanja PPP ili PPTP veze. No, mislimo da je već i standardni cron sasvim dovoljan za ovu svrhu. Pripazite samo da korisnik pod kojim ćete izvršavati ovaj cronjob može čitati datoteku *.private (generirani ključ sa početka priče). Ako treba, primijenite chown/chmod.

Ukoliko ne proradi, povećajte razinu debuga s naredbom **#rndc trace 10**, te provjerite jesu li datoteke u istom direktoriju i čitljive trenutnom korisniku (korisnik ne mora biti root da bi mogao osvjježavati zone).

Ukoliko je sve u redu, u logovima na serveru vidjet ćete ovakve zapise:

```
Dec 16 15:46:10 server named[18538]: client A.B.C.D#56281: signer "at.home.domena.hr"  
approved  
Dec 16 15:46:10 server named[18538]: client A.B.C.D#56281: updating zone 'home.domena  
.hr/IN': delete all rrsets from name 'home.domena.hr'  
Dec 16 15:46:10 server named[18538]: client A.B.C.D#56281: updating zone 'home.domena  
.hr/IN': adding an RR at 'home.domena.hr' A  
Dec 16 15:46:10 server named[18538]: zone home.domena.hr/IN: sending notifies (serial  
2014051903)
```

Naravno, kao i kod navedenih komercijalnih dinamičkih DNS servisa, nemojte zaboraviti konfigurirati svoj DSL ili kablanski modem. Postavite *Port Forwarding* ili rezervirajte točnu adresu vašeg kućnog računala i postavite je u DMZ, jer ćete u protivnom umjesto računala dobiti web sučelje modema.

pet, 2014-12-19 13:54 - Domagoj Vuković **Kuharice:** [Linux](#) [1]

Kategorije: [Servisi](#) [2]

Vote: 5

Vaša ocjena: Nema Average: 5 (2 votes)

Source URL: <https://sysportal.carnet.hr/node/1480>

Links

- [1] <https://sysportal.carnet.hr/taxonomy/term/17>
- [2] <https://sysportal.carnet.hr/taxonomy/term/28>