DNS and BIND: Supplement

# Notes and References

Table 4-2 lists the release dates for the major versions of BIND. Table 4-3 provides the version of BIND included in the Linux distributions under consideration.

Table 4-2. Release dates for major versions of BIND

|  |  |  |  |
| --- | --- | --- | --- |
| 9.4.0 2/2007 | 9.6.0 12/2008 | 9.8.0 3/2011 | 9.10.0 4/2014 |
| 9.5.0 7/2008 | 9.7.0 2/2010 | 9.9.0 3/2012 | 9.11.0 10/2016 |

Table 4-3. Default included version of BIND, by Linux distribuition

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| CentOS |  | 5.10 | 9.3.6-20 | 14 | 9.8.1 | Ubuntu |  |
| 7.4-1709 | 9.9.4-50 | 5.9 | 9.3.6-20 | 13 | 9.8.1 | 17.10 | 9.10.3 |
| 7.3-1611 | 9.9.4-37 | 5.8 | 9.3.6-20 | 12 | 9.7.3 | 17.04 | 9.10.3 |
| 7.2-1511 | 9.9.4-29 | 5.7 | 9.3.6-16 | 11 | 9.7.3 | 16.10 | 9.10.3 |
| 7.1-1503 | 9.9.4-18 | 5.6 | 9.3.6-6 | 10 | 9.7.1 | 16.04 | 9.10.3 |
| 7.0-1406 | 9.9.4-14 | Mint |  | OpenSuSE | | 15.10 | 9.9.5 |
| 6.8 | 9.8.2-0 | 18.3 | 9.10.3 | 42.3 | 9.11.2 | 15.04 | 9.9.5 |
| 6.7 | 9.8.2-0 | 18.2 | 9.10.3 | 42.2 | 9.9.9P1 | 14.10 | 9.9.5 |
| 6.6 | 9.8.2-0 | 18.1 | 9.10.3 | 42.1 | 9.9.6P1 | 14.04 | 9.9.5 |
| 6.5 | 9.8.2-0 | 18 | 9.10.3 | 13.2 | 9.9.5P1 | 13.10 | 9.9.3 |
| 6.4 | 9.8.2-0 | 17.3 | 9.9.5 | 13.1 | 9.9.3P2 | 13.04 | 9.9.2 |
| 6.3 | 9.8.2-0 | 17.2 | 9.9.5 | 12.3 | 9.9.2P1 | 12.10 | 9.8.1 |
| 6.2 | 9.7.3-8 | 17.1 | 9.9.5 | 12.2 | 9.9.1P2 | 12.04 | 9.8.1 |
| 6.1 | 9.7.3-2 | 17 | 9.9.5 | 12.1 | 9.8.1-4 | 11.10 | 9.7.3 |
| 6.0 | 9.7.0-5 | 16 | 9.9.3 | 11.4 | 9.7.3-1 | 11.04 | 9.7.3 |
| 5.11 | 9.3.6-20 | 15 | 9.9.2 |  |  |  |  |

Exercises

1. Build a pair of BIND DNS servers, one acting as a master, and one acting as a slave. Disable zone transfers except from the master to the slave. Modify the version string for BIND. Turn off recursion, except for a well-defined internal network.
2. Build a second pair of DNS servers, on a different namespace and a different address space. Configure these as in question 1. Add forwarder statements so that queries for information from network 1 can be answered by servers in network 2.
3. The host command is another BIND tool that can be used to lookup data from a nameserver. What information can be obtained from host? Can it be used to perform a zone transfer?
4. Run the DNS amplification attack against a local target. Estimate the amount of traffic sent out by the attacker, and the amount of traffic received by the target. Is the ratio comparable to the ratio of the packet size? Why or why not?
5. (Advanced) The contents of the cache can be dumped to a file with the command

[root@Spica data]# **rndc dumpdb**

Select the location of the dump file in named.conf by specifying a writeable location for dump-file in the options group. Dump the cache, and read it. Repeat after flushing the cache with rndc flush.

1. (Advanced) Rather than use forwarders, construct a stub zone using directives like

zone "nebula.example" in {

type stub;

masters{ 10.0.4.10; 10.0.4.11;};

file "data/stub.nebula.example";

};

Compare the two approaches.