

The logo for NSD 4 features the letters 'NSD' in a bold, teal, 3D font. The letter 'S' is a solid red circle. To the right of 'NSD' is a large, stylized number '4' in a teal, 3D font with a white outline. Below the logo, the text 'Almost released' is written in a teal, sans-serif font.

NSD 4

Almost released

<http://www.nlnetlabs.nl/downloads/nsd/nsd-4.0.0rc2.tar.gz>

The NLnet Labs logo consists of the text 'NLnet' in a teal, sans-serif font above the text 'Labs' in a larger, black, sans-serif font. To the left of 'Labs' is a vertical column of binary code (0s and 1s) in black.

NLnet Willem Toorop
Willem@NLnetLabs.nl
Labs 16 October 2013

History

- June 16, 2003 **NSD1.0** Mean and lean authoritative only
- February 14, 2004 **NSD2.0** DNSSEC, AXFR, configuration file
- September 15, 2006 **NSD3.0** IXFR (in), NSEC3, TSIG, DNAME
- May 5, 2011 **NSD** plans presented at RIPE62
- December 13, 2012 **NSD4.0b1**
- Januari 10, 2013 **NSD4.0b2**
- Januari 23, 2012 **NSD4.0b3**
- Februari 5, 2012 **NSD4.0b4**
- July 15, 2012 **NSD4.0b5**
- October 7, 2013 **NSD4.0rc1**
- October 14, 2013 **NSD4.0rc2**
- October 21, 2013 **NSD4.0** **Expected release**

With respect to NSD3

NS4

than NSD3

- ▶ is faster
 - ▶ Major rework in internal data structures and file back-end (radix-tree and a live “mmaped” back-end)

With respect to NSD3

NS4

than NSD3

- ▶ is faster
 - ▶ Major rework in internal data structures and file back-end
- ▶ can handle more tcp connections
 - ▶ epoll/kqueue support with libevent

With respect to NSD3

NS4

than NSD3

- ▶ is faster
 - ▶ Major rework in internal data structures and file back-end
- ▶ can handle more tcp connections
- ▶ can execute NSEC3-IXFRs faster
 - ▶ Time relative to size of the IXFR and not the zone

With respect to NSD3

NSD4

than NSD3

- ▶ is faster
 - ▶ Major rework in internal data structures and file back-end
- ▶ can handle more tcp connections
- ▶ can execute NSEC3-IXFRs faster
- ▶ can handle more zones
 - ▶ integrated zone compiler (live back-end)
 - ▶ *patterns* for common configuration options among zones
 - ▶ use `nsd-control` to add zones tied to *patterns*
 - ▶ No need for a restart any more

With respect to NSD3

NSD4

than NSD3

- ▶ is faster
 - ▶ Major rework in internal data structures and file back-end
- ▶ can handle more tcp connections
- ▶ can execute NSEC3-IXFRs faster
- ▶ can handle more zones
- ▶ is better manageable
 - ▶ Selectively read in modified zone files
(with `kill -HUP $pid` or `nsd-control reload`)
 - ▶ Change TSIG keys, *patterns* and zones without restart
(with `nsd-control reconfig`)
 - ▶ No need for restart any more
 - ▶ Does not change pid when reloading
 - ▶ Does not fork away when attached to a console
(for daemon management suites)
 - ▶ Secure remote provisioning and control with `nsd-control`

With respect to NSD3

NS4

than NSD3

- ▶ is faster
 - ▶ Major rework in internal data structures and file back-end
- ▶ can handle more tcp connections
- ▶ can execute NSEC3-IXFRs faster
- ▶ can handle more zones
 - ▶ integrated zone compiler (live back-end)
 - ▶ *patterns* for common configuration options among zones
 - ▶ use `nsd-control` to add zones tied to *patterns*
- ▶ is better manageable
 - ▶ Selectively read in modified zone files
 - ▶ Change TSIG keys, *patterns* and zones without restart
 - ▶ Does not change pid when reloading
 - ▶ Does not fork away when attached to a console
 - ▶ Secure remote provisioning and control with `nsd-control`
- ▶ uses more memory

With respect to NSD3 - Upgrading

NSD4 is backwards compatible with NSD3

- ▶ The DNS protocol logic itself has not been touched

With respect to NSD3 - Upgrading

NSD4 is backwards compatible with NSD3

- ▶ The DNS protocol logic itself has not been touched
 - ▶ The old NSD3 config can be read without problems
 - ▶ **difffile:** ixfr.db is ignored
 - ▶ Not the other way around
- (zonelistfile:, xfrdir:, remote-control: and pattern:)

With respect to NSD3 - Upgrading

NSD4

is backwards compatible with

NSD3

- ▶ The DNS protocol logic itself has not been touched
- ▶ The old NSD3 config can be read without problems
 - ▶ `difffile: ixfr.db` is ignored
 - ▶ Not the other way around
(`zonelistfile:`, `xfrdir:`, `remote-control:` and `pattern:`)
- ▶ `nsd.db` has new format and is converted on first startup
 - ▶ Needs to be writeable now
 - ▶ Not the other way around
(recreate an old NSD3 compatible `nsd.db` with `zonec`)

With respect to NSD3 - Upgrading

NSD4 is backwards compatible with NSD3

- ▶ The DNS protocol logic itself has not been touched
- ▶ The old NSD3 config can be read without problems
 - ▶ `difffile: ixfr.db` is ignored
 - ▶ Not the other way around
(`zonelistfile:`, `xfrdir:`, `remote-control:` and `pattern:`)
- ▶ `nsd.db` has new format and is converted on first startup
 - ▶ Needs to be writeable now
 - ▶ Not the other way around
(recreate an old NSD3 compatible `nsd.db` with `zonec`)
- ▶ `nsdc` is no longer needed and removed
 - ▶ Cron job for `nsdc patch` no longer needed
(or use `nsd-control write` to write zone files for secondaries)
 - ▶ `nsdc reload` → `kill -HUP $pid`
 - ▶ `nsdc stop` → `kill -TERM $pid`
 - ▶ or use `nsd-control`

Provisioning and control

NSD remote server control utility

```
nsd-control [-c cfgfile] [-s server] command
```

- ▶ Contacts the **NSD** server over SSL
 - ▶ By default limited to 127.0.0.1 (by the server), but you can configure it to use a different IP address.

Provisioning and control

NSD remote server control utility

```
nsd-control [-c cfgfile] [-s server] command
```

- ▶ Contacts the **NSD** server over SSL
 - ▶ By default limited to 127.0.0.1 (by the server), but you can configure it to use a different IP address.
 - ▶ Confidentiality, Authenticity, Integrity
 - ▶ X509 based authorization (i.e. no shared secret)

Provisioning and control

NSD remote server control utility

```
nsd-control [-c cfgfile] [-s server] command
```

- ▶ Contacts the **NSD** server over SSL
 - ▶ By default limited to 127.0.0.1 (by the server), but you can configure it to use a different IP address.
 - ▶ Confidentiality, Authenticity, Integrity
 - ▶ X509 based authorization (i.e. no shared secret)
 - ▶ the **NSD** server authenticates the `nsd-control`
 - ▶ the `nsd-control` authenticates the **NSD** server
 - ▶ i.e. (ultimately) signed by the **NSD** server

Provisioning and control

NSD remote server control utility

```
nsd-control [-c cfgfile] [-s server] command
```

- ▶ Contacts the **NSD** server over SSL
 - ▶ the **NSD** server authenticates the nsd-control
 - ▶ the nsd-control authenticates the **NSD** server
 - ▶ i.e. (ultimately) signed by the **NSD** server
 - ▶ nsd-control config: /etc/nsd.conf

```
remote-control:  
control-enable:    yes  
server-cert-file:  /etc/nsd/nsd_server.pem  
control-key-file:  /etc/nsd/nsd_control.key  
control-cert-file: /etc/nsd/nsd_control.pem
```

- ▶ **NSD** server config: /etc/nsd.conf

```
remote-control:  
control-enable:    yes  
server-key-file:   /etc/nsd/nsd_server.key  
server-cert-file:  /etc/nsd/nsd_server.pem
```


Provisioning and control

NSD remote server control utility

```
nsd-control [-c cfgfile] [-s server] command
```

- ▶ Contacts the **NSD** server over SSL

- ▶ nsd-control config: /etc/nsd.conf

```
remote-control:
    control-enable:    yes
    server-cert-file:  /etc/nsd/nsd_server.pem
    control-key-file:  /etc/nsd/nsd_control.key
    control-cert-file: /etc/nsd/nsd_control.pem
```

- ▶ **NSD** server config: /etc/nsd.conf

```
remote-control:
    control-enable:    yes
    server-key-file:   /etc/nsd/nsd_server.key
    server-cert-file: /etc/nsd/nsd_server.pem
```

- ▶ **nsd-control-setup** [-d dir] - setup SSL keys for nsd-control
-d dir use directory to store keys and certificates.
default: /etc/nsd

Provisioning and control

NSD remote server control utility

```
nsd-control [-c cfgfile] [-s server] command
```

Commands:

start	start server; runs nsd
stop	stops the server
reload [<u>zone</u>]	reload modified zonefiles from disk
reconfig	reload the config file
repattern	the same as reconfig
log_reopen	reopen logfile (for log rotate)
status	display status of server
stats	print statistics
stats_noreset	peek at statistics
addzone <u>name</u> <u>pattern</u>	add a new zone
delzone <u>name</u>	remove a zone
write [<u>zone</u>]	write changed zonefiles to disk
notify [<u>zone</u>]	send NOTIFY messages to slave servers
transfer [<u>zone</u>]	try to update slave zones to newer serial
force_transfer [<u>zone</u>]	update slave zones with AXFR, no serial check
zonestatus [<u>zone</u>]	print state, serial, activity
serverpid	get pid of server process
verbosity [<u>number</u>]	change logging detail

Provisioning and control Patterns

- ▶ Can be used within the config file
- ▶ /etc/nsd/nsd.conf

```
server:
    zonesdir:      "/etc/nsd"
pattern:
    name:          "secondary-4-nlnetlabs"
    zonefile:      "secondaries/%z/%s"
    allow-notify:  2001:7b8:206:1::1 NOKEY
    request-xfr:   2001:7b8:206:1::1 NOKEY
zone:
    name:          "nlnetlabs.nl"
    include-pattern: "secondary-4-nlnetlabs"
zone:
    name:          "unbound.net"
    include-pattern: "secondary-4-nlnetlabs"
```

- ▶ **zonefile**: processes the names of the zones:
 - %s zone name
 - %z top level domain of zone name
 - %1 first character of zone name
 - %y second label from top
 - %2 second character of zone name
 - %x third label from top
 - %3 third character of zone name

Provisioning and control Patterns

- ▶ Can be used within the config file
- ▶ Can be nested
 - ▶ /etc/nsd/nsd.conf

```
pattern:
    name:                "common-masters"
    zonefile:            "master/%1/%2/%3/%s"
pattern:
    name:                "secondary-at-nlnetlabs"
    notify:              2001:7b8:206:1::1 NOKEY
    provide-xfr:         2001:7b8:206:1::1 NOKEY
    include-pattern:    "common-masters"
pattern:
    name:                "secondary-at-cwi"
    notify:              192.16.197.229 NOKEY
    provide-xfr:         192.16.197.229 NOKEY
    include-pattern:    "common-masters"
pattern:
    name:                "secondary-at-nlnetlabs-and-cwi"
    include-pattern:    "secondary-at-nlnetlabs"
    include-pattern:    "secondary-at-cwi"
```

Provisioning and control

Patterns

- ▶ Can be used within the config file
- ▶ Can be nested
- ▶ To dynamically add and remove zones
 - ▶ `/etc/nsd/nsd.conf`

```
server:
    zonelistfile: "/var/db/nsd/zone.list"
pattern:
    name:          "secondary-4-nlnetlabs"
    zonefile:      "secondaries/%z/%s"
pattern:
    name:          "secondary-at-cwi"
    zonefile:      "master/%1/%2/%3/%s"
```

- ▶ `nsd-control addzone credns.net secondary-4-nlnetlabs`
- ▶ `nsd-control addzone toorop.net secondary-at-cwi`

Provisioning and control

Patterns

- ▶ Can be used within the config file
- ▶ Can be nested
- ▶ To dynamically add and remove zones
 - ▶ `/etc/nsd/nsd.conf`

```
server:
    zonelistfile: "/var/db/nsd/zone.list"
pattern:
    name:          "secondary-4-nlnetlabs"
    zonefile:      "secondaries/%z/%s"
pattern:
    name:          "secondary-at-cwi"
    zonefile:      "master/%1/%2/%3/%s"
```

- ▶ `nsd-control addzone credns.net secondary-4-nlnetlabs`
- ▶ `nsd-control addzone toorop.net secondary-at-cwi`
- ▶ `/var/db/nsd/zone.list`

```
# NSD zone list
# name pattern
add credns.net secondary-4-nlnetlabs
add toorop.net secondary-at-cwi
```

Provisioning and control

Patterns

- ▶ Can be used within the config file
- ▶ Can be nested
- ▶ To dynamically add and remove zones
 - ▶ `/etc/nsd/nsd.conf`

```
server:
    zonelistfile: "/var/db/nsd/zone.list"
pattern:
    name:         "secondary-4-nlnetlabs"
    zonefile:     "secondaries/%z/%s"
pattern:
    name:         "secondary-at-cwi"
    zonefile:     "master/%1/%2/%3/%s"
```

- ▶ `nsd-control addzone credns.net secondary-4-nlnetlabs`
- ▶ `nsd-control addzone toorop.net secondary-at-cwi`
- ▶ **Zonefiles:**

```
credns.net /etc/nsd/secondaries/net/credns.net
toorop.net /etc/nsd/master/t/o/o/toorop.net
```

Provisioning and control

Statistics

nsd-control stats

nsd-control stats_noreset

► Output counter values

```
server0.queries=77355
num.queries=77355
time.boot=119877.247897
time.elapsed=280.069877
size.db.disk=334430208
size.db.mem=122032188
size.xfrd.mem=12736584
size.config.disk=199
size.config.mem=61784
num.type.A=47590
num.type.AS=1527
num.type.MD=0
num.type.MF=0
num.type.CNAME=18
num.type.SOA=172
num.type.MB=0
num.type.MG=0
num.type.MR=0
num.type.NULL=0
num.type.WKS=0
num.type.PTR=100
num.type.HINFO=0
```

```
num.type.MINFO=0
num.type.MX=3124
num.type.TXT=354
num.type.RP=0
num.type.AFSDB=0
num.type.X25=0
num.type.ISDN=0
num.type.RT=0
num.type.NSAP=0
num.type.SIG=0
num.type.KEY=0
num.type.PX=0
num.type.AAAA=3815
num.type.LOC=0
num.type.NXT=0
num.type.SRV=179
num.type.NAPTR=0
num.type.KX=0
num.type.CERT=0
num.type.TYPE38=31
num.type.DNAME=0
num.type.OPT=0
```

```
num.type.APL=0
num.type.DS=2309
num.type.SSHFP=0
num.type.IPSECKEY=0
num.type.RRSIG=2
num.type.NSEC=0
num.type.DNSKEY=199
num.type.DHCID=0
num.type.NSEC3=0
num.type.NSEC3PARAM=0
num.type.TLSA=0
num.type.SPF=225
num.type.NID=0
num.type.L32=0
num.type.L64=0
num.type.LP=0
num.type.TYPE252=3
num.type.TYPE255=362
num.opcode.QUERY=65845
num.class.IN=79761
num.class.CH=23
num.rcode.NOERROR=74009
```

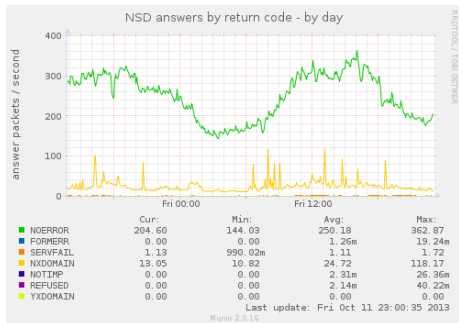
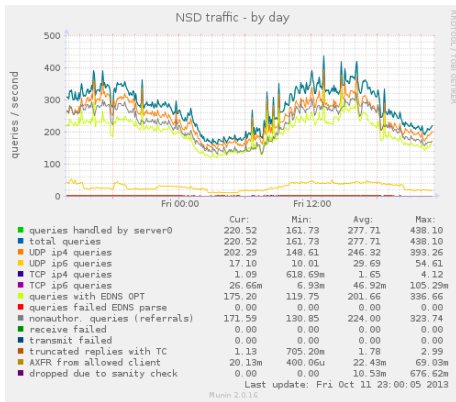
```
num.rcode.FORMERR=3
num.rcode.SERVFAIL=295
num.rcode.NXDOMAIN=5073
num.rcode.NOTIMP=0
num.rcode.REFUSED=0
num.rcode.YXDOMAIN=0
num.edns=60404
num.ednserr=0
num.udp=70392
num.tcp=389
num.tcp6=18
num.answer_wo_aa=65001
num.rxerr=0
num.txerr=0
num.raxfr=3
num.truncated=419
num.dropped=0
zone.master=7
zone.slave=50
```


Provisioning and control

Statistics

nsd-control stats

- Munin plugin in contrib utilizing nsd-control stats

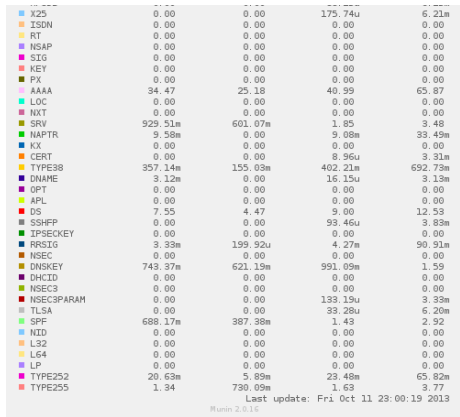
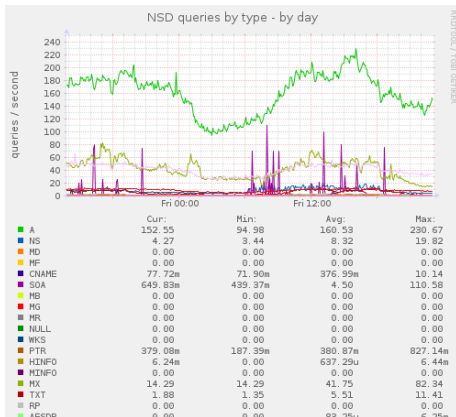


Provisioning and control

Statistics

nsd-control stats

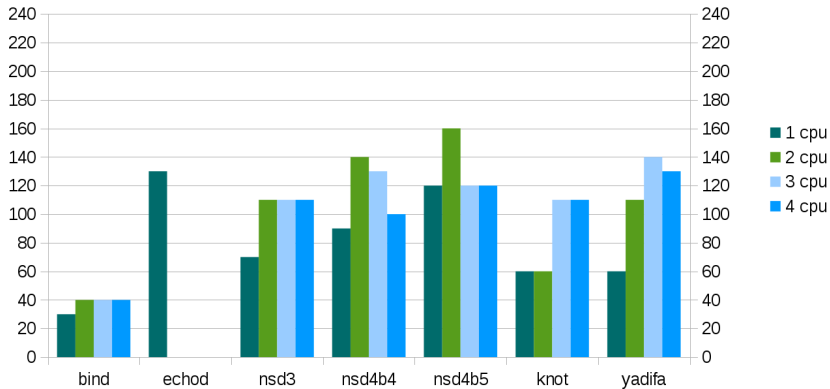
- Munin plugin in contrib utilizing nsd-control stats



Performance

- ▶ More detailed treatment this afternoon at 14:00 in
Which habitat fits your name servers nature best?

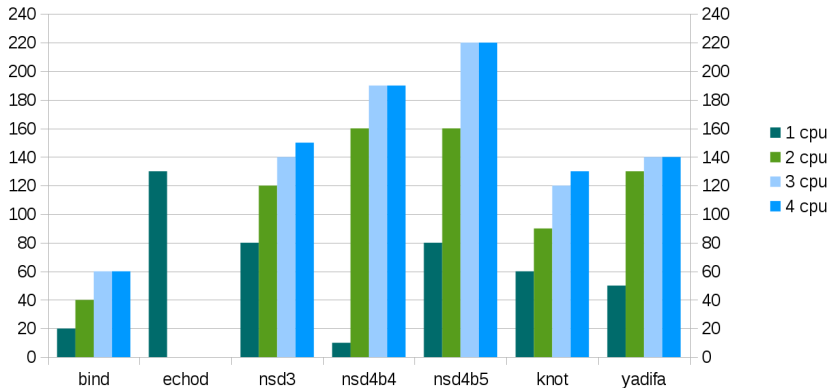
Linux 3.9



Performance

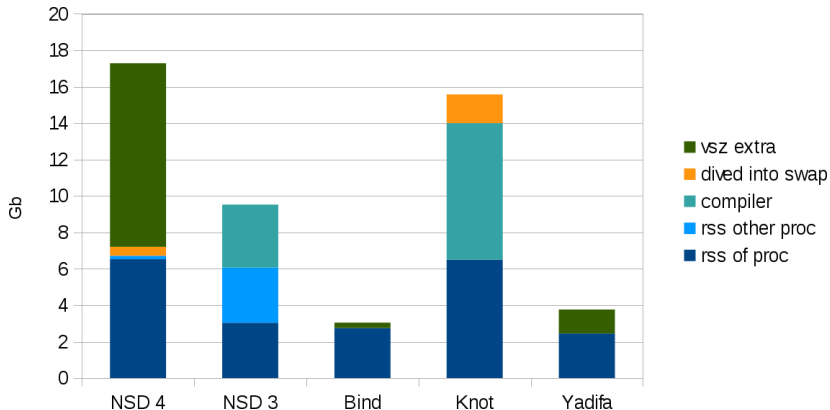
- ▶ More detailed treatment this afternoon at 14:00 in
Which habitat fits your name servers nature best?

freebsd 9.1



Performance

- ▶ More detailed treatment this afternoon at 14:00 in **Which habitat fits your name servers nature best?**



Resources



Release candidate 2

download	http://www.nlnetlabs.nl/downloads/nsd/nsd-4.0.0rc2.tar.gz
web	http://www.nlnetlabs.nl/projects/nsd/
mailing-list	nsd-users@nlnetlabs.nl
subscribe	http://open.nlnetlabs.nl/mailman/listinfo/nsd-users/
subversion	http://www.nlnetlabs.nl/svn/nsd/
donations	http://www.nlnetlabs.nl/labs/contributors/
support	http://www.nlnetlabs.nl/projects/nsd/support.html
me	Willem Toorop < willem@nlnetlabs.nl >