

BLOG O’ MATTY



HOME

BLOG HOME

ARTICLES

CODE

PRESENTATIONS

One way to avoid tcpdump “packets dropped by kernel” messages

I have been knee deep this week debugging a rather complex DNS issue. I’ll do a full write up on that next week. While I was debugging the issue I needed to fire up tcpdump to watch the DNS queries from one of my authoritative servers to various servers on the Internet. What I noticed when I fed the data into Wireshark were periods of time with no data, and I wasn’t quite sure why at first.

Based on what I could find on the tcpdump / BPF sites when tcpdump is busy processing existing data and is not able to take packets captured by BPF out of the queue fast enough, the kernel will drop them. If this occurs you will see the tcpdump message “packets dropped by kernel” become non-zero:

```
$ tcpdump -w dns-capture.cap -s 1520 -ttt -vvv -i bond0 port 53
```

```
.....
9559 packets captured
12533 packets received by filter
2974 packets dropped by kernel
```

I started to do some digging to see why tcpdump couldn’t keep up, and after a bit of profiling I noticed that the program was spending an excessive amount of time resolving IPs to names. This processing was stalling the program from reading more data from the queue, and resulted in packets being dropped. Once I ran tcpdump with the “-n” (do not resolve IPs to names) option I no longer experienced this issue:

```
$ tcpdump -w dns-capture.cap -s 1520 -ttt -vvv -n -i bond0 port 53
```

```
.....
9339 packets captured
9339 packets received by filter
0 packets dropped by kernel
```

This stopped gaps from occurring in my Wireshark display, and since Wireshark can resolve IPs to names all was well. It’s really crazy how you can start debugging one issue and wind up debugging 3 – 4 more prior to solving the original problem. Debugging issues is definitely fun, and I guess it gives me plenty to write about. :) This past week I’ve learned more about the DNS protocol and the various implementations than I have in the past 10 years. It’s amazing how many cool nuggets of information are buried in the various DNS RFCs!

Related Posts

- [Configuring a caching only DNS server on Solaris hosts](#)
- [Converting from nslookup to dig](#)
- [Limiting how much memory BIND can use](#)
- [Logfile format for BIND queries](#)
- [Measuring DNS latency with nsping](#)
- [Monitoring DNS servers](#)

matty on June 9, 2011 | Filed Under [Linux Debugging](#)

One Comment



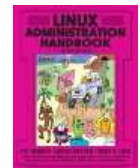
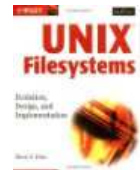
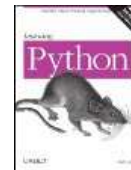
Jim on June 12th, 2011

“It’s really crazy how you can start debugging one issue and wind up debugging 3 – 4 more prior to solving the original problem.”

A particularly hairy yak...

Leave a Comment

Recommended Books



Search

Search for:

Blogroll

Adam Leventhal
Ben Rockwood
Brendan Gregg
Chris Siebenmann
Derek Crudgington
Gerardo López-Fernández
OpenBSD Journal
Planet CentOS
Planet Solaris
Planet SysAdmin
Scott Cromar
Scott Dickson

Categories

AIX Debugging (1)
AIX Package Management (2)
Apache (29)
Apple (27)
Articles, Presentations and Certifications (43)

Username (required) :

Email (required) :

Web Site :

Comment :

Submit

- Book Reviews (1)
- Brocade (8)
- cfengine (5)
- Debian Linux (1)
- Djbdns (1)
- DNS & BIND (15)
- Emulex (3)
- Firefox (3)
- Food and Beverages (1)
- FreeBSD Misc (2)
- FreeBSD Networking (1)
- FreeBSD Utilities (2)
- FreeNAS (1)
- Gadgets (2)
- Games (1)
- Gardening (1)
- Gnome (4)
- GNU Privacy Guard (4)
- Hardware (13)
- Health Foods (2)
- Home Security (1)
- HTTP (4)
- Illumos (1)
- Investing (2)
- ISC DHCP (3)
- Java (12)
- Libvirt (1)
- Links (15)
- Linux Authentication (1)
- Linux Debugging (14)
- Linux Gluster (8)
- Linux Installation (4)
- Linux iSCSI (2)
- Linux Kernel (18)
- Linux Kickstart (2)
- Linux KVM (10)
- Linux LVM (3)
- Linux LXC Containers (1)
- Linux Misc (11)
- Linux Networking (24)
- Linux NFS (4)
- Linux Package Management (26)
- Linux performance (5)
- Linux Recovery (4)
- Linux Resource Controls (1)
- Linux Security (19)
- Linux SELinux (2)
- Linux Spacewalk (1)
- Linux Storage (41)
- Linux Utilities (112)
- Linux Virtualization (2)
- Linux X Windows (3)
- Logging (1)
- Microsoft DNS (1)
- Monitoring (5)

Music (40)
MySQL (8)
net-snmp (4)
Networking (4)
NFSv3 (5)
OpenBSD Kernel (7)
OpenBSD Misc (1)
OpenBSD Networking (2)
OpenBSD Ports (3)
OpenBSD Security (7)
OpenBSD Utilities (7)
OpenFiler (1)
OpenLDAP (4)
OpenSSH (15)
OpenSSL (8)
Oracle (3)
OS X (2)
Perl (11)
pets (1)
PHP (1)
Postfix (2)
Procmail (1)
Puppet (2)
Python (7)
QLogic (1)
Rants (27)
Ruby (1)
Samba (2)
Secure Shell (2)
Security (9)
Sendmail (3)
Service providers (9)
Shell (10)
Smart Phones (2)
Smartmontools (7)
Snort (1)
Software (18)
Solaris Cluster (7)
Solaris Debugging (19)
Solaris DTrace (33)
Solaris Fault Management (7)
Solaris Install (3)
Solaris Kernel (7)
Solaris KVM (1)
Solaris Linker (6)
Solaris Live Upgrade (2)
Solaris Misc (22)
Solaris Networking (27)
Solaris NFS (4)
Solaris Package Management (1)
Solaris Patching (20)
Solaris Performance Tuning (2)
Solaris Recovery (2)
Solaris Resource Management (2)

Solaris Security (13)
Solaris Shell (1)
Solaris SMF (9)
Solaris Storage (41)
Solaris Utilities (67)
Solaris Volume Manager (7)
Solaris Xen (3)
Solaris ZFS (32)
Solaris Zones (18)
Storage (2)
Storage Area Networking (9)
Sun Directory Server (3)
Sun Servers (3)
Sun Web Server (1)
Syslog (2)
syslog-ng (2)
Truecrypt (1)
Uncategorized (33)
UNIX (3)
UNIX Shell (33)
Veritas Cluster Server (1)
Veritas File System (6)
Veritas Netbackup (3)
Veritas Volume Manager (19)
VirtualBox (1)
VMWare ESX Server (13)
Web development (4)
Web Utilities (1)
Windows Server (4)
Wireless (2)
Wordpress (7)

Archives

December 2012 (1)
August 2012 (3)
July 2012 (7)
June 2012 (1)
May 2012 (1)
February 2012 (14)
January 2012 (15)
December 2011 (1)
November 2011 (25)
October 2011 (10)
September 2011 (3)
August 2011 (5)
July 2011 (6)
June 2011 (3)
May 2011 (5)
April 2011 (4)
March 2011 (8)
February 2011 (3)
January 2011 (9)
December 2010 (5)
November 2010 (7)
October 2010 (6)

September 2010 (3)
August 2010 (5)
July 2010 (14)
June 2010 (4)
May 2010 (7)
April 2010 (6)
March 2010 (8)
February 2010 (2)
January 2010 (5)
December 2009 (13)
November 2009 (11)
October 2009 (7)
September 2009 (10)
August 2009 (17)
July 2009 (28)
June 2009 (29)
May 2009 (25)
April 2009 (34)
March 2009 (24)
February 2009 (14)
January 2009 (5)
December 2008 (7)
November 2008 (2)
October 2008 (3)
September 2008 (2)
July 2008 (7)
June 2008 (2)
May 2008 (1)
April 2008 (4)
March 2008 (5)
February 2008 (12)
January 2008 (5)
December 2007 (5)
November 2007 (15)
October 2007 (16)
September 2007 (6)
August 2007 (4)
July 2007 (8)
June 2007 (20)
May 2007 (13)
April 2007 (14)
March 2007 (13)
February 2007 (13)
January 2007 (34)
December 2006 (27)
November 2006 (24)
October 2006 (17)
September 2006 (23)
August 2006 (18)
July 2006 (31)
June 2006 (23)
May 2006 (19)
April 2006 (30)
March 2006 (25)
February 2006 (28)

January 2006 (25)
December 2005 (23)
November 2005 (30)
October 2005 (54)
September 2005 (49)
August 2005 (10)
July 2005 (7)
June 2005 (5)
May 2005 (10)
April 2005 (6)
March 2005 (6)
February 2005 (13)
January 2005 (15)
December 2004 (3)
November 2004 (4)
October 2004 (2)

The content on prefetch.net is copyrighted to Blog O' Matty and may not be reproduced on other websites.

All information is provided AS IS, and WITHOUT ANY WARRANTY; without even the implied
warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

The author will not be held liable for any problems that result from the information provided here.

Copyright Blog O' Matty | [Privacy Policy](#) | [Corpvox WordPress Theme](#)