

Linux Server (for Centos7.X)

- DNS -

Copyright @ 2016 MajunSoft co.,Ltd

소 속	IDC실
이 름	신용우 매니저
E-mail	tech@tongkni.co.kr

통큰아이

INDEX

- 1. 개요 3
- 2. DNS 서버 구축하기. 4
 - 2.1 DNS 구축에 필요한 프로그램 설치. 4
 - 2.2 DNS 설정. 5
 - 2.3 호스트 추가. (zone 파일 생성) 7
 - 2.4 상위기관에 네임서버 등록.(네임호스트 추가) 11
- 3. 활용 - 레코드 값의 정의와 설정. 15

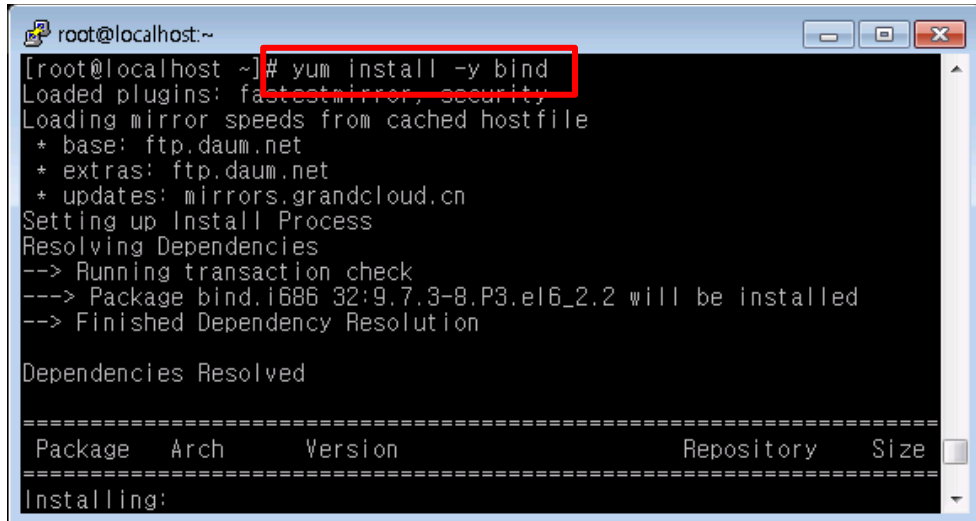
1. 개요.

- DNS(Domain Name System)는 원하는 서버에 접근하기 위해 입력한 알기 쉬운 문자로 된 도메인 주소를 컴퓨터가 처리할 수 있는 IP주소로 변환시켜주는 서비스입니다. 이러한 서비스를 제공하는 서버를 네임서버라고 합니다.
- 본인 소유의 서버를 네임서버로 이용하려면 현재 소유하고 있는 도메인이 있어야 합니다. 도메인을 등록한 업체를 통하여 네임서버 호스트 등록을 하면 도메인 등록 업체에서는 이에 대한 정보를 업데이트하여 최상위 기관에서도 조회할 수 있도록 조치하며, 이러한 절차를 거치고 나면 비로소 네임서버로 사용할 수 있습니다. (챕터 2.4)
- 네임서버를 구축하는 절차는 아래와 같습니다.
 - 1 DNS 구축에 필요한 프로그램 설치.
 - 2 DNS 설정.
 - 3 호스트 추가하기.
 - 4 상위 기관에 네임서버 등록하기.(네임 호스트 추가)..
- 본 매뉴얼은 DNS 서비스를 하기 위한 DNS 설치 및 구축 방법에 대해 작성되었습니다.

2. DNS 서버 구축하기.

2.1 DNS 구축에 필요한 프로그램 설치.

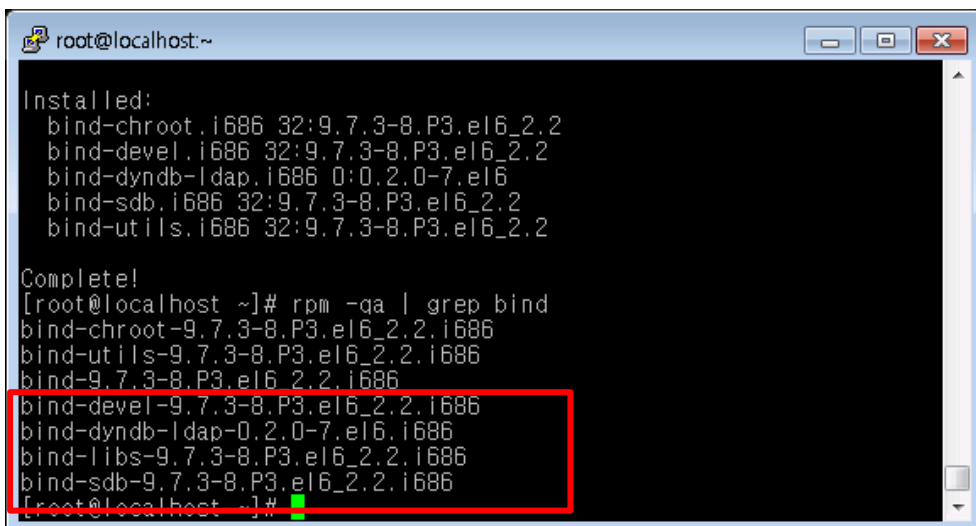
- 1 DNS 구축을 위해 bind 관련 패키지를 설치해야 합니다. yum을 이용하여 설치합니다.
→ yum install -y bind*



```
root@localhost:~  
[root@localhost ~]# yum install -y bind  
Loaded plugins: fastestmirror, security  
Loading mirror speeds from cached hostfile  
* base: ftp.daum.net  
* extras: ftp.daum.net  
* updates: mirrors.grandcloud.cn  
Setting up Install Process  
Resolving Dependencies  
--> Running transaction check  
---> Package bind.i686 32:9.7.3-8.P3.el6_2.2 will be installed  
--> Finished Dependency Resolution  
  
Dependencies Resolved  
  
=====
```

Package	Arch	Version	Repository	Size
Installing:				

- 2 bind가 정상적으로 설치되었는지 확인합니다.
→ rpm -qa | grep bind

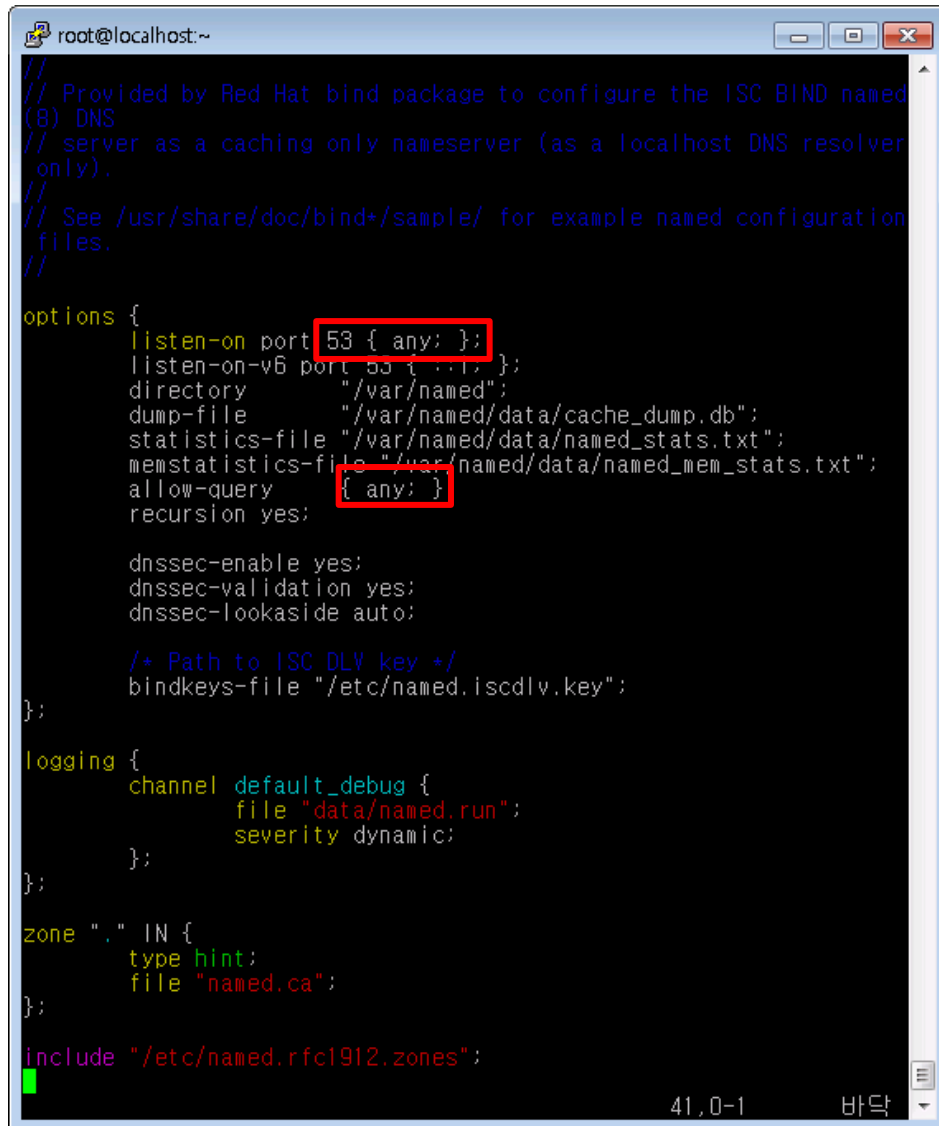


```
root@localhost:~  
Installed:  
bind-chroot.i686 32:9.7.3-8.P3.el6_2.2  
bind-devel.i686 32:9.7.3-8.P3.el6_2.2  
bind-dyndb-ldap.i686 0:0.2.0-7.el6  
bind-sdb.i686 32:9.7.3-8.P3.el6_2.2  
bind-utils.i686 32:9.7.3-8.P3.el6_2.2  
  
Complete!  
[root@localhost ~]# rpm -qa | grep bind  
bind-chroot-9.7.3-8.P3.el6_2.2.i686  
bind-utils-9.7.3-8.P3.el6_2.2.i686  
bind-9.7.3-8.P3.el6_2.2.i686  
bind-devel-9.7.3-8.P3.el6_2.2.i686  
bind-dyndb-ldap-0.2.0-7.el6.i686  
bind-libs-9.7.3-8.P3.el6_2.2.i686  
bind-sdb-9.7.3-8.P3.el6_2.2.i686  
[root@localhost ~]#
```

2.2 DNS 설정.

1 /etc/named.conf 는 네임서버의 기본적인 설정을 담당합니다. /etc/named.conf 파일을 vi편집기로 열어 빨간 글씨 부분을 수정합니다.

- vim /etc/named.conf
listen-on port **53** { any; };
allow-query { **any**; };



```
root@localhost:~
// 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 { any; };
listen-on-v6 port 53 { ::: };
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 { any; };
recursion yes;

dnsssec-enable yes;
dnsssec-validation yes;
dnsssec-lookaside auto;

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

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

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

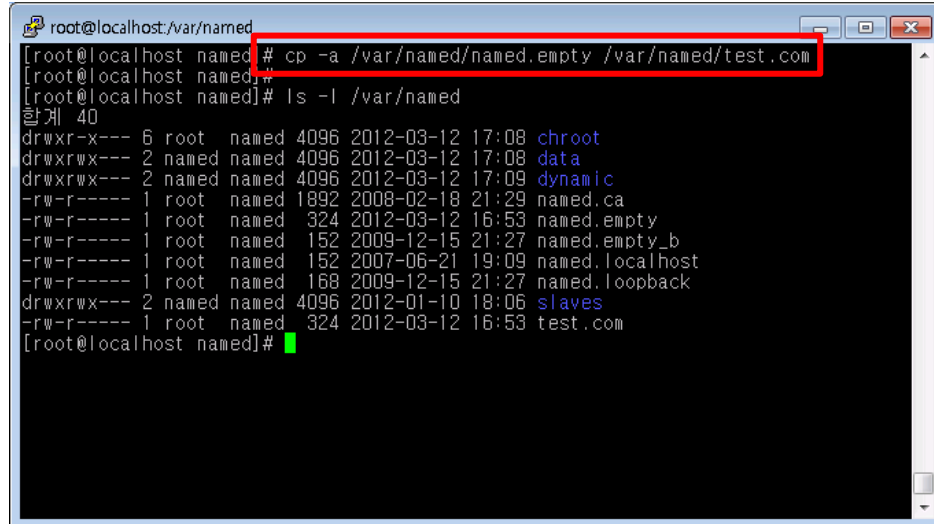
include "/etc/named.rfc1912.zones";
41,0-1 바닥
```

2 /etc/named.rfc1912.zones 는 zone 파일(실제로 도메인 주소와 IP 등의 정보를 설정한 파일)의 위치 및 zone 영역에 대한 설정을 담당합니다. 예를 들어 test.com 이란 도메인을 추가할 경우 설정에 아래 양식처럼 추가하고 저장합니다.

- vim /etc/named.rfc1912.zones
zone "**test.com**" IN {
type **master**;

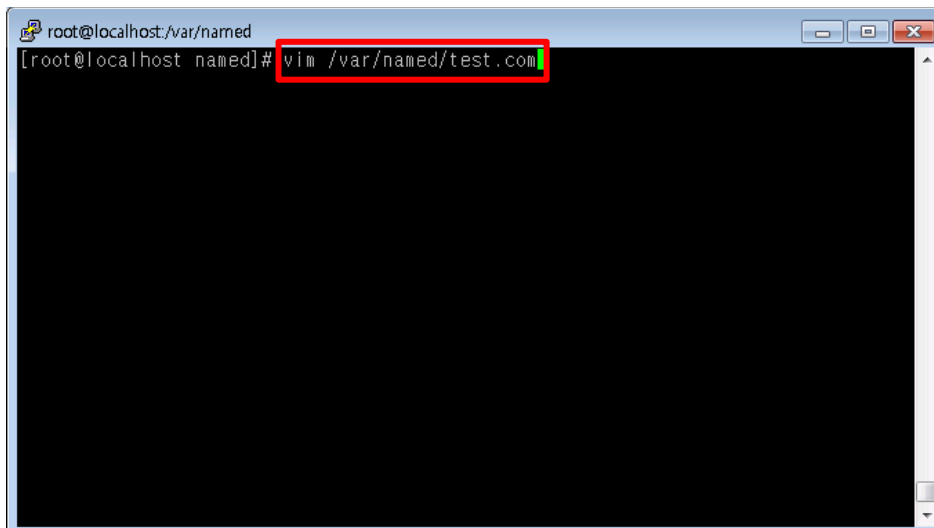
2.3 호스트 추가. (zone파일 생성.)

- 1 named.rfc1912.named 설정은 /var/named/ 디렉토리에 있는 zone파일을 불러옵니다. 샘플을 이용하여 양식대로 zone 파일 생성을 위해 named.empty 파일을 해당 폴더에 복사합니다.
➔ cp -a /var/named/named.empty /var/named/test.com



```
root@localhost:/var/named
[root@localhost named]# cp -a /var/named/named.empty /var/named/test.com
[root@localhost named]#
[root@localhost named]# ls -l /var/named
합계 40
drwxr-x--- 6 root named 4096 2012-03-12 17:08 chroot
drwxrwx--- 2 named named 4096 2012-03-12 17:08 data
drwxrwx--- 2 named named 4096 2012-03-12 17:09 dynamic
-rw-r----- 1 root named 1892 2008-02-18 21:29 named.ca
-rw-r----- 1 root named 324 2012-03-12 16:53 named.empty
-rw-r----- 1 root named 152 2009-12-15 21:27 named.empty_b
-rw-r----- 1 root named 152 2007-06-21 19:09 named.localhost
-rw-r----- 1 root named 168 2009-12-15 21:27 named.loopback
drwxrwx--- 2 named named 4096 2012-01-10 18:06 slaves
-rw-r----- 1 root named 324 2012-03-12 16:53 test.com
[root@localhost named]#
```

- 2 복사한 샘플 zone 파일을 vi 편집기로 편집합니다.
➔ vim /var/named/test.com



```
root@localhost:/var/named
[root@localhost named]# vim /var/named/test.com
```

- 3 zone파일을 양식에 맞추어 고객님 도메인 정보를 등록합니다. 아래는 예시입니다.
※ 주의 : 도메인 명을 입력할 때는 반드시 맨 뒤에 "."을 붙여주어야 합니다.

```
root@localhost:/var/named
$TTL 86400
@      IN SOA ns1.test.com. dnsmaster.test.com. (
        20120312; serial
        3H      ; refresh
        15M     ; retry
        1W      ; expire
        1D     ) ; minimum

        IN NS   ns1.test.com.
        IN MX  10 mail.test.com.
        IN A   192.168.0.40
ns1     IN A   192.168.0.40
www     IN A   192.168.0.40
mail    IN A   192.168.0.40
ftp     IN A   192.168.0.40
tongkni IN CNAME www.tongkni.co.kr
~
~
~
~
~
~
:~q~
```

- **\$TTL** : Time To Live의 약어로 DNS 데이터가 네트워크에 무한정 돌아다니지 않도록 하기 위한 시간설정. 초단위로 86400은 하루를 의미.
- **IN** : 클래스 이름으로 internet을 의미.
- **@** : named.rfc1912.zones에서 설정한 도메인 주소. (test.com)
- **SOA** : Start Of Authority 약어로 권한의 시작을 의미. SOA 뒤의 ns1.test.com.은 Master DNS를 의미하고 그 뒤의 dnsmaster.test.com은 이메일 주소 dnsmaster@test.com을 의미.
- **20120312 ; serial** : 일련번호, 보통 날짜로 지정.
- **3H ; refresh** : 2차 네임서버가 1차 네임서버 데이터를 재확인할 시간 간격 (3H = 3시간)
- **15M ; retry** : 1차 네임서버가 다운 시 2차 네임서버가 접속을 시도할 시간 간격 (15M = 15분)
- **1W ; expiry** : dns 데이터 만료기간(1차 네임서버가 다운 시 2차 네임서버가 데이터를 사용할 기간), (1W=1주일)
- **1D ; minimum** : 다른 네임서버가 캐시에 저장할 시간, (1D=하루)
- ; : 주석.
- **NS** : Name Server 의 약어로 설정된 도메인의 네임 서버 역할을 하는 컴퓨터를 지정.
- **MX** : Mail Exchanger 의 약어로 메일 서버를 설정. 숫자는 우선순위 값.
- **A** : 호스트 이름에 매핑하는 IP 주소를 지정.
- **CNAME** : 다른 도메인 주소로 매핑.

※ 레코드에 대한 자세한 내용은 챗터 3을 참고하시기 바랍니다.

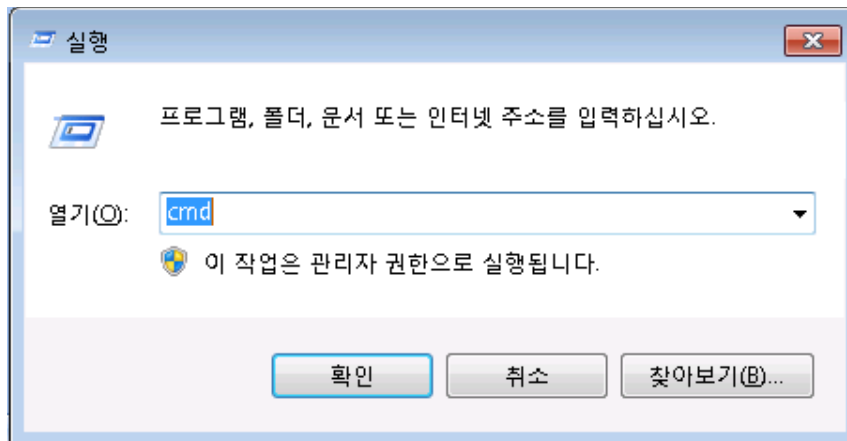
- 4 저장 후 named를 재 시작 합니다.
- ➔ service named restart


```

root@localhost:/var/named
[root@localhost named]# service named restart
named 중지 :
named 시작 :
[root@localhost named]# [ OK ]
[ OK ]

```

- 5 네임서버가 제대로 구성되었는지 확인합니다.
테스트를 진행할 외부 PC에서 시작 -> 실행 -> cmd 를 입력하여 창을 띄웁니다.



- 6 아래와 같이 “nslookup - <네임서버 주소>”를 입력한 후 찾고자 하는 도메인의 IP를 입력하여 확인합니다.
 ➔ nslookup - 192.168.0.8
 > www.test.com
 > ftp.test.com

```
관리자: C:\Windows\system32\cmd.exe - nslookup - 192.168.0.40
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\myunggu> nslookup - 192.168.0.40
기본 서버: UnKnown
Address: 192.168.0.40

> www.test.com
서버: UnKnown
Address: 192.168.0.40
이름: www.test.com
Address: 192.168.0.40

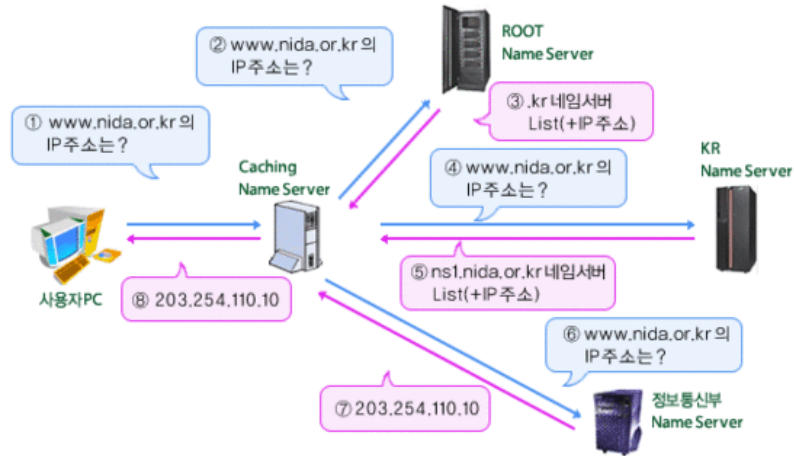
> ftp.test.com
서버: UnKnown
Address: 192.168.0.40
이름: ftp.test.com
Address: 192.168.0.40

>
```

2.4 상위 기관에 네임서버 등록하기(네임호스트 추가).

- 1 내 도메인으로 직접 네임서버를 운영하는 경우, 도메인을 등록한 업체를 통하여 네임서버 호스트 등록을 해야 네임서버로 사용할 수 있습니다

※ 네임서버가 먼저 구축이 완료된 후 진행하셔야 원활한 진행을 할 수 있습니다.



DNS 쿼리과정

- 2 여기서는 tongkni.co.kr이란 도메인을 소유하고 있고 ns1.tongkni.co.kr 이라는 주소를 네임서버를 사용하려는 경우를 예로 들어 안내해 드리겠습니다.

네임서버에서 tongkni.co.kr의 NS 레코드 값을 ns1.tongkni.co.kr으로 등록하기 위해 /etc/named.rfc1912.zones을 수정 후 /var/named/tongkni.co.kr zone파일을 생성합니다.

```

root@localhost:/var/named
// ISC BIND named zone configuration for zones recommended by
// RFC 1912 section 4.1 : localhost TLDs and address zones
// and http://www.ietf.org/internet-drafts/draft-ietf-dnsop-default-local-zones-0
// 2.txt
// (c)2007 R W Franks
// See /usr/share/doc/bind+/sample/ for example named configuration files.
zone "test.com" IN {
    type master;
    file "test.com";
    allow-update { none; };
};
zone "tongkni.co.kr" IN {
    type master;
    file "tongkni.co.kr";
    allow-update { none; };
};
    
```

/etc/named.rfc1912.zones

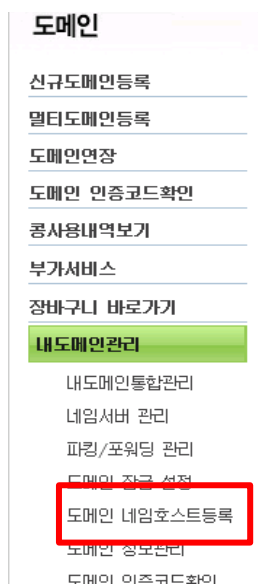
```

root@localhost:/var/named
RTT: 0.65400
@ IN SOA ns1.tongkni.co.kr. dnsmaster.tongkni.co.kr.
                                201200127 : serial
                                3H : refresh
                                15M : retry
                                1W : expire
                                1D : minimum
      IN NS ns1.tongkni.co.kr.
ns1 IN A 123.123.123.123
test IN A 111.111.111.111
~
~
~
~
~
~
~
~
~
~
:~q!

```

/var/named/tongkni.co.kr

- 3 tongkni.co.kr 도메인을 등록한 업체에 ns1.tongkni.co.kr 주소를 네임서버로 사용할 수 있도록 요청합니다. (아래 그림은 <http://www.nunauri.co.kr> 에서의 네임 호스트 등록방법이며 각 업체별로 메뉴 이름이 상이할 수 있습니다.)



- 4 네임서버로 사용하려는 주소(ns1.tongkni.co.kr)와 네임 서버 IP주소를 입력합니다..
 ※ 적용되는데 빠르면 반 나절, 최대 1~2일의 시간이 소요될 수 있습니다.

신규 네임호스트명	신규 네임호스트 아이피명
ns1.tongkni.co.kr	123,123,123,123

호스트IP 수정시 입력란안에 네임호스트명과 새로운 아이피를 입력하시고 변경버튼을 클릭해 주세요

네임 호스트 등록이 완료되면 이제 ns1.tongkni.co.kr 주소는 서버는 네임서버 주소로 이용이 가능합니다.

※ 1대의 네임서버로 운영 중 장애가 생길 경우 큰 문제가 발생할 수 있으므로, 같은 방식으로 네임 서버를 최소 2대 이상 구성하여 안정적으로 사용하는 것을 권장합니다.

- 5 마지막으로 도메인 등록업체에서 네임서버를 변경하는 메뉴를 찾아, 네임서버를 이용할 도메인의 네임서버 주소를 변경해주면 완료됩니다.

※ 적용되는데 빠르면 반 나절, 최대 1~2일의 시간이 소요될 수 있습니다.

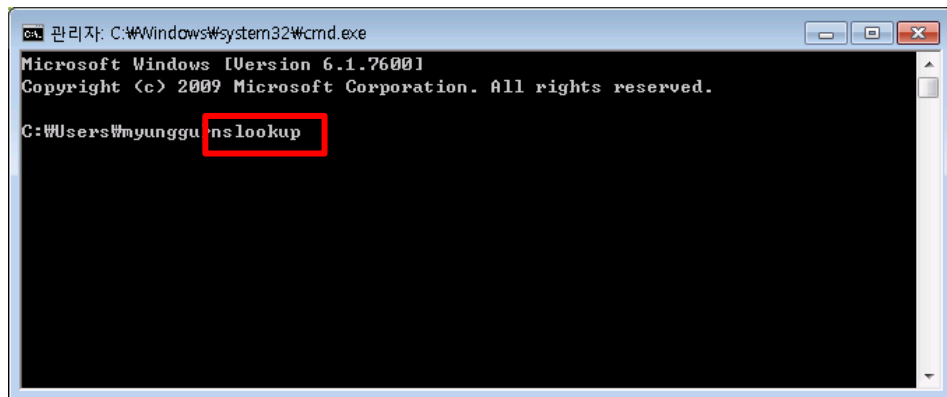
변경할 네임서버

1차 네임서버명	ns1.tongkni.co.kr	1차 네임서버 아이피	123,123,123,123
2차 네임서버명		2차 네임서버 아이피	
3차 네임서버명		3차 네임서버 아이피	
4차 네임서버명		4차 네임서버 아이피	
5차 네임서버명		5차 네임서버 아이피	

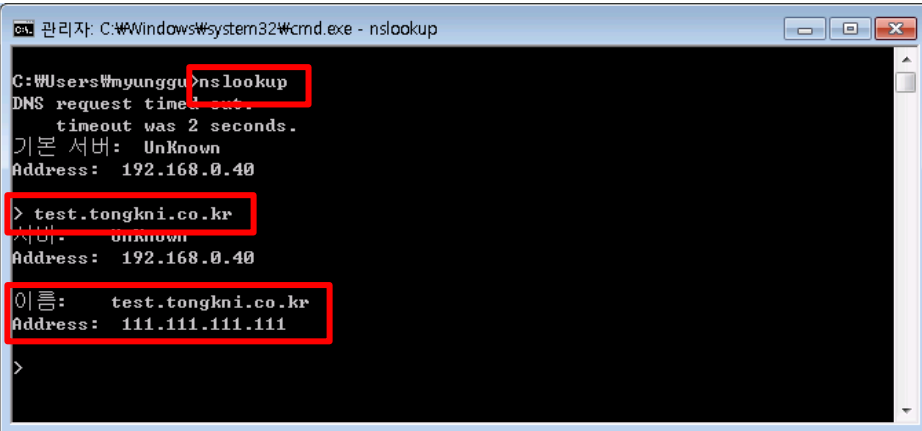
★ 주의 사항 ★

1. 사용하실 네임서버는 호스트 등록이 되어 있고 실제로 존재해야만 합니다.
(그렇지 않은 네임서버를 입력하시면 에러가 나가나 도메인을 사용할 수 없습니다.)
2. 1차 2차 네임서버 명과 아이피를 모두 입력해 주시기 바랍니다.
3. 네임서버 변경이 완료 된 후에 최대 2-3일의 갱신 시간이 필요합니다.

- 6 네임서버가 아닌 외부 PC에서 아래와 같이 “nslookup”을 입력합니다



- 7 “test.tongkni.co.kr” 혹은 자체 구축한 네임서버를 이용하는 도메인을 입력하여 원하는 IP주소가 조회되는지 확인합니다.



```
관리자: C:\Windows\system32\cmd.exe - nslookup
C:\Users\Wmyunggu>nslookup
DNS request timed out.
    timeout was 2 seconds.
기본 서버: Unknown
Address: 192.168.0.40
> test.tongkni.co.kr
서버: Unknown
Address: 192.168.0.40
이름: test.tongkni.co.kr
Address: 111.111.111.111
>
```

- 8 그 외의 도메인을 추가할 경우에는, 네임호스트 등록 과정 없이 네임서버에 정보를 추가하고 도메인의 네임서버만 변경하면 됩니다.

3. 레코드 값의 정의와 설정.

1 SOA 레코드

- SOA(Start Of Authority : 권한 시작)는 영역의 시작을 알리는 첫 번째 레코드입니다. 영역의 새로 고침 간격, 보조 영역으로 전송하는 기간 및 만료기간, 영역 내 각 리소스 레코드의 유효기간 등을 설정할 수 있습니다.


```

root@localhost:/var/named
$TTL 86400
@ IN SOA @ ns1.test.com. (
                                20120312: serial
                                3H   : refresh
                                15M  : retry
                                1W   : expire
                                1D ) : minimum

                                IN      NS      ns1.test.com.
                                IN      MX      10 mail.test.com.

ns1  IN      A      192.168.0.40
www  IN      A      192.168.0.40
mail IN      A      192.168.0.40
ftp  IN      A      192.168.0.40
test1 IN     A      192.168.0.40
test2 IN     A      192.168.0.40
test3 IN     A      192.168.0.40
test4 IN     A      192.168.0.40
test5 IN     A      192.168.0.40
test6 IN     A      192.168.0.40

```

Ex2) test.com의 IP가 변경되어도 test.com의 A 레코드 값 하나만 변경하면 됨.

```

root@localhost:/var/named
$TTL 86400
@ IN SOA @ ns1.test.com. (
                                20120312: serial
                                3H   : refresh
                                15M  : retry
                                1W   : expire
                                1D ) : minimum

                                IN      NS      ns1.test.com.
                                IN      MX      10 mail.test.com.

ns1  IN      CNAME test.com
www  IN      CNAME test.com
mail IN      CNAME test.com
ftp  IN      CNAME test.com
test1 IN     CNAME test.com
test2 IN     CNAME test.com
test3 IN     CNAME test.com
test4 IN     CNAME test.com
test5 IN     CNAME test.com
test6 IN     CNAME test.com

```

4 A 레코드.

→ A 레코드는 해당 주소로 조회 요청이 되었을 때 IP주소로 정보를 제공합니다.


```

root@localhost:/var/named
$TTL 86400
@ IN SOA ns1.test.com. (
                                20120312: serial
                                3H   : refresh
                                15M  : retry
                                1W   : expire
                                1D   : minimum
)
IN NS ns1.test.com.
IN MX 10 mail.test.com.
ns1 IN A 192.168.0.40
www IN A 192.168.0.40
mail IN A 192.168.0.40
ftp  IN A 192.168.0.40
tongkni IN CNAME www.tongkni.co.kr
~
~
~
~
:wq!

```

5 MX 레코드.

- MX(Mail Exchanger) 레코드는 메일 송수신을 담당하는 메일 서버의 주소를 제공합니다.
Ex) test.com 도메인을 사용하는 계정(ex : webmaster@test.com, admin@test.com 등)으로 E-mail을 주고 받을 때 구글 메일서버(aspmx.l.google.com)를 통해 발송 및 수신을 하도록 설정.

```

root@localhost:/var/named
$TTL 86400
@ IN SOA ns1.test.com. dnsmaster.test.com. (
                                20120312: serial
                                3H   : refresh
                                15M  : retry
                                1W   : expire
                                1D   : minimum
)
IN NS ns1.test.com.
IN MX 10 aspmx.l.google.com.
IN A 192.168.0.40
ns1 IN A 192.168.0.40
www IN A 192.168.0.40
mail IN A 192.168.0.40
ftp  IN A 192.168.0.40
tongkni IN CNAME www.tongkni.co.kr
~
~
~
~
:wq!

```

※ MX 레코드 값이 여러 개 일 경우 우선 순위가 낮은 MX 레코드 값 부터 참조합니다.

6 TXT 레코드.

- 개인 도메인네임이나 기업 도메인네임으로 이메일을 사용할 경우, 스팸으로 악용되는 도메인이 아님을 알리기 위해서 해당 도메인을 White Domain으로 등록을 해야 합니다. 이 때 네임서버에서 TXT 레코드를 이용한 SPF 레코드를 생성해야 합니다.

● 메일서버 등록제 (SPF: Sender Policy Framework)

메일서버 정보를 사전에 DNS에 공개 등록함으로써 수신자로 하여금 이메일에 표시된 발송자 정보가 실제 메일 서버의 정보와 일치하는지를 확인할 수 있도록 하는 인증기술

* 대다수 스팸발송자가 자신의 신원을 감추기 위하여 발송자 주소나 전송경로를 허위로 표기하거나 변경하는 경우가 많다는데 착안

☞ SPF를 이용한 이메일 인증절차:

- 발신자 : 자신의 메일서버 정보와 정책을 나타내는 SPF 레코드를 해당 DNS에 등록
- 수신자 : 이메일 수신시 발송자의 DNS에 등록된 SPF 레코드를 확인하여 해당 이메일에 표시된 발송IP와 대조하고 그 결과값에 따라 수신여부를 결정
(메일서버나 스팸차단솔루션에 SPF 확인기능이 설치되어 있어야 함)

☞ SPF 개발 및 도입현황:

- 1998년 Paul Vixie의 'Repudiating Mail From'에서 처음으로 아이디어가 제안된 이후 Pobox.com의 Meng Weng Wong에 의해 SPF가 개발됨
- 2004년 2월 IETF(Internet Engineering Task Force)에 공식 RFC(Request For Comments)로 제안되었으며, 2004년 12월 SPF의 모든 기술적 내용들이 최종 완성됨
- SPF는 타 인증기술에 비해 적용이 용이하고 호환성이 좋으며 오픈소스를 기반으로 하므로 전 세계적으로 폭넓은 지지기반을 확보하고 있음
- 한국을 비롯한 미국, 캐나다, 일본 등 여러 국가들이 정부차원에서 사업자들을 대상으로 SPF 레코드 출판 및 확인기능 도입을 통한 스팸차단 활용을 적극 권고하고 있음

※ 화이트 도메인은 한국인터넷진흥원(<http://www.kisarbl.or.kr>)에서 관리하고 있습니다.

※ 화이트 도메인 등록을 위한 SPF 레코드 생성 방법은 아래 URL 주소를 참고하시기 바랍니다.
https://www.kisarbl.or.kr/spf/spfWizard_step1.jsp#

감사합니다.