Table Of Contents

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

Home > Faq > Bind dns

axfr-get: fatal: unable to parse AXFR results: protocol error and Solution
Posted by Vivek Gite <vivek@nixcraft.com>

I'm trying to get data (AXFR query) from master tinydns server to secondary DNS server using tcpclient as follows:
tcpclient -v a.ns.example.com 53 axfr-get example.com example.com example.com.tmp

But I'm getting an error which read as follows:

> **>axfr-get: fatal: unable to parse AXFR results: protocol error**

How do I fix this problem?

Try the following to get rid of this problem:

DJBDNS [1]

Make Sure axfrdns Configured and Running

axfrdns is a DNS zone-transfer server supplied with djbdns. It reads a zone-transfer request in DNS-over-TCP format from its standard input, and responds with locally configured information. Use netstat command [2] or sockstat command to see current port status:

```
# netstat -tulpn | grep :53
```

OR

```
# sockstat -4 -p 53
```

Make Sure TCP port 53 is Open For Business

Make sure firewall is not blocking tcp port # 53. Use iptables command to list current firewall rules:

```
# iptables -L -n
# iptables -L -n | less
# iptables -L -n | grep 53
```

PF firewall rules can be listed using the following command:

```
# pfctl -sr
# pfctl -sr | grep "port = domain"
```

How Do I Open TCP Port # 53 under Linux Iptables Firewall?

Update your script as follows (assuming that 202.54.1.1 is tinydns / axfrdns server address):

```
$IPT -A INPUT -i eth0 -s 0/0 -d 202.54.1.1 -p udp --dport 53 -j ACCEPT
$IPT -A INPUT -i eth0 -s 0/0 -d 202.54.1.1 -p tcp --dport 53 -j ACCEPT
```

How Do I Open TCP Port # 53 under *BSD PF Firewall?

Update your /etc/pf.conf as follows (assuming that 202.54.1.1 is tinydns / axfrdns server address):

```
pass in on $ext_if inet proto udp from any to 202.54.1.1 port domain
pass in on $ext_if inet proto tcp from any to 202.54.1.1  port domain flags S/SA synproxy s
```

◄   III   ►

Make Sure TCPRULES are Set Correctly For axfrdns

tcp file defines rules for AXFR. The following will allow only AXFR to ns2.example.com but not to the rest of the world (tcp file is located at /etc/axfardns or /var/axfardns directory):

```
ns2.example.com:allow,AXFR="example.com"
:allow,AXFR=""
```

Save and close the file. Run make to update changes:

```
# make
```

Only ns2.example.com is allowed to transfer zone, others can only connect to TCP port 53.

Troubleshooting Tip: Dig and tcpclient Command

Try tcpclient command as follows:

```
$ tcpclient -v ns1.example.com 53 axfr-get example.com fn fn.tmp
```

Try passing client IP to ns1.example.com (this is required if you've multiple IP address):

```
$ tcpclient -i ns2.example.com -v ns1.example.com 53 axfr-get oxdba.net fn fn.tmp
```

Try dig command as follows:

```
$ dig @ns1.example.com example.com A +tcp
$ dig @ns1.example.com example.com AXFR +tcp
```

4000+ howtos and counting! Want to read more Linux / UNIX howtos, tips and tricks? Subscribe to our daily email newsletter or weekly newsletter to make sure you don't miss a single tip/tricks. Alternatively, subscribe via RSS/XML feed.

Article printed from Frequently Asked Questions About Linux / UNIX: **http://www.cyberciti.biz/faq/**

URL to article: **http://www.cyberciti.biz/faq/axfr-get-fatal-unable-to-parse-axfr-results-protocol-error/**

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/category/djbdns/**
[2] netstat command: **http://www.cyberciti.biz/faq/find-out-which-service-listening-specific-port/**