

BIND: rndc greške



Na CARNetovim poslužiteljima funkciju DNS servisa već dugi niz godina obavlja Bind, najpopularniji softver za DNS. Iako se neki ne bi složili da je Bind alfa i omega DNS-a, svoj posao obavlja tiho i neprimjetno. Uz povremena dodavanja novih hostova, ni ne traži neku veliku pozornost. Možda baš zbog toga postoje mnogi loše konfigurirani poslužitelji na mreži, kako kod nas tako i na ostatku Interneta. No, sad nećemo pričati o njima. Skrenut ćemo vam pozornost na grešku koja se zna pojaviti kod nadogradnji, bilo cijelog poslužitelja bilo Bind-a. Greška obično spominje "rndc" (skraćeno od "Remote name daemon control"), alat za kontrolu Bind DNS poslužitelja (za više informacija pogledajte man stranicu).

Puna poruka greške je sljedeća (javlja se nakon pokušaja pokretanja ili gašenja named daemona):

```
# /etc/init.d/bind9 start
Stopping domain name service: namedrndc: connection to remote host closed
This may indicate that the remote server is using an older version of the
command protocol, this host is not authorized to connect, or the key is
invalid.
```

Greška se može manifestirati i u ovom obliku:

```
rndc: connect failed: 127.0.0.1#953: connection refused
```

U logovima (obično /var/log/daemon.log) se mogu vidjeti ovakve poruke:

```
none:0: open: etc/bind/rndc.key: permission denied
couldn't add command channel 127.0.0.1#953: permission denied.
```

Problem je u nedostatku rndc.key datoteke, nepravilno postavljenim pravima nad njom ili konfiguraciji zaostaloj od prethodnih verzija. Ukoliko nedostaje /etc/bind/rndc.key datoteka, prvo učinite sljedeće:

```
# rndc-confgen -a
```

Datoteka i njeni atributi trebaju biti postavljeni ovako:

```
# ls -l /etc/bind/ | grep rndc
```

```
-rw-r----- 1 root bind 77 Dec 12 2003 rndc.key
```

Ukoliko rndc.key postoji, a u named.conf postoji unos sličan ovom, obrišite ga:

```
key rndc-key {
```

```
algorithm hmac-md5;
secret "xxxxxxxxxxxxxxxxxxxxxxxxxxxxx==";
};

controls {
  inet * port 953 allow { any; } keys { rndc-key; };
};
```

Obrišite `/etc/bind/rndc.conf` i `/etc/rndc.conf` ako postoje. Ovo će prisiliti `rndc` i `named` da se vrate na default ponašanje, a to je upravo uporaba datoteke `rndc.key`. Naravno, prije brisanja valja napraviti zaštitnu kopiju svih datoteka koje se mijenjaju.

Problem je u tome što `rndc` i `named` mogu rabiti različite ključeve, što brisanjem konfiguracije svodimo na korištenje default vrijednosti i jedinstvenog ključa.

Drugi razlog je nemogućnost čitanja datoteke sa ključem `rndc.key`, što sprječava `rndc` u obavljanju svojih dužnosti. To što `rndc` pokrećete kao `root` nema nikakvih prednosti, jer se odmah po pokretanju programa privilegije spuštaju na razinu korisnika `"bind"`.

KEYWORDS: `rndc` BIND `bind9` `named`

- [Logirajte](#) [1] se za dodavanje komentara

uto, 2008-06-17 14:57 - Željko Boroš **Vijesti:** [Linux](#) [2]

Kuharice: [Za sisteme](#) [3]

Kategorije: [Servisi](#) [4]

Vote: 0

No votes yet

Source URL: <https://sysportal.carnet.hr./node/398>

Links

[1] <https://sysportal.carnet.hr./sysportallogin>

[2] <https://sysportal.carnet.hr./taxonomy/term/11>

[3] <https://sysportal.carnet.hr./taxonomy/term/22>

[4] <https://sysportal.carnet.hr./taxonomy/term/28>