فصل پانزدهم

سرویس‌های DNS و DHCP

سرویس DNS

name resolution مکانیسمی است که چگونگی تبدیل نام‌ها به آدرس‌ها را فراهم می‌کند. در سیستم‌عامل‌های یونیکسی/لینوکسی دو گزینه اصلی برای به دست آوردن آدرس‌های معادل هر نام وجود دارد. فرض کنید که دو ماشین به نام‌های pc1 و hadi که به ترتیب دارای آدرس‌های ۱۹۲,۱۶۸,۱,۱ و ۱۹۲,۱۶۸,۱,۲ وجود دارند که قصد دارید ارتباطی میان آن‌ها را با استفاده از نام‌هایشان ایجاد کنید. اگر از روی ماشین pc1 دستور ping 192.168.1.2 را اجرا کنید و از روی ماشین hadi دستور ping 192.168.1.1 را اجرا کنید قطعاً پاسخ درست خواهید گرفت چون هر دوی این ماشین‌ها در یک شبکه هستند؛ اما اگر از روی ماشین pc1 دستور ping hadi و از روی ماشین hadi دستور ping pc1 را اجرا کنید با اینکه همه چیز درست است و از طریق آدرس‌ها قادر به ping هستید ولی با ping توسط نام‌ها به مشکل می‌خورید. سیستم‌عامل‌های یونیکسی (لینوکسی) ابتدا برای بدست آوردن آدرس معادل یک نام در فایل /etc/hosts به جستجو می‌پردازند. این فایل باید به‌صورت دستی بر روی هر یک از ماشین‌ها تنظیم شود. فرض کنید ۱۰ ماشین در شبکه داریم پس لازم است در هر ماشین به

ازای ۹ ماشین دیگر آدرس و نام معادل را وارد کنیم که از معایب این فایل در شبکه‌های بزرگ به حساب می‌آید. از دیگر معایب آن این است که پس از تغییر آدرس یک ماشین باید این تغییر را در ۹ ماشین دیگر نیز به‌صورت دستی اعمال کنیم. پس اگر فرض کنیم ۱۰ ماشین داریم پس حداقل باید ۹ آدرس و نام معادلشان را در هر ماشین به‌صورت دستی وارد نماییم؛ اما می‌توان حداکثری هم برای تنظیم دستی آدرس و نام معادل بیان کرد به این صورت که اگر در خود ماشینی مانند pc1 با آدرس ۱۹۲,۱۶۸,۱,۱ دستور ping 192.168.1.1 را اجرا کنیم قطعاً در صورت عدم مشکلی پاسخ درست خواهیم گرفت ولی اگر در خود ماشین pc1 دستور ping pc1 را اجرا کنیم چون مکانیسمی برای تبدیل نام به آدرس وجود ندارد قطعاً در خود همین ماشین هم به مشکل برمی‌خوریم پس می‌توان حداکثری را این‌طور گفت که اگر ۱۰ ماشین داشته باشیم به همراه وارد کردن آدرس‌ها و نام‌های معادل ۹ ماشین دیگر باید آدرس و نام معادل خود همان ماشین را هم در فایل /etc/hosts وارد کرد که می‌شود حداکثر ۱۰ ماشین. فایل /etc/hosts با سرویس dhcp به هیچ عنوان در تعامل نمی‌باشد؛ یعنی نباید این‌طور فرض شود که وقتی dhcp به ماشینی آدرس می‌دهد (به کارت شبکه ماشینی آدرس می‌دهد) این فایل به‌صورت خودکار بروز خواهد شد. بلکه باید دوباره آدرس جدید را به‌صورت دستی روی تک‌تک دیگر ماشین‌ها وارد نمود یا به عبارتی این فایل حالت استاتیک (Static) دارد.

فایل‌های hosts در تمامی سیستم‌عامل‌ها وجود دارند و اولین منبعی است که سیستم‌عامل برای نگاشت آدرس‌های ip به hostname ها به آن رجوع می‌کند. در هر خط این فایل یک IP و جلوی آن hostname معادلش نوشته می‌شود. لینوکس اول این فایل را می‌خواند و در صورت نیافتن پاسخ از DNS برای نگاشت آدرس‌های IP به hostname استفاده می‌کند. این فایل در دایرکتوری /etc و به‌صورت یک فایل متنی ساده ذخیره شده است.

نمونه‌ای از این فایل را در زیر مشاهده می‌کنید:

```
cat /etc/hosts
# Do not remove the following line, or various
programs
# that require network functionality will fail.
127.0.0.1 template.x.com template
localhost.localdomain localhost
::1 localhost6.localdomain6 localhost6
192.168.1.16 x.raja.com
192.168.11.19 mail.raja.com
12.18.11.28 www.raja.com
```

در هر خط این فایل آن ابتدا یک IP و جلوی آن hostname معادلش قرار دارد. آدرس IP و hostname معادلش با یک فاصله Tab از هم جدا می‌شوند. خطوطی که ابتدایشان # باشد توضیحات هستند. فرمت کلی هر خط آن به‌صورت زیر است:

IP_address canonical_hostname [aliases…]

Host Name ها می‌توانند شامل حروف، اعداد، کاراکتر – (dash) و کاراکتر نقطه باشند ولی باید حتماً با یک حرف آغاز شوند و با یک حرف هم پایان یابند. Alias ها (نام‌های مستعار) یک نام اضافی و یا کوتاه شده hostname و یا برای تعیین نوع hostname بکار می‌روند. به‌طور مثال localhost یک نام مستعار که تعیین کننده نوع hostname است.

گزینه بهتر و ساده‌تر که با dhcp نیز در تعامل است استفاده از dns است. شما یک ماشین را به‌عنوان dns server در نظر می‌گیرید. وقتی dns را روی ماشینی نصب می‌کنید نسبت به فایل etc/hosts/ دارای امکانات فراوانی هستید. اصلی‌ترین مزیت برای تمام مدیران مدیریت

ساده‌تر آدرس‌ها و نام‌های معادلشان است. با نصب و تنظیم dns نیاز به ایجاد و تنظیم فایل‌هایی به نام zone fileها دارید. در اصل zone fileها، پایگاه داده‌هایی هستند که مانند فایل etc/hosts/ دارای آدرس و نام‌های معادلشان هستند. از دیگر مزیت‌های dns اینکه شما بجای تنظیم دستی تک‌تک فایل‌های etc/hosts/ در هر ماشین فقط نیاز دارید یک‌بار آدرس هر ماشین و نام معادلش را در zone file مربوطه وارد کنید و یا در صورت تغییر یک آدرس فقط و فقط یک فایل در dns server را تغییر می‌دهید؛ یعنی در zone file مربوطه در dns server فقط باید یک بار همان آدرس را تغییر دهید و سپس تمامی دیگر ماشین‌ها این تغییر را متوجه خواهند شد. مزیت دیگر استفاده از dns ادغام یا همکاری آن با سرویس dhcp است. با تنظیم dhcp ویژگی وجود دارد که وقتی dhcp به ماشینی جدید، آدرس ip می‌دهد خود dhcp آدرس و نام معادل آن را به‌صورت خودکار در zone file وارد می‌کند؛ اما چگونه؟ برای این کار باید در تنظیم dhcp دو پارامتر زیر را تنظیم کنید. با فرض اینکه از قبل dns server را که دارای آدرس ۱۹۲,۱۶۸,۱,۳ است تنظیم کرده باشیم اولین پارامتر تنظیم شده زیر اشاره به نام دامنه دارد که به‌طور مثال raja.local است و دومین پارامتر اشاره به آدرس dns server دارد.

```
;    option domain-name    "raja.local"
;    option domain-name-servers    "192.168.1.3"
```

وقتی ماشینی از dhcp آدرس می‌گیرد به‌صورت خودکار آدرس dns server آن ۱۹۲,۱۶۸,۱,۳ تنظیم خواهد شد؛ اما پارامتری که باعث ثبت خودکار آدرس و نام ماشین در zone file در dns server می‌شود پارامتر زیر است. مقدار توصیه شده برای آن interim است.

```
ddns-update-style    "interim";
```

البته اگر به هر دلیلی آدرس ماشینی را تغییر دادید دیگر dhcp وظیفه تغییر آدرس در dns server را ندارد و خودتان باید دستی آن را

تغییر دهید؛ اما فقط در یک ماشین، در یک فایل و یک بار آدرس را تغییر خواهید داد که نسبت به فایل etc/hosts/ ساده‌تر مدیریت می‌شود.

فایل etc/resolv.conf/ در سیستم‌های یونیکسی (لینوکسی) در کلاینت‌ها و دیگر ماشین‌ها برای تنظیم آدرس name server ها استفاده می‌شود. در این فایل آدرس dns server های شبکه که باید کلاینت یا هر ماشینی از آن‌ها آدرس معادل نام را بخواهد به‌صورت زیر قرار می‌گیرد. در هر خط این فایل جلوی عبارت nameserver یک آدرس قرار می‌گیرد.

nameserver DNS_IP_ADDR

zone file‌ها که تعریف شدند باید آن‌ها را در فایل etc/named.conf/ معرفی کنیم. نمونه‌ای از این تعریف به‌صورت زیر است:

```
zone "dri.com" IN {
        type master;
        file "dri.com.zone";
        allow-update { none; };
        allow-transfer { none; };
};
```

اما در لینوکس چگونه ترتیب بین استفاده از فایل etc/hosts/ و dns معلوم می‌شود؟ اگر فرض کنیم که هر دو روش یعنی فایل etc/hosts/ و فایل etc/resolv.conf/ را داشته باشیم، برای داشتن آدرس dns server ها لینوکس از فایلی به نام etc/host.conf/ برای فهمیدن اینکه اولویت با کدام روش است (فایل etc/hosts/ یا dns server) استفاده می‌کند. این فایل در اصل پایگاه داده‌ای است که برای تعیین روش و اولویت name resolution می‌باشد که در سیستم‌عامل‌های یونیکسی (لینوکسی) استفاده می‌شود. خطی مانند زیر در این فایل قرار دارد که معلوم می‌کند ماشین لینوکسی باید ابتدا برای به دست آوردن آدرس

معادل نام از فایل etc/hosts/ استفاده کند و درصورتی‌که از این فایل بـه نتیجه‌ای نرسید به سراغ dns برود.

```
cat /etc/host.conf
order hosts,bind
```

منظور از hosts در خط بـالا همـان فایـل etc/hosts/ اسـت و چـون پیش از bind آمده است پس اولویت اول است. منظور از bind هـم ایـن اســت کــه ماشــین لینوکســی فایــل etc/resolv.conf/ را خوانــده، آدرس(های) dns server (ها) را پیدا کـرده و درخواسـت را بـه آن (هـا) ارسال می‌کند.

در نهایت نمونه‌ای از فایل‌هـای etc/named.conf/، zone file هـا و etc/resolv.conf/ ارائه شده است که می‌تواند به‌صورت عملی شما را در تنظیم یک DNS Server واقعی کمک کند.

```
cat /etc/named.conf
//
// named.caching-nameserver.conf
//
// Provided by Red Hat caching-nameserver package to
configure the
// ISC BIND named(8) DNS server as a caching only
nameserver
// (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named
configuration files.
//
// DO NOT EDIT THIS FILE - use system-config-bind
or an editor
// to create named.conf - edits to this file will be lost on
```

```
// caching-nameserver package upgrade.
//
options {
        #listen-on port 53 { 127.0.0.1; };
        #listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file
"/var/named/data/named_mem_stats.txt";
        recursion no;

        // Those options should be used carefully because
they disable port
        // randomization
        // query-source    port 53;
        // query-source-v6 port 53;

        #allow-query     { localhost; };
        #allow-query-cache { localhost; };
};
logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};
```

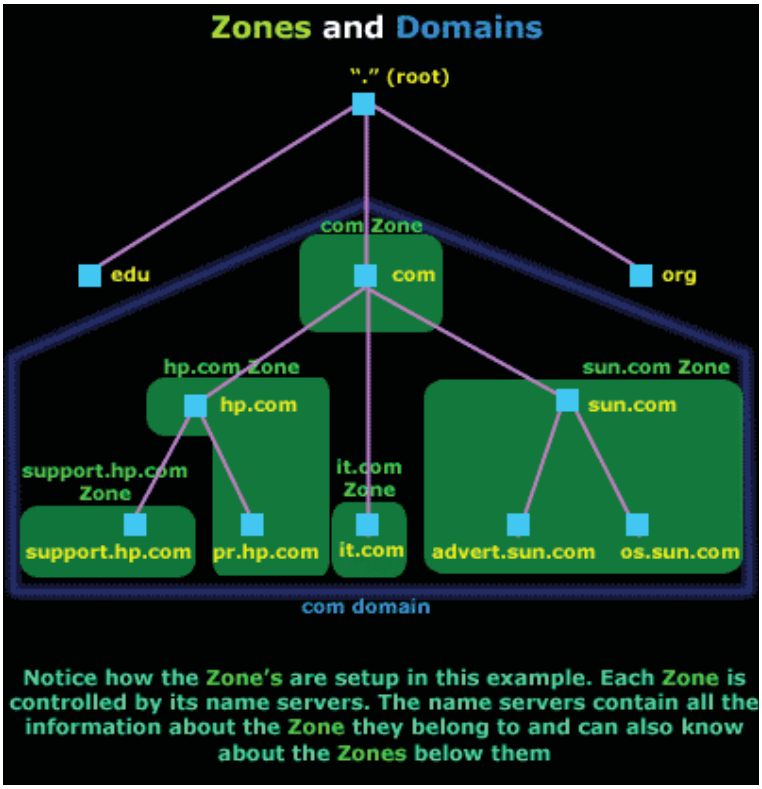
```
zone "dri.com" IN {
        type master;
        file "dri.com.zone";
        allow-update { none; };
        allow-transfer { none; };
};

zone "dri.net" IN {
        type master;
        file "dri.net.zone";
        allow-update { none; };
        allow-transfer { none; };
};

zone "dri.org" IN {
        type master;
        file "dri.org.zone";
        allow-update { none; };
        allow-transfer { none; };
};
zone "dri.ir" IN {
        type master;
        file "dri.ir.zone";
        allow-update { none; };
        allow-transfer { none; };
};

#zone "salamdri.com" IN {
```

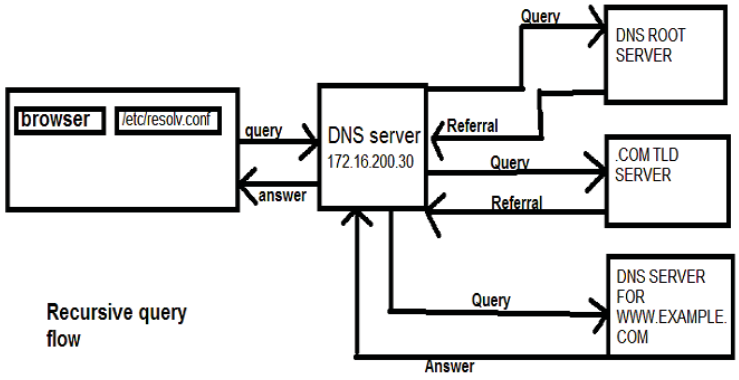
```
#       type master;
#      file "salamdri.com.zone";
#     allow-update { none; };
#    allow-transfer { none; };
#};

include "/etc/rndc.key";

include "/etc/named.rfc1912.zones";


cat /var/named/dri.com.zone
$TTL    86400
@               IN SOA  ns1.dri.ir.          netadmin.dri.com.
(
                                2011010901      ; serial (d.
adams)
                                2H              ; refresh
                                5M              ; retry
                                2H              ; expiry
                                1H )            ; minimum
;Nameservers
                IN NS           ns1.dri.ir.
;MailServers
                IN MX   10      mx1.dri.com.

;Hosts
ns1             IN A            192.168.10.196
```

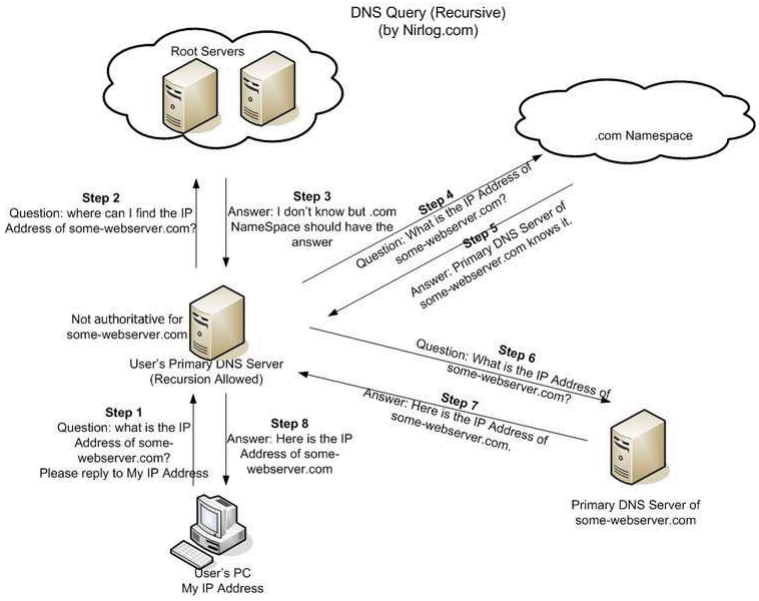
```
mailserver      IN A            192.168.10.197
mx1             IN CNAME        mailserver
imap            IN CNAME        mailserver
smtp            IN CNAME        mailserver
mail            IN A            192.168.10.198
;@              IN A            192.168.10.198
@               IN TXT          "v=spf1 mx ~all"
_domainkey      IN TXT          "o=-"
default._domainkey      IN TXT  "k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQK
BgQDAZbSzYbe+gCGpkVJXGPcKwEans10aVYkYTGe
Bz7PIEw8mj3iEp3GH+iNwRObT1CSSPuHewUVEzKE
DWj9E9JxfP2MnXGB8caMXfash0i0VC3I7Qb08QxEwY
ldYWwGjit1w2ZkLnhgbwwL4kHf7w4w9fc8kgh00nHx5s
skzF45dlQIDAQAB;"

cat /var/named/dri.ir.zone
$TTL    86400
@               IN SOA  ns1.dri.ir.          netadmin.dri.com.
(
                                2011010901      ; serial (d.
adams)
                                2H              ; refresh
                                5M              ; retry
                                2H              ; expiry
                                1H )            ; minimum
;Nameservers
                IN NS           ns1.dri.ir.
```

```
;MailServers
            IN MX   10      mx1.dri.com.

;Hosts
ns1             IN A            192.168.10.196
mailserver      IN A            192.168.10.197
mx1             IN CNAME        mailserver
imap            IN CNAME        mailserver
smtp            IN CNAME        mailserver
mail            IN A            192.168.10.198
;@              IN A            192.168.10.198
@               IN TXT          "v=spf1 mx ~all"
_domainkey      IN TXT          "o=-"
default._domainkey      IN TXT  "k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQK
BgQDAZbSzYbe+gCGpkVJXGPcKwEans10aVYkYTGe
Bz7PIEw8mj3iEp3GH+iNwRObT1CSSPuHewUVEzKE
DWj9E9JxfP2MnXGB8caMXfash0i0VC3I7Qb08QxEwY
ldYWwGjit1w2ZkLnhgbwwL4kHf7w4w9fc8kgh00nHx5s
skzF45dlQIDAQAB;"

cat /etc/resolv.conf
192.168.10.196
```

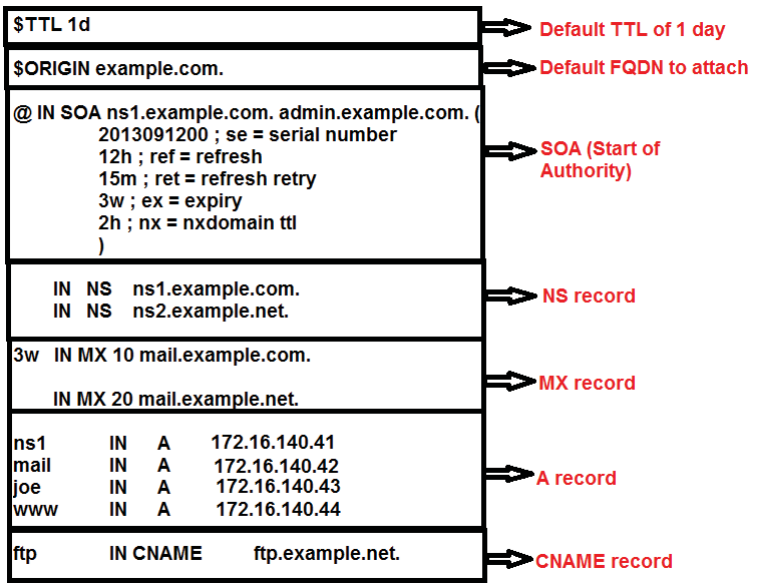
تصاویر و دستورات dig و dnstracer که در زیر ارائه شده‌اند، نحوه عملکرد DNS را بررسی می‌نمایند:


Zones and Domains
"." (root)
com Zone
edu
com
org
hp.com Zone
hp.com
sun.com Zone
sun.com
support.hp.com Zone
it.com Zone
support.hp.com
pr.hp.com
it.com
advert.sun.com
os.sun.com
com domain
Notice how the Zone's are setup in this example. Each Zone is controlled by its name servers. The name servers contain all the information about the Zone they belong to and can also know about the Zones below them


browser
/etc/resolv.conf
query
answer
DNS server
172.16.200.30
Query
DNS ROOT SERVER
Referral
Query
.COM TLD SERVER
Referral
Query
DNS SERVER FOR WWW.EXAMPLE.COM
Answer
Recursive query flow



Resource Record	Description
SOA (Start of Authority)	Indicates that the server is the best authoritative source for data concerning the zone. Each zone must have an SOA record, and only one SOA record can be in a zone.
NS (Name Server)	Identifies a DNS server functioning as an authority for the zone. Each DNS server in the zone (whether primary master or secondary) must be represented by an NS record.
A (Address)	Provides a name-to-address mapping that supplies an IPv4 address for a specific DNS name. This record type performs the primary function of the DNS: converting names to addresses
AAAA (Address)	Provides a name-to-address mapping that supplies an IPv6 address for a specific DNS name. This record type performs the primary function of the DNS: converting names to addresses.
PTR (Pointer)	Provides an address-to-name mapping that supplies a DNS name for a specific address in the in-addr.arpa domain. This is the functional opposite of an A record, used for reverse lookups only.
CNAME (Canonical Name)	Creates an alias that points to the canonical name (that is, the "real" name) of a host identified by an A record. Administrators use CNAME records to provide alternative names by which systems can be identified.
MX (Mail Exchange)	Identifies a system that will direct email traffic sent to an address in the domain to the individual recipient, a mail gateway, or another mail server.



how dns works

http://www.slashroot.in/how-dns-works

[root@linuxfedora ~]# dig +trace www.google.com

; <<>> DiG 9.10.3-P3-RedHat-9.10.3-10.P3.fc23 <<>> +trace www.google.com

;; global options: +cmd

. 9532 IN NS d.root-servers.net.

. 9532 IN NS j.root-servers.net.

. 9532 IN NS m.root-servers.net.

. 9532 IN NS e.root-servers.net.

. 9532 IN NS f.root-servers.net.

. 9532 IN NS c.root-servers.net.

. 9532 IN NS h.root-servers.net.

. 9532 IN NS g.root-servers.net.

. 9532 IN NS k.root-servers.net.

. 9532 IN NS l.root-servers.net.

. 9532 IN NS a.root-servers.net.

. 9532 IN NS i.root-servers.net.

. 9532 IN NS b.root-servers.net.

;; Received 460 bytes from 192.168.7.1#53(192.168.7.1) in 1 ms

com. 172800 IN NS l.gtld-servers.net.

com. 172800 IN NS a.gtld-servers.net.

com. 172800 IN NS g.gtld-servers.net.

com. 172800 IN NS j.gtld-servers.net.

com. 172800 IN NS h.gtld-servers.net.

com. 172800 IN NS d.gtld-servers.net.

com. 172800 IN NS b.gtld-servers.net.

com. 172800 IN NS m.gtld-servers.net.

com. 172800 IN NS i.gtld-servers.net.

com. 172800 IN NS f.gtld-servers.net.

com. 172800 IN NS e.gtld-servers.net.

com. 172800 IN NS c.gtld-servers.net.

com. 172800 IN NS k.gtld-servers.net.

com. 86400 IN DS 30909 8 2 E2D3C916F6DEEAC73294E8268FB5885044A833FC54 59588F4A9184CF C41A5766

com. 86400 IN RRSIGDS 8 1 86400 20161017050000 20161004040000 39291 . XYjYLC7xG5vEb9pblGMVIZCZHdPdB2OvsjTI5G1flwf pmad+YhKnUqyN 2KsJWm09p5AW2SenmbEBXjm+zZgTXBt7Z3gA5C1n BsJkiZxhPBIl/C6T Fs0mFeOpSgLT0sEYkm/OpgwJm2LM0pgkm9ewcaFRP vTqiYCZmOFLZkBP eJp1mfMHCgwwjesBxXixr17mKEVONYrxdPUdrIPwNz Xb2ZqExNoN1+4z 5Z7qhpoD9+k2KDfSgTtTx+BVJsjqVTYj1vtkae+NSTMe SSH3RtmgeBSs GfZ5CyB6oMNEbej9GsSwJjW4Rpw2CXUKc3i1EN0zT YOSBiQGAXkBAKH0 /6WwSQ==

;; Received 866 bytes from 192.36.148.17#53(i.root-servers.net) in 1763 ms

google.com. 172800 IN NS ns2.google.com.

google.com. 172800 IN NS ns1.google.com.

google.com. 172800 IN NS ns3.google.com.

google.com. 172800 IN NS ns4.google.com.

CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 86400 IN NSEC3 1 1 0 - CK0Q1GIN43N1ARRC9OSM6QPQR81H5M9A NS SOA RRSIG DNSKEY NSEC3PARAM

CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 86400 IN RRSIG NSEC3 8 2 86400 20161009044157 20161002033157 27452 com. M41sYMa1AlSgKf/CWelF3cJ4O2uGYGJEWlS1b8b2WlsMKCXnhK/rYlrb FAtAWNcgyzdspmEEZtRcZqLj4x4Oizr3zHPz2EM18IPuDsSdeIIHV70y gwEnInozpTeqk1A0u/fVVSDpfcurgcZcW9bGbu74cLlg9KZ+J2V//br1 +7w=

S84AE3BIT99DKIHQH27TRC0584HV5KOH.com. 86400 IN NSEC3 1 1 0 - S84J17P3PT4RKMEJOHNGD73C5Q5NV5S9 NS DS RRSIG

S84AE3BIT99DKIHQH27TRC0584HV5KOH.com. 86400 IN RRSIG NSEC3 8 2 86400 20161011044630 20161004033630 27452 com.

jS48lJO+/4fRTdvb//Mk+r9+MglfhwHagL11fhTbRJTMZ
8qSmEc9Jccw
ppRWsS2VDiyiemuMgC8ZzY4bhAMfiWx648BOgVWU
WVsh4m3Q6EewUuDO
ZT12d6l0RZR5O13SwrKFCBcgHrlI+up2UQuxG40UKZ
LJQP75R0Is2Wlo Tqk=

;; Received 664 bytes from 192.41.162.30#53(l.gtld-servers.net) in 1659 ms

www.google.com. 300 IN A 172.217.16.196

;; Received 48 bytes from 216.239.34.10#53(ns2.google.com) in 1629 ms

[root@linuxfedora ~]#

[root@linuxfedora ~]# dnstracer -s . -4 -o www.google.com

bash: dnstracer: command not found...

^C

[root@linuxfedora ~]# dnf install dnstracer

Failed to synchronize cache for repo 'google-chrome' from 'http://dl.google.com/linux/chrome/rpm/stable/i386':

```
repomd.xml parser error: Parse error at line: 1 (syntax
error), disabling.

Last metadata expiration check performed 1:36:27 ago on
Tue Oct  4 18:03:19 2016.

Dependencies resolved.

==============================================
==============================================
==============================================
======================================

 Package                                      Arch
Version                                  Repository
Size

==============================================
==============================================
==============================================
======================================

Installing:

 dnstracer                  i686                 1.9-
13.fc23                  fedora                   30 k


Transaction Summary

==============================================
==============================================
```

```
================================================================================
================================================================================
Install  1 Package

Total download size: 30 k
Installed size: 41 k
Is this ok [y/N]: y
Downloading Packages:
dnstracer-1.9-13.fc23.i686.rpm
4.2 kB/s |  30 kB     00:07
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
----------
Total
1.5 kB/s |  30 kB     00:20
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Installing       :       dnstracer-1.9-13.fc23.i686
1/1
```

```
  Verifying        :  dnstracer-1.9-13.fc23.i686
1/1

Installed:
  dnstracer.i686 1.9-13.fc23

Complete!
[root@linuxfedora ~]# dnstracer -s . -4 -o
www.google.com
Tracing to www.google.com[a] via A.ROOT-
SERVERS.NET, maximum of 3 retries
A.ROOT-SERVERS.NET [.] (198.41.0.4)
 |\___ m.gtld-servers.net [com] (192.55.83.30)
 |      |\___ ns4.google.com [google.com] (216.239.38.10)
Got authoritative answer
 |      |\___ ns3.google.com [google.com] (216.239.36.10)
Got authoritative answer
 |      |\___ ns1.google.com [google.com] (216.239.32.10)
Got authoritative answer
 |       \___ ns2.google.com [google.com] (216.239.34.10)
Got authoritative answer
 |\___ l.gtld-servers.net [com] (192.41.162.30)
```

| |___ ns4.google.com [google.com] (216.239.38.10) (cached)

| |___ ns3.google.com [google.com] (216.239.36.10) (cached)

| |___ ns1.google.com [google.com] (216.239.32.10) (cached)

| ___ ns2.google.com [google.com] (216.239.34.10) (cached)

|___ k.gtld-servers.net [com] (192.52.178.30)

| |___ ns4.google.com [google.com] (216.239.38.10) (cached)

| |___ ns3.google.com [google.com] (216.239.36.10) (cached)

| |___ ns1.google.com [google.com] (216.239.32.10) (cached)

| ___ ns2.google.com [google.com] (216.239.34.10) (cached)

|___ j.gtld-servers.net [com] (192.48.79.30)

| |___ ns4.google.com [google.com] (216.239.38.10) (cached)

| |___ ns3.google.com [google.com] (216.239.36.10) (cached)

| |___ ns1.google.com [google.com] (216.239.32.10) (cached)

| ___ ns2.google.com [google.com] (216.239.34.10) (cached)

|___ i.gtld-servers.net [com] (192.43.172.30)

| |___ ns4.google.com [google.com] (216.239.38.10) (cached)

| |___ ns3.google.com [google.com] (216.239.36.10) (cached)

| |___ ns1.google.com [google.com] (216.239.32.10) (cached)

| ___ ns2.google.com [google.com] (216.239.34.10) (cached)

|___ h.gtld-servers.net [com] (192.54.112.30)

| |___ ns4.google.com [google.com] (216.239.38.10) (cached)

| |___ ns3.google.com [google.com] (216.239.36.10) (cached)

| |___ ns1.google.com [google.com] (216.239.32.10) (cached)

| ___ ns2.google.com [google.com] (216.239.34.10) (cached)

|___ g.gtld-servers.net [com] (192.42.93.30)

| |___ ns4.google.com [google.com] (216.239.38.10) (cached)

| |___ ns3.google.com [google.com] (216.239.36.10) (cached)

| |___ ns1.google.com [google.com] (216.239.32.10) (cached)

| ___ ns2.google.com [google.com] (216.239.34.10) (cached)

|___ f.gtld-servers.net [com] (192.35.51.30)

| |___ ns4.google.com [google.com] (216.239.38.10) (cached)

| |___ ns3.google.com [google.com] (216.239.36.10) (cached)

| |___ ns1.google.com [google.com] (216.239.32.10) (cached)

| ___ ns2.google.com [google.com] (216.239.34.10) (cached)

|___ e.gtld-servers.net [com] (192.12.94.30)

| |___ ns4.google.com [google.com] (216.239.38.10) (cached)

| |___ ns3.google.com [google.com] (216.239.36.10) (cached)

| |___ ns1.google.com [google.com] (216.239.32.10) (cached)

| ___ ns2.google.com [google.com] (216.239.34.10) (cached)

```
 |\___ d.gtld-servers.net [com] (192.31.80.30)
 |     |\___ ns4.google.com [google.com] (216.239.38.10)
(cached)
 |     |\___ ns3.google.com [google.com] (216.239.36.10)
(cached)
 |     |\___ ns1.google.com [google.com] (216.239.32.10)
(cached)
 |     \___ ns2.google.com [google.com] (216.239.34.10)
(cached)
 |\___ c.gtld-servers.net [com] (192.26.92.30)
 |     |\___ ns4.google.com [google.com] (216.239.38.10)
(cached)
 |     |\___ ns3.google.com [google.com] (216.239.36.10)
(cached)
 |     |\___ ns1.google.com [google.com] (216.239.32.10)
(cached)
 |     \___ ns2.google.com [google.com] (216.239.34.10)
(cached)
 |\___ b.gtld-servers.net [com] (192.33.14.30)
 |     |\___ ns4.google.com [google.com] (216.239.38.10)
(cached)
 |     |\___ ns3.google.com [google.com] (216.239.36.10)
(cached)
```

| |___ ns1.google.com [google.com] (216.239.32.10) (cached)

| ___ ns2.google.com [google.com] (216.239.34.10) (cached)

|___ a.gtld-servers.net [com] (2001:0503:a83e:0000:0000:0000:0002:0030) Not queried

___ a.gtld-servers.net [com] (192.5.6.30)

|___ ns4.google.com [google.com] (216.239.38.10) (cached)

|___ ns3.google.com [google.com] (216.239.36.10) (cached)

|___ ns1.google.com [google.com] (216.239.32.10) (cached)

___ ns2.google.com [google.com] (216.239.34.10) (cached)

ns2.google.com (216.239.34.10) www.google.com -> 172.217.16.196

ns1.google.com (216.239.32.10) www.google.com -> 172.217.16.196

ns3.google.com (216.239.36.10) www.google.com -> 172.217.16.196

ns4.google.com (216.239.38.10) www.google.com -> 172.217.16.196

```
[root@linuxfedora ~]# dig -4 maps.google.com. +norecurse +trace

; <<>> DiG 9.10.3-P3-RedHat-9.10.3-10.P3.fc23 <<>> -4 maps.google.com. +norecurse +trace
;; global options: +cmd
.                       9647    IN      NS      i.root-servers.net.
.                       9647    IN      NS      b.root-servers.net.
.                       9647    IN      NS      d.root-servers.net.
.                       9647    IN      NS      j.root-servers.net.
.                       9647    IN      NS      m.root-servers.net.
.                       9647    IN      NS      e.root-servers.net.
.                       9647    IN      NS      f.root-servers.net.
.                       9647    IN      NS      c.root-servers.net.
.                       9647    IN      NS      h.root-servers.net.
```

. 9647 IN NS g.root-servers.net.

. 9647 IN NS k.root-servers.net.

. 9647 IN NS l.root-servers.net.

. 9647 IN NS a.root-servers.net.

;; Received 460 bytes from 192.168.7.1#53(192.168.7.1) in 1 ms

com. 172800 IN NS j.gtld-servers.net.

com. 172800 IN NS i.gtld-servers.net.

com. 172800 IN NS c.gtld-servers.net.

com. 172800 IN NS h.gtld-servers.net.

com. 172800 IN NS f.gtld-servers.net.

com. 172800 IN NS g.gtld-servers.net.

com. 172800 IN NS m.gtld-servers.net.

com. 172800 IN NS e.gtld-servers.net.

com. 172800 IN NS l.gtld-servers.net.

com. 172800 IN NS b.gtld-servers.net.

com. 172800 IN NS k.gtld-servers.net.

com. 172800 IN NS a.gtld-servers.net.

com. 172800 IN NS d.gtld-servers.net.

com. 86400 IN DS 30909 8 2 E2D3C916F6DEEAC73294E8268FB5885044A833FC54 59588F4A9184CF C41A5766

com. 86400 IN RRSIGDS 8 1 86400 20161017050000 20161004040000 39291 . XYjYLC7xG5vEb9pblGMVIZCZHdPdB2OvsjTI5G1flwf pmad+YhKnUqyN 2KsJWm09p5AW2SenmbEBXjm+zZgTXBt7Z3gA5C1n BsJkiZxhPBIl/C6T Fs0mFeOpSgLT0sEYkm/OpgwJm2LM0pgkm9ewcaFRP vTqiYCZmOFLZkBP

eJp1mfMHCgwwjesBxXixr17mKEVONYrxdPUdrIPwNz
Xb2ZqExNoN1+4z
5Z7qhpoD9+k2KDfSgTtTx+BVJsjqVTYj1vtkae+NSTMe
SSH3RtmgeBSs
GfZ5CyB6oMNEbej9GsSwJjW4Rpw2CXUKc3i1EN0zT
YOSBiQGAXkBAKH0 /6WwSQ==

;; Received 867 bytes from 192.5.5.241#53(f.root-servers.net) in 1756 ms

google.com. 172800 IN NS ns2.google.com.

google.com. 172800 IN NS ns1.google.com.

google.com. 172800 IN NS ns3.google.com.

google.com. 172800 IN NS ns4.google.com.

CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 86400 IN NSEC3 1 1 0 - CK0Q1GIN43N1ARRC9OSM6QPQR81H5M9A NS SOA RRSIG DNSKEY NSEC3PARAM

CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 86400 IN RRSIG NSEC3 8 2 86400 20161009044157 20161002033157 27452 com. M41sYMa1AlSgKf/CWelF3cJ4O2uGYGJEWlS1b8b2Wl

sMKCXnhK/rYlrb
FAtAWNcgyzdspmEEZtRcZqLj4x4Oizr3zHPz2EM18IPu
DsSdeIIHV70y
gwEnInozpTeqk1A0u/fVVSDpfcurgcZcW9bGbu74cLlg9
KZ+J2V//br1 +7w=

S84AE3BIT99DKIHQH27TRC0584HV5KOH.com.
86400 IN NSEC3 1 1 0 -
S84J17P3PT4RKMEJOHNGD73C5Q5NV5S9 NS DS
RRSIG

S84AE3BIT99DKIHQH27TRC0584HV5KOH.com.
86400 IN RRSIG NSEC3 8 2 86400 20161011044630
20161004033630 27452 com.
jS48lJO+/4fRTdvb//Mk+r9+MglfhwHagL11fhTbRJTMZ
8qSmEc9Jccw
ppRWsS2VDiyiemuMgC8ZzY4bhAMfiWx648BOgVWU
WVsh4m3Q6EewUuDO
ZT12d6l0RZR5O13SwrKFCBcgHrlI+up2UQuxG40UKZ
LJQP75R0Is2Wlo Tqk=

;; Received 665 bytes from 192.54.112.30#53(h.gtld-servers.net) in 1784 ms

maps.google.com. 300 IN A
172.217.17.142

;; Received 49 bytes from
216.239.32.10#53(ns1.google.com) in 1725 ms

[root@linuxfedora ~]#

پیکربندی سرویس DNS بصورت Master، Slave و Reverse

پس از بررسی مفاهیم اولیه DNS، فایل‌های مربوطه و همچنین پیکربندی، در این قسمت یک سناریوی عملی برای پیکربندی سرویس DNS بصورت Master، Slave و Reverse ارائه می‌دهیم.

My Testing Environment:

Master DNS Server

IP Address : 192.168.7.122

Host-name : masterdns.raja.com

OS : Centos 6.6 Final

Slave DNS Server

IP Address : 192.168.7.123

Host-name : slavedns.raja.com

OS : Centos 6.6 Final

Client Machine to use DNS

IP Address : 192.168.7.210

Host-name : node1.raja.com

OS : Centos 6.6 Final

Requirement Packages:

bind, bind-utils, bind-chroot

Configuration Files Used:

config file : /etc/named.conf

script file : /etc/init.d/named

Setup Master DNS Server

[root@linuxcent Desktop]# ifconfig eth0

eth0 Link encap:Ethernet HWaddr 00:0C:29:50:2E:DE

inet addr:192.168.7.122 Bcast:192.168.7.255 Mask:255.255.255.0

inet6 addr: fe80::20c:29ff:fe50:2ede/64 Scope:Link

UP BROADCAST RUNNING PROMISC MULTICAST MTU:1500 Metric:1

RX packets:8876 errors:0 dropped:0 overruns:0 frame:0

TX packets:2392 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:5333527 (5.0 MiB) TX bytes:198221 (193.5 KiB)

Interrupt:19 Base address:0x2000

[root@linuxcent Desktop]# hostname masterdns.raja.com

[root@masterdns Desktop]# hostname

masterdns.raja.com

[root@masterdns Desktop]#

[root@masterdns Desktop]# cat /etc/redhat-release

CentOS release 6.6 (Final)

[root@masterdns Desktop]# yum --skip-broken install bind* -y

Loaded plugins: aliases, changelog, downloadonly, fastestmirror, kabi, presto,

: refresh-packagekit, security, tmprepo, verify, versionlock

Loading support for CentOS kernel ABI

Setting up Install Process

Loading mirror speeds from cached hostfile

* base: mirrors.coreix.net

* epel: epel.scopesky.iq

* extras: mirrors.coreix.net

* remi: mirrors.netix.net

* rpmfusion-free-updates: kartolo.sby.datautama.net.id

* rpmfusion-nonfree-updates: kartolo.sby.datautama.net.id

* updates: mirrors.coreix.net

Resolving Dependencies

--> Running transaction check

---> Package bind.i686 32:9.8.2-0.30.rc1.el6 will be updated

---> Package bind.i686 32:9.8.2-0.47.rc1.el6_8.1 will be an update

---> Package bind-chroot.i686 32:9.8.2-0.30.rc1.el6 will be updated

---> Package bind-chroot.i686 32:9.8.2-0.47.rc1.el6_8.1 will be an update

---> Package bind-devel.i686 32:9.8.2-0.47.rc1.el6_8.1 will be installed

---> Package bind-dyndb-ldap.i686 0:2.3-5.el6 will be updated

---> Package bind-dyndb-ldap.i686 0:2.3-8.el6 will be an update

---> Package bind-libs.i686 32:9.8.2-0.30.rc1.el6 will be updated

---> Package bind-libs.i686 32:9.8.2-0.47.rc1.el6_8.1 will be an update

---> Package bind-license.noarch 32:9.9.4-18.el7 will be installed

---> Package bind-sdb.i686 32:9.8.2-0.47.rc1.el6_8.1 will be installed

---> Package bind-to-tinydns.i686 0:0.4.3-15.20140818gitdf0ddc3.el6 will be installed

---> Package bind-utils.i686 32:9.8.2-0.30.rc1.el6 will be updated

---> Package bind-utils.i686 32:9.8.2-0.47.rc1.el6_8.1 will be an update

--> Finished Dependency Resolution

Dependencies Resolved

```
================================================================================
 Package                 Arch          Version                      Repository  Size
================================================================================
Installing:
 bind-devel              i686          32:9.8.2-0.47.rc1.el6_8.1    updates    383 k
 bind-license            noarch        32:9.9.4-18.el7              c7-media    80 k
 bind-sdb                i686          32:9.8.2-0.47.rc1.el6_8.1    updates    313 k
 bind-to-tinydns         i686          0.4.3-15.20140818gitdf0ddc3.el6
                                                                    epel        18 k
Updating:
 bind                    i686          32:9.8.2-0.47.rc1.el6_8.1    updates    4.0 M
```

bind-chroot i686 32:9.8.2-0.47.rc1.el6_8.1 updates 75 k

bind-dyndb-ldap i686 2.3-8.el6 base 71 k

bind-libs i686 32:9.8.2-0.47.rc1.el6_8.1 updates 900 k

bind-utils i686 32:9.8.2-0.47.rc1.el6_8.1 updates 186 k

Transaction Summary

==========

==========

Install 4 Package(s)

Upgrade 5 Package(s)

Total download size: 6.0 M

Downloading Packages:

Setting up and reading Presto delta metadata

updates/prestodelta | 160 kB 00:02

Processing delta metadata

Package(s) data still to download: 6.0 M

(1/9): bind-9.8.2-0.47.rc1.el6_8.1.i686.rpm | 4.0 MB 02:27

(2/9): bind-chroot-9.8.2-0.47.rc1.el6_8.1.i686.rpm | 75 kB 00:00

(3/9): bind-devel-9.8.2-0.47.rc1.el6_8.1.i686.rpm | 383 kB 00:06

(4/9): bind-dyndb-ldap-2.3-8.el6.i686.rpm | 71 kB 00:00

(5/9): bind-libs-9.8.2-0.47.rc1.el6_8.1.i686.rpm | 900 kB 00:17

(7/9): bind-sdb-9.8.2-0.47.rc1.el6_8.1.i686.rpm | 313 kB 00:05

(8/9): bind-to-tinydns-0.4.3-15.20140818gitdf0ddc3.el6.i | 18 kB 00:00

(9/9): bind-utils-9.8.2-0.47.rc1.el6_8.1.i686.rpm | 186 kB 00:03

Total 33 kB/s | 6.0 MB 03:08

Running rpm_check_debug

Running Transaction Test

Transaction Test Succeeded

Running Transaction

Installing : 32:bind-license-9.9.4-18.el7.noarch 1/14

Updating : 32:bind-libs-9.8.2-0.47.rc1.el6_8.1.i686 2/14

Installing : 32:bind-devel-9.8.2-0.47.rc1.el6_8.1.i686 3/14

Updating : 32:bind-9.8.2-0.47.rc1.el6_8.1.i686 4/14

warning: /etc/named.conf created as /etc/named.conf.rpmnew

Updating : 32:bind-chroot-9.8.2-0.47.rc1.el6_8.1.i686 5/14

Updating : bind-dyndb-ldap-2.3-8.el6.i686 6/14

Installing : 32:bind-sdb-9.8.2-0.47.rc1.el6_8.1.i686 7/14

Updating : 32:bind-utils-9.8.2-0.47.rc1.el6_8.1.i686 8/14

Installing : bind-to-tinydns-0.4.3-15.20140818gitdf0ddc3.el6.i686 9/14

Cleanup : bind-dyndb-ldap-2.3-5.el6.i686 10/14

Cleanup : 32:bind-chroot-9.8.2-0.30.rc1.el6.i686 11/14

Cleanup : 32:bind-9.8.2-0.30.rc1.el6.i686 12/14

Cleanup : 32:bind-utils-9.8.2-0.30.rc1.el6.i686 13/14

Cleanup : 32:bind-libs-9.8.2-0.30.rc1.el6.i686 14/14

Verifying : 32:bind-sdb-9.8.2-0.47.rc1.el6_8.1.i686 1/14

Verifying : 32:bind-license-9.9.4-18.el7.noarch 2/14

Verifying : bind-to-tinydns-0.4.3-15.20140818gitdf0ddc3.el6.i686 3/14

Verifying : 32:bind-9.8.2-0.47.rc1.el6_8.1.i686 4/14

Verifying : bind-dyndb-ldap-2.3-8.el6.i686 5/14

Verifying : 32:bind-libs-9.8.2-0.47.rc1.el6_8.1.i686 6/14

Verifying : 32:bind-utils-9.8.2-0.47.rc1.el6_8.1.i686 7/14

Verifying : 32:bind-chroot-9.8.2-0.47.rc1.el6_8.1.i686 8/14

Verifying : 32:bind-devel-9.8.2-0.47.rc1.el6_8.1.i686 9/14

Verifying : 32:bind-libs-9.8.2-0.30.rc1.el6.i686 10/14

Verifying : 32:bind-chroot-9.8.2-0.30.rc1.el6.i686 11/14

Verifying : 32:bind-9.8.2-0.30.rc1.el6.i686 12/14

Verifying : bind-dyndb-ldap-2.3-5.el6.i686 13/14

Verifying : 32:bind-utils-9.8.2-0.30.rc1.el6.i686 14/14

Installed:

bind-devel.i686 32:9.8.2-0.47.rc1.el6_8.1

bind-license.noarch 32:9.9.4-18.el7

bind-sdb.i686 32:9.8.2-0.47.rc1.el6_8.1

bind-to-tinydns.i686 0:0.4.3-15.20140818gitdf0ddc3.el6

Updated:

bind.i686 32:9.8.2-0.47.rc1.el6_8.1

bind-chroot.i686 32:9.8.2-0.47.rc1.el6_8.1

bind-dyndb-ldap.i686 0:2.3-8.el6

bind-libs.i686 32:9.8.2-0.47.rc1.el6_8.1

bind-utils.i686 32:9.8.2-0.47.rc1.el6_8.1

Complete!

[root@masterdns Desktop]#

Installing and Configuring Bind

[root@masterdns Desktop]# vim /etc/named.conf

[root@masterdns Desktop]# cat /etc/named.conf

//

// named.conf

//

// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS

// server as a caching only nameserver (as a localhost DNS resolver only).

//

// See /usr/share/doc/bind*/sample/ for example named configuration files.

//

```
options {
        listen-on port 53 { 127.0.0.1; 192.168.7.122; };#Here we need to add our DNS Server IP or Master DNS Server
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
      statistics-file "/var/named/data/named_stats.txt";
      memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { localhost; 192.168.7.0/24; };# subnet range where my hosts are allowed to query our DNS
        #allow-transfer  { localhost; 192.168.7.123; }; # Here we need to our Slave DNS server IP.
        recursion no;

        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;

        /* Path to ISC DLV key */
```

```
        bindkeys-file "/etc/named.iscdlv.key";

        managed-keys-directory "/var/named/dynamic";
};

logging {
      channel default_debug {
            file "data/named.run";
            severity dynamic;
      };
};

# Note: If you want to your DNS Server able to ask root DNS Server Uncomment Bellow lines and set reursion to yes.
#zone "." IN {
#       type hint;
#       file "named.ca";
#};
```

```
zone "raja.com" IN {
        type master;
        file "raja.com.zone";
        allow-update { none; };
        allow-transfer { none; };
};

# Note: if you want to have reverse zone uncomment bellow lines.
#zone "7.168.192.in-addr.arpa" IN {
#       type master;
#       file "raja.com.rev.zone";
#       allow-update { none; };
#};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";

[root@masterdns Desktop]#
```

```
[root@masterdns Desktop]# cat /var/named/named.localhost
$TTL 1D
@       IN SOA  @ rname.invalid. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      @
        A       127.0.0.1
        AAAA    ::1
[root@masterdns Desktop]# cat /var/named/named.loopback
$TTL 1D
@       IN SOA  @ rname.invalid. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
```

```
        NS      @
        A       127.0.0.1
        AAAA    ::1
        PTR     localhost.
[root@masterdns Desktop]#
```

```
cp /var/named/named.localhost /var/named/raja.com.zone
cp /var/named/named.loopback /var/named/raja.com.rev.zone
```

```
vim /var/named/raja.com.zone
$TTL 86400
@       IN SOA  masterdns.raja.com.     root.raja.com. (
2016060601    ; serial
3600    ; refresh
1800    ; retry
604800    ; expire
86400 )  ; minimum
; Name server's
@       IN      NS      masterdns.raja.com.
```

#Note:if you have slave name server uncomment the followed commented line

#@ IN NS slavedns.raja.com.

; Name server hostname to IP resolve.

@ IN A 192.168.7.122

#@ IN A 192.168.7.123

; Hosts in this Domain

@ IN A 192.168.7.210

@ IN A 192.168.7.220

masterdns IN A 192.168.7.122

#slavedns IN A 192.168.7.123

node1 IN A 192.168.0.210

rhel1 IN A 192.168.0.220

$TTL 86400

[root@masterdns Desktop]# vim /var/named/raja.com.rev.zone

[root@masterdns Desktop]# cat /var/named/raja.com.rev.zone

$TTL 86400

@ IN SOA masterdns.raja.com. root.raja.com. (

```
2016060602      ; serial
3600      ; refresh
1800      ; retry
604800      ; expire
86400 )    ; minimum
; Name server's
@       IN      NS      masterdns.raja.com.
@       IN      NS      slavedns.raja.com.
@       IN      PTR     raja.com.
; Name server hostname to IP resolve.
masterdns       IN      A       192.168.7.122
slavedns        IN      A       192.168.7.123
;Hosts in Domain
node1           IN      A       192.168.0.210
rhel            IN      A       192.168.0.220
122             IN      PTR     masterdns.raja.com.
123             IN      PTR     slavedns.raja.com.
210             IN      PTR     node1.raja.com.
220             IN      PTR     rhel1.raja.com.
[root@masterdns Desktop]#
```

#####Check the group ownership of forward look-up & reverse look-up files, before checking for any errors in configuration.

[root@masterdns Desktop]# ls -l /var/named/

total 44

drwxr-x---. 6 root named 4096 Sep 28 14:21 chroot

drwxrwx---. 2 named named 4096 Oct 6 14:40 data

drwxrwx---. 2 named named 4096 Oct 6 20:12 dynamic

-rw-r--r-- 1 root root 1287 May 11 2013 linuxcbt.internal.zone

-rw-r----- 1 root named 3171 Jan 11 2016 named.ca

-rw-r----- 1 root named 152 Dec 15 2009 named.empty

-rw-r----- 1 root named 152 Jun 21 2007 named.localhost

-rw-r----- 1 root named 168 Dec 15 2009 named.loopback

-rw-r--r-- 1 root root 745 Oct 6 21:02 raja.com.rev.zone

-rw-r--r-- 1 root root 742 Oct 6 20:58 raja.com.zone

drwxrwx---. 2 named named 4096 Sep 28 14:21 slaves

[root@masterdns Desktop]#

####Here we can see both the files are in root users ownership, because files which we makes a copy from sample files are available under /var/named/. Change the group to named on both files using following commands.

[root@masterdns Desktop]# chgrp named /var/named/raja.com.rev.zone

[root@masterdns Desktop]# chgrp named /var/named/raja.com.zone

[root@masterdns Desktop]# ls -l /var/named/

total 44

drwxr-x---. 6 root named 4096 Sep 28 14:21 chroot

drwxrwx---. 2 named named 4096 Oct 6 14:40 data

drwxrwx---. 2 named named 4096 Oct 6 20:12 dynamic

-rw-r--r-- 1 root root 1287 May 11 2013 linuxcbt.internal.zone

-rw-r----- 1 root named 3171 Jan 11 2016 named.ca

-rw-r----- 1 root named 152 Dec 15 2009 named.empty

-rw-r----- 1 root named 152 Jun 21 2007 named.localhost

-rw-r----- 1 root named 168 Dec 15 2009 named.loopback

-rw-r--r-- 1 root named 745 Oct 6 21:02 raja.com.rev.zone

-rw-r--r-- 1 root named 742 Oct 6 20:58 raja.com.zone

drwxrwx---. 2 named named 4096 Sep 28 14:21 slaves

[root@masterdns Desktop]#

#####Now, check for the errors in zone files, before starting the DNS service. First check the named.conf file, then check other zone files.

[root@masterdns Desktop]# named-checkconf /etc/named.conf

[root@masterdns Desktop]# echo $?

0

[root@masterdns Desktop]# named-checkzone masterdns.raja.com /var/named/raja.com.zone

/var/named/raja.com.zone:10: unknown RR type 'you'

/var/named/raja.com.zone:14: #\@.masterdns.raja.com: bad owner name (check-names)

/var/named/raja.com.zone:19: #slavedns.masterdns.raja.com: bad owner name (check-names)

zone masterdns.raja.com/IN: loading from master file /var/named/raja.com.zone failed: unknown class/type

zone masterdns.raja.com/IN: not loaded due to errors.

```
[root@masterdns Desktop]#

[root@masterdns Desktop]# vim /var/named/raja.com.zone
[root@masterdns Desktop]# cat /var/named/raja.com.zone
$TTL 86400
@       IN SOA  masterdns.raja.com.     root.raja.com. (
2016060601    ; serial
3600    ; refresh
1800    ; retry
604800    ; expire
86400 )  ; minimum
; Name server's
@       IN      NS      masterdns.raja.com.
; Name server hostname to IP resolve.
@       IN      A       192.168.7.122
; Hosts in this Domain
@       IN      A       192.168.7.210
@       IN      A       192.168.7.220
masterdns       IN      A       192.168.7.122
```

node1 IN A 192.168.7.210

rhel1 IN A 192.168.7.220

[root@masterdns Desktop]#

[root@masterdns Desktop]# named-checkzone masterdns.raja.com /var/named/raja.com.zone

zone masterdns.raja.com/IN: loaded serial 2016060601

OK

[root@masterdns Desktop]#

[root@masterdns Desktop]# named-checkzone masterdns.raja.com /var/named/raja.com.rev.zone

zone masterdns.raja.com/IN: NS 'masterdns.raja.com' has no address records (A or AAAA)

zone masterdns.raja.com/IN: not loaded due to errors.

[root@masterdns Desktop]#

Note: Solve The problem same to prior

#####By default iptables was running and our DNS server is restricted to localhost, if client wants to resolve name from our DNS Server, then we have to allow the inbound

request, for that we need to add iptables inbound rule for the port 53.

[root@masterdns Desktop]# iptables -I INPUT -p udp --dport 53 -m state --state NEW -j ACCEPT

[root@masterdns Desktop]# iptables -L INPUT

Chain INPUT (policy ACCEPT)

target prot opt source destination

ACCEPT udp -- anywhere anywhere udp dpt:domain state NEW

ACCEPT udp -- anywhere anywhere udp dpt:domain

ACCEPT tcp -- anywhere anywhere tcp dpt:domain

ACCEPT udp -- anywhere anywhere udp dpt:bootps

ACCEPT tcp -- anywhere anywhere tcp dpt:bootps

ACCEPT all -- anywhere anywhere state RELATED,ESTABLISHED

ACCEPT icmp -- anywhere anywhere

ACCEPT all -- anywhere anywhere

ACCEPT tcp -- anywhere anywhere
state NEW tcp dpt:ssh

ACCEPT tcp -- anywhere anywhere
state NEW tcp dpt:smtp

ACCEPT tcp -- anywhere anywhere
state NEW tcp dpt:pop3

ACCEPT udp -- anywhere anywhere
state NEW udp dpt:ipp

ACCEPT udp -- anywhere 224.0.0.251
state NEW udp dpt:mdns

ACCEPT tcp -- anywhere anywhere
state NEW tcp dpt:ipp

ACCEPT udp -- anywhere anywhere
state NEW udp dpt:ipp

ACCEPT tcp -- anywhere anywhere
state NEW tcp dpt:http

ACCEPT tcp -- anywhere anywhere
state NEW tcp dpt:https

REJECT all -- anywhere anywhere
reject-with icmp-host-prohibited

[root@masterdns Desktop]# service iptables save

iptables: Saving firewall rules to /etc/sysconfig/iptables:[
OK]

[root@masterdns Desktop]# service iptables restart

iptables: Setting chains to policy ACCEPT: nat mangle filte[OK]

iptables: Flushing firewall rules: [OK]

iptables: Unloading modules: [OK]

iptables: Applying firewall rules: [OK]

[root@masterdns Desktop]#

Start the named service and make it persistent.

[root@masterdns Desktop]# service named start

Starting named: named: already running [OK]

[root@masterdns Desktop]# service named restart

Stopping named: .umount: /var/named/chroot/var/named: device is busy.

(In some cases useful info about processes that use

the device is found by lsof(8) or fuser(1))

[OK]

Starting named: [OK]

[root@masterdns Desktop]# chkconfig named on

[root@masterdns Desktop]# chkconfig --list named

named 0:off 1:off 2:on 3:on 4:on 5:on 6:off

[root@masterdns Desktop]#

Finally, test the configured Master DNS zone files (forward and reverse), using dig & nslookup tools.

[root@masterdns Desktop]# vim /etc/resolv.conf

[root@masterdns Desktop]# cat /etc/resolv.conf

Generated by NetworkManager

search linuxcbt.internal

nameserver 192.168.7.122

#nameserver 8.8.8.8

[root@masterdns Desktop]#

[root@masterdns Desktop]# dig masterdns.raja.com

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.47.rc1.el6_8.1 <<>> masterdns.raja.com

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25252

;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; WARNING: recursion requested but not available

;; QUESTION SECTION:

;masterdns.raja.com. IN A

;; ANSWER SECTION:

masterdns.raja.com. 86400 IN A
192.168.7.122

;; AUTHORITY SECTION:

raja.com. 86400 IN NS
masterdns.raja.com.

;; Query time: 43 msec

;; SERVER: 192.168.7.122#53(192.168.7.122)

;; WHEN: Thu Oct 6 21:20:28 2016

;; MSG SIZE rcvd: 66

[root@masterdns Desktop]#

Reverse Query

```
[root@masterdns Desktop]# dig -x 192.168.7.122

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.47.rc1.el6_8.1 <<>>
-x 192.168.7.122
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED,
id: 16320
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0,
ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;122.7.168.192.in-addr.arpa.   IN        PTR

;; Query time: 16 msec
;; SERVER: 192.168.7.122#53(192.168.7.122)
;; WHEN: Thu Oct  6 21:21:34 2016
;; MSG SIZE  rcvd: 44
```

```
[root@masterdns Desktop]#

[root@masterdns Desktop]# nslookup raja.com
Server:         192.168.7.122
Address:        192.168.7.122#53

Name: raja.com
Address: 192.168.7.220
Name: raja.com
Address: 192.168.7.122
Name: raja.com
Address: 192.168.7.210

[root@masterdns Desktop]# nslookup masterdns.raja.com
Server:         192.168.7.122
Address:        192.168.7.122#53

Name: masterdns.raja.com
Address: 192.168.7.122

[root@masterdns Desktop]#
```

Setup Slave DNS Server

In Slave machine, also we need to install same bind packages as shown in Master, so let's install them using following command.

$ sudo yum install bind* -y

$ sudo vim /etc/named.conf

Make changes as shown, as per your requirements.

//

// named.conf

//

// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS

// server as a caching only nameserver (as a localhost DNS resolver only).

//

// See /usr/share/doc/bind*/sample/ for example named configuration files.

//

```
options {
listen-on port 53 { 127.0.0.1; 192.168.7.123}; # Our Slave DNS server IP
listen-on-v6 port 53 { ::1; };
directory       "/var/named";
dump-file       "/var/named/data/cache_dump.db";
statistics-file "/var/named/data/named_stats.txt";
memstatistics-file "/var/named/data/named_mem_stats.txt";
allow-query     { localhost; 192.168.7.0/24; };
recursion no;
dnssec-enable yes;
dnssec-validation yes;
dnssec-lookaside auto;
/* Path to ISC DLV key */
bindkeys-file "/etc/named.iscdlv.key";
managed-keys-directory "/var/named/dynamic";
};
logging {
channel default_debug {
file "data/named.run";
```

```
severity dynamic;
};
};
zone "." IN {
type hint;
file "named.ca";
};
## Define our slave forward and reverse zone, Zone files are replicated from master.
zone"raja.com" IN {
type slave;
file "slaves/raja.com.zone";
masters { 192.168.7.122; };
};
zone"7.168.192.in-addr.arpa" IN {
type slave;
file "slaves/raja.com.rev.zone";
masters { 192.168.7.122; };
};
#####
include "/etc/named.rfc1912.zones";
```

include "/etc/named.root.key";

$ sudo service named start

$ sudo ls -l /var/named/slaves

$ sudo cat /var/named/slaves/raja.com.zone

$ sudo cat /var/named/slaves/raja.com.rev.zone

$ sudo iptables -I INPUT -p udp --dport 53 -m state --state NEW -j ACCEPT

Save the iptables rules and restart the iptables service.

$ sudo service iptables save

$ sudo service iptables restart

Make the service persistent on system boot.

$ sudo chkconfig iptables on

Check whether persistent set for run-levels .

$ sudo chkconfig --list iptables

Configure Client Machine

In client side we need to assign the Primary (192.168.7.122) and Secondary DNS (192.168.7.123) entry in network settings to get assign a hostname.

$ vim /etc/resolv.conf

search raja.com

nameserver 192.168.7.122

nameserver 192.168.7.123

$ ifconfig | grep inet

$ hostname

$ nslookup raja.com

Now, check the forward & Reverse DNS look-up using.

$ dig masterdns.raja.com

$ dig -x 192.168.7.122

Jail یا chroot کردن DNS Server

مسئله مهمی که از نظر امنیتی در پیکربندی سرور DNS وجـود دارد ایمن نمودن DNS Server می‌باشد. یکی از راه‌های ایمن نمودن DNS Server انجام عملیات chroot یا Jail کـردن آن مـی‌باشـد. Chroot در لینوکس، عملیاتی است که دایرکتوری ریشه یا هر دایرکتـوری دیگـری را برای فرآیند در حال اجرا به همراه تمام زیرمجموعه هـای دایرکتـوری بـه دایرکتوری دیگر منتقل می‌کند (تمام فرآیندها و وابستگی‌ها). وقتی مکان یک دایرکتوری را به دایرکتوری دیگر تغییر می‌دهید، دیگر به دستورات و فایـل‌هـای خـارج از آن دایرکتـوری دسترسـی ندارید. ایـن دایرکتـوری chroot jail یا زندان chroot خوانده مـی‌شـود. Jail یـا chroot کـردن DNS Server باعث می‌شود از بسیاری از حملات در امان باشد.

در ادامه پیکربنـدی chroot jail بـر روی DNS Server ارائـه شـده است که توجه خوانندگان عزیز را به آن جلب می‌نماییم:

[root@masterdns ~]# cat /etc/sysconfig/named | grep ROOTDIR

ROOTDIR="/var/named/chroot" -- will run named in a chroot environment.

empty in the ROOTDIR directory. It will simplify maintenance of your

at startup. Don't add -t here, use ROOTDIR instead.

ROOTDIR=/var/named/chroot

[root@masterdns ~]# vim /etc/sysconfig/named

1. Install Bind-Chroot :

[root@CentOS63 ~]# yum install bind-chroot bind -y

2. Copy all bind related files to prepare bind chrooted environments :

[root@CentOS63 ~]# cp -R /usr/share/doc/bind-*/sample/var/named/* /var/named/chroot/var/named/

3. Create bind related files into chrooted directory :

[root@CentOS63 ~]# touch /var/named/chroot/var/named/data/cache_dump.db

[root@CentOS63 ~]# touch /var/named/chroot/var/named/data/named_stats.txt

[root@CentOS63 ~]# touch /var/named/chroot/var/named/data/named_mem_stats.txt

[root@CentOS63 ~]# touch /var/named/chroot/var/named/data/named.run

[root@CentOS63 ~]# mkdir /var/named/chroot/var/named/dynamic

[root@CentOS63 ~]# touch /var/named/chroot/var/named/dynamic/managed-keys.bind

4. Bind lock file should be writeable, therefore set the permission to make it writable as below :

[root@CentOS63 ~]# chmod -R 777 /var/named/chroot/var/named/data

[root@CentOS63 ~]# chmod -R 777 /var/named/chroot/var/named/dynamic

5. Set if you do not use IPv6 :

[root@CentOS63 ~]# echo 'OPTIONS="-4"' >> /etc/sysconfig/named

6. Configure main bind configuration in /etc/named.conf. Append the ehowstuff.local information to the file :

[root@CentOS63 ~]# vi /var/named/chroot/etc/named.conf

//

// named.conf

//

```
// Provided by Red Hat bind package to configure the ISC
BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS
resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named
configuration files.
//

options {
        listen-on port 53 { 127.0.0.1;192.168.2.58; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file
"/var/named/data/named_mem_stats.txt";
        allow-query     { localhost; };
        recursion yes;

        dnssec-enable yes;
        dnssec-validation yes;
```

```
        dnssec-lookaside auto;

        /* Path to ISC DLV key */
        bindkeys-file "/etc/named.iscdlv.key";

        managed-keys-directory "/var/named/dynamic";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};

zone "ehowstuff.local" {
```

```
    type master;
    file "ehowstuff.local.zone";
};
zone "2.168.192.in-addr.arpa" IN {
        type master;
        file "192.168.2.zone";
};

include "/etc/rndc.key";
include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

Execution:

```
[root@masterdns ~]# cp /etc/named.conf /var/named/chroot/etc/
```

7. Create Forward and Reverse zone files for domain ehowstuff.local.

a) Create Forward Zone :

[root@CentOS63 ~]# vi /var/named/chroot/var/named/ehowstuff.local.zone

```
;
;       Addresses and other host information.
;
$TTL 86400
@               IN      SOA     ehowstuff.local. hostmaster.ehowstuff.local. (
                                2013022401      ; Serial
                                43200           ; Refresh
                                3600            ; Retry
                                3600000         ; Expire
                                2592000 )       ; Minimum

;       Define the nameservers and the mail servers

                IN      NS      ns.ehowstuff.local.
                IN      A       192.168.2.58
                IN      MX      10 mail.ehowstuff.local.
```

```
mail        IN    A     192.168.2.58
ns          IN    A     192.168.2.58
```

b) Create Reverse Zone :

```
[root@CentOS63 ~]# vi /var/named/chroot/var/named/192.168.2.zone

;
;       Addresses and other host information.
;
$TTL 86400
@           IN      SOA     ehowstuff.local. hostmaster.ehowstuff.local. (
                            2013022402      ; Serial
                            43200       ; Refresh
                            3600        ; Retry
                            3600000     ; Expire
                            2592000 )   ; Minimum
```

2.168.192.in-addr.arpa. IN NS centos63.ehowstuff.local.

58.2.168.192.in-addr.arpa. IN PTR mail.ehowstuff.local.

58.2.168.192.in-addr.arpa. IN PTR ns.ehowstuff.local.

[root@masterdns ~]# cd /var/named/

[root@masterdns named]# ls

chroot linuxcbt.internal.zone named.ca named.loopback slaves

data my.external.zone.db named.empty raja.com.rev.zone

dynamic my.internal.zone.db named.localhost raja.com.zone

[root@masterdns named]# cp raja.com.zone chroot/

dev/ etc/ usr/ var/

[root@masterdns named]# cp raja.com.zone chroot/var/named/

cp: `raja.com.zone' and `chroot/var/named/raja.com.zone' are the same file

[root@masterdns named]# cp raja.com.rev.zone chroot/var/named/

cp: `raja.com.rev.zone' and `chroot/var/named/raja.com.rev.zone' are the same file

[root@masterdns named]#

8. RHEL 6 and CentOS 6 apparently no longer generates the rndc.key during installation. Instead, the key is automatically generated on the first start of named service.

Start Bind service :

[root@CentOS6 ~]# service named start

Generating /etc/rndc.key: [OK]

Starting named: [OK]

9. Configure Bind auto start at boot :

[root@CentOS63 ~]# chkconfig --levels 235 named on

10. Verifying permissions and ownership. Created the files required inside the jail, but the matter of setting the permissions and ownership should remains.

Go to chroot/var/named/ directory :

[root@CentOS63 ~]# cd /var/named/chroot/var/named/

Change owner as below :

[root@CentOS63 named]# chown root:named ehowstuff.local.zone

[root@CentOS63 named]# chown root:named 192.168.2.zone

[root@CentOS63 named]# chown root:named my.external.zone.db

[root@CentOS63 named]# chown root:named my.internal.zone.db

[root@CentOS63 named]# chown root:named named.ca

[root@CentOS63 named]# chown root:named named.localhost

[root@CentOS63 named]# chown root:named named.loopback

Verify permissions and ownership rest of the chrooted directories :

```
[root@CentOS63 ~]# ll /var/named/

total 32
drwxr-x--- 6 root  named 4096 Feb 24 13:51 chroot
drwxrwx--- 2 named named 4096 Dec  7 04:49 data
drwxrwx--- 2 named named 4096 Dec  7 04:49 dynamic
-rw-r----- 1 root  named 1892 Feb 18  2008 named.ca
-rw-r----- 1 root  named  152 Dec 15  2009 named.empty
-rw-r----- 1 root  named  152 Jun 21  2007 named.localhost
-rw-r----- 1 root  named  168 Dec 15  2009 named.loopback
drwxrwx--- 2 named named 4096 Dec  7 04:49 slaves

[root@CentOS63 ~]# ll /var/named/chroot/

total 16
drwxr-x--- 2 root named 4096 Feb 24 13:51 dev
drwxr-x--- 4 root named 4096 Feb 24 14:40 etc
drwxr-x--- 3 root named 4096 Feb 24 13:51 usr
drwxr-x--- 6 root named 4096 Feb 24 13:51 var
```

```
[root@CentOS63 ~]# ll /var/named/chroot/etc

total 32
-rw-r--r-- 1 root root   372 Feb 20 06:51 localtime
drwxr-x--- 2 root named 4096 Dec  7 04:49 named
-rw-r--r-- 1 root named 1201 Feb 24 14:16 named.conf
-rw-r--r-- 1 root named 2389 Dec  7 04:49 named.iscdlv.key
-rw-r----- 1 root named  931 Jun 21  2007 named.rfc1912.zones
-rw-r--r-- 1 root named  487 Jul 19  2010 named.root.key
drwxr-x--- 3 root named 4096 Feb 24 13:51 pki
-rw-r----- 1 root named   77 Feb 24 14:00 rndc.key

[root@CentOS63 ~]# ll /var/named/chroot/var/named/

total 44
-rw-r-xr-x 1 root named  551 Feb 24 15:28 192.168.2.zone
drwxrwxrwx 2 named named 4096 Feb 24 14:04 data
```

drwxrwxrwx 2 named named 4096 Feb 24 15:30 dynamic

-rw-r-xr-x 1 root named 681 Feb 24 15:28 ehowstuff.local.zone

-rw-r--r-- 1 root named 56 Feb 24 13:54 my.external.zone.db

-rw-r--r-- 1 root named 56 Feb 24 13:54 my.internal.zone.db

-rw-r--r-- 1 root named 1892 Feb 24 13:54 named.ca

-rw-r--r-- 1 root root 152 Feb 24 13:54 named.empty

-rw-r--r-- 1 root named 152 Feb 24 13:54 named.localhost

-rw-r--r-- 1 root named 168 Feb 24 13:54 named.loopback

drwxr-xr-x 2 named named 4096 Feb 24 13:54 slaves

11. Test and make sure it’s working.

[root@CentOS63 ~]# host -t mx ehowstuff.local

ehowstuff.local mail is handled by 10 mail.ehowstuff.local.

[root@CentOS63 ~]# nslookup

> set type=any

> ehowstuff.local

Server: 192.168.2.58

Address: 192.168.2.58#53

ehowstuff.local

origin = ehowstuff.local

mail addr = hostmaster.ehowstuff.local

serial = 2013023401

refresh = 43200

retry = 3600

expire = 3600000

minimum = 2592000

ehowstuff.local nameserver = ns.ehowstuff.local.

Name: ehowstuff.local

Address: 192.168.2.58

ehowstuff.local mail exchanger = 10 mail.ehowstuff.local.

12. If your server does not have nslookup, host or dig command, then you should install bind-utils. All this utilities are the friendly and useful utilities to test and diagnose the DNS issue.

```
[root@CentOS6 ~]# yum install bind-utils
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: centos.biz.net.id
 * extras: centos.biz.net.id
 * updates: centos.biz.net.id
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package bind-utils.x86_64 32:9.8.2-0.10.rc1.el6_3.6 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
================================================================================
 Package                 Arch                 Version
Repository          Size
```

```
================================================================================
================================================================================
================================================================================
Installing:
 bind-utils                  x86_64                  32:9.8.2-
0.10.rc1.el6_3.6             updates                 182 k

Transaction Summary
================================================================================
================================================================================
================================================================================
Install       1 Package(s)

Total download size: 182 k
Installed size: 438 k
Is this ok [y/N]: y
Downloading Packages:
bind-utils-9.8.2-0.10.rc1.el6_3.6.x86_64.rpm
| 182 kB     00:02
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
```

Running Transaction

Installing : 32:bind-utils-9.8.2-0.10.rc1.el6_3.6.x86_64 1/1

Verifying : 32:bind-utils-9.8.2-0.10.rc1.el6_3.6.x86_64 1/1

Installed:

bind-utils.x86_64 32:9.8.2-0.10.rc1.el6_3.6

Complete!

[root@masterdns named]# ps -aux | grep named

Warning: bad syntax, perhaps a bogus '-'? See /usr/share/doc/procps-3.2.8/FAQ

named 8548 0.1 0.9 66072 9908 ? Ssl 19:54 0:01 /usr/sbin/named-sdb -u named -4 -t /var/named/chroot

root 9164 0.0 0.0 4352 732 pts/0 S+ 20:08 0:00 grep named

[root@masterdns named]#