BLOG O’ MATTY

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

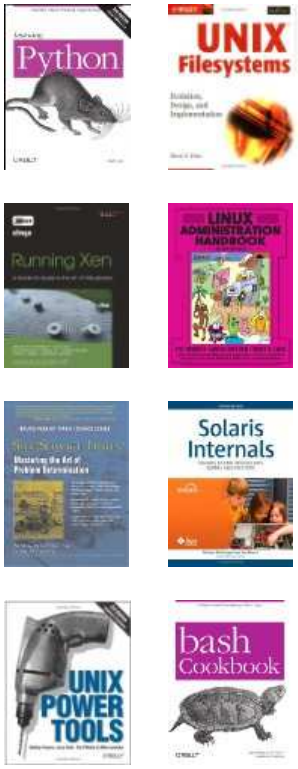
Jim on June 12th, 2011

“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:
Search

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

Archives

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)

Search