



DNS

Matthew Dees

Simplify.



All trademarks used herein are the sole property of their respective owners.

Simplify.

Scope of Presentation

- »» Basics of DNS
- »» The BIND Nameserver
- »» cPanel's Interaction with BIND
- »» Nameserver Setup & Configuration
- »» Troubleshoot BIND & DNS

Introduction to DNS

- »» Nervous System Of The Internet
- »» Used to give all the sites on the web an address
- »» Works on a Distributed Protocol
- »» BIND Nameserver

DNS Terminology

- »» Record – An Entry inside of a Zone
- »» Zone - A series of records used for a domain
- »» Named – Internet domain server, the part of BIND that handles the hosting of DNS services
- »» BIND – Berkley Internet Name Daemon
- »» rndc – The name server control utility

Types of Records

- »» A Record – Points a Domain Name to An IP Address
- »» CNAME – Aliases a Domain Name to another Domain Name
- »» MX - Mail Exchange
- »» NS – Name Server Record
- »» PTR – Used to assign an IP address a domain name, also known as “reverse DNS”

How Nameservers Work

- Your Machine Sends Request to resolving Nameserver
- Resolving Nameserver queries root for the host's Nameserver
- Resolving Nameserver Gives you the IP of the host's Nameserver
- Your machine queries the host's Nameserver for IP of the zone you are looking for
- Will be delayed by the TTL that states how often a zone can be refreshed

cPanel & DNS

- »» Several Different Configuration Types
- »» Scalable for the needs of a host
- »» Flexible
- »» Can be set up to use dedicated Nameservers

DNS Only

- »» Synchronizes DNS Changes Between Servers
- »» Works on Access Keys
- »» Very Flexible
- »» Not able to edit zones

Stand Alone DNS

- »» Two Spare IP's on the server
- »» Best for Small Webhosts on a minimal Budget
- »» No Failover

Remote DNS Cluster

- »» Minimum of Three Servers
 - 1+ Hosting Server
 - 2 DNS Servers (preferably at different datacenters)
- »» Safest Configuration
- »» Best For Large Hosting Environment
- »» Configure Via “Cluster Control” in WHM
- »» Syncs all changes between servers, but not on the shared hosting servers.

Standalone & Remote

- »» Two Machines
 - Shared hosting
 - DNS Only
- »» Sync Everything

cPanel/BIND Interaction

Editing DNS

- »» "Edit DNS Zone" in WHM
- »» "Edit MX Entry"
- »» Zone Templates
- »» DNS Cleanup

DNS Templates

➤➤ Used to setup default zones on your server

➤➤ works using hashes (you can view these in /scripts/wwwacct)

```
%domain%. %nsttl% IN NS %nameserver%.
```

```
%nameserverentry%. IN A %nameservera%
```

```
%domain%. IN A %ip%
```

```
localhost.%domain%. IN A 127.0.0.1
```

```
%domain%. IN MX 0 %domain%.
```

```
mail IN CNAME %domain%.
```

```
www IN CNAME %domain%.
```

```
ftp IN CNAME %domain%.
```

```
support IN A 192.168.0.0.
```

BIND Basics

Simplify.

Registration & Configuration

- »» Have Two Spare IP's for the Nameservers
- »» Register Nameservers With your Domain Registrar
- »» Go to “Nameservers Setup” inside of WHM
- »» Setup Reverse DNS for the IP's you've assigned your Nameservers (this is not necessary, but part of RFC and required for PCI Compliance)

/etc/named.conf

- »» Controls your Nameserver
- »» All Options are configured here
- »» Includes from /var/named for individual zones.

rndc

- » nameserver control utility
- » This is a secure method of interacting with BIND to add, remove and reload zones
- » whenever you make a change to a zone file type “rndc reload domain.com” and your changes will be implemented
- » requires port 953 to be accessible

Recursion

- Recursion is Allowing Machines to use your server to lookup zones
- Two Methods – both set up inside of options { } in /etc/named.conf
- Required to be non-public for PCI Compliance
- Allow Recursion with ACLs
 - allow-recursion { 127.0.0.1; 192.168.1.1/24 }
- No Recursion
 - recursion no;



Zone File Header

```
$TTL 14400
@      86400      IN      SOA      ns1.cpanel.net. matt.cpanel.net.
(
      2006033101      ; serial, todays date+todays
      86400           ; refresh, seconds
      7200            ; retry, seconds
      3600000         ; expire, seconds
      86400 )         ; minimum, seconds
```

Simplify.



Zone File Records

```
cpanel.net. 86400 IN NS ns1.cpanel.net.  
cpanel.net. 86400 IN NS ns2.cpanel.net.  
cpanel.net. IN A 192.168.0.0  
localhost.cpanel.net. IN A 127.0.0.1  
cpanel.net. IN MX 0 cpanel.net.  
mail IN CNAME cpanel.net.  
www IN CNAME cpanel.net.  
ftp IN CNAME cpanel.net.
```

Simplify.

Common Issues & Troubleshooting Techniques

Simplify.

DNS Error Logging

- » Will be in `/var/log/messages`
- » Where BIND logs to can be changed in `/etc/named.conf`
- » You can watch the logs with with the command: `tail -f /var/log/messages | grep named`

DNS Troubleshooting Methods

- »» /var/log/messages
- »» Ensuring that port 53 is open
- »» Check to see that you have reverse DNS and that your nameservers are registered

DNS Troubleshooting Tools

- »» dig – Used for Pull records from nameservers
- »» nslookup – allows you to see what a host resolves to and the nameservers used to get this information
- »» host – used to get the A/PTR record of a domain name or IP
- »» ping – will always return the IP of the zone you are pinging
- »» whois – lets you see information of a domain

dig

»» Used for interrogating name servers, you can select any type of record on a domain using dig

```
matt@seminar~$ dig ns google.com
```

```
:: ANSWER SECTION:
```

```
google.com.      345344 IN      NS      ns1.google.com.  
google.com.      345344 IN      NS      ns2.google.com.  
google.com.      345344 IN      NS      ns3.google.com.  
google.com.      345344 IN      NS      ns4.google.com.
```

```
:: Query time: 125 msec  
:: SERVER: 208.67.222.222#53(208.67.222.222)  
:: WHEN: Fri May 25 16:53:14 2007  
:: MSG SIZE rcvd: 100
```

ping

- ping can be used for finding an IP on windows
- Go to Command Prompt and simply run “ping hostname”

```
C:\Documents and Settings\Matt Dees>ping google.com
```

```
Pinging google.com [64.233.167.99] with 32 bytes of data:
```

```
Reply from 64.233.167.99: bytes=32 time=55ms TTL=242
```

```
Reply from 64.233.167.99: bytes=32 time=58ms TTL=242
```

```
Reply from 64.233.167.99: bytes=32 time=58ms TTL=242
```

```
Reply from 64.233.167.99: bytes=32 time=57ms TTL=242
```

```
Ping statistics for 64.233.167.99:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:
```

```
        Minimum = 55ms, Maximum = 58ms, Average = 56ms
```

whois

- whois is a client for querying the registrar's database for information on a domain
- whois is useful for getting information on a domain such as the registrar, nameservers, expiration and domain owner contact information

`matt@seminar:~$: w hois slashdot.org`

Domain Name:SLASHDOT.ORG

Created On:05-Oct-1997 04:00:00 UTC

Last Updated On:22-Aug-2006 21:52:42 UTC

Expiration Date:04-Oct-2007 04:00:00 UTC

Registrant ID:tujtsKsILE5qOx6G

Registrant Name:DNS Administration

Registrant Organization:VA Software Corporation (OSTG)

Registrant Street1:46939 Bayside Parkway

Name Server:NS1.VASOFTWARE.COM

Name Server:NS2.VASOFTWARE.COM

Name Server:NS3.VASOFTWARE.COM

Name Server:NS1.OSTG.COM

Name Server:NS2.OSTG.COM

DNSStuff.com – Web Tools for Troubleshooting DNS

- »» Drawback: Not Local Results
- »» DNS Report
- »» DNS Lookup
- »» ISP Cached DNS Lookup
- »» DNS Timing
- »» WHOIS Lookup
- »» Reverse DNS Lookup

Corrupted RNDK Key

```
Apr 22 13:21:54 ns1 named[11055]: /etc/rndc.key:1:
configuring key 'rndc-key': bad base64 encoding
Apr 22 13:21:54 ns1 named[11055]: loading
configuration: bad base64 encoding
Apr 22 13:21:54 ns1 named[11055]: exiting (due to fatal
error)
Apr 22 13:21:54 ns1 named: named startup failed
```

- »» Problem: rndc.key is corrupted
- »» Solution #1: run `/scripts/fixrndc`
- »» Solution #2 (if #1 does not work): run `rndc-confgen` and follow it's instructions

BIND is Listening on localhost Only

```
root@seminar [~]# netstat -nlp | grep 53
```

```
tcp      0      0 127.0.0.1:53          0.0.0.0:*          LISTEN    13841/named
tcp      0      0 127.0.0.1:953         0.0.0.0:*          LISTEN    13841/named
udp      0      0 127.0.0.1:53          0.0.0.0:*          13841/named
```

- Problem: BIND Only Listening on localhost
- Solution #1: comment out the listen directive in /etc/named.conf
- Solution #2: add an IP address list to the listen directive of just the IP's you want to listen on

Question & Answer

Simplify.