DNS Server

bind
named.service

개요

- DNS(Domain Name Service)는 호스트의 도메인 이름을 IP 주소를 바꾸거나 그 반대의 변환을 위해 개발되었다.
- DNS 서버는 보유한 도메인을 관리해주는 역할을 수행하지만, 클라이언트에서 도메인명에 대한 IP 주소의 조회를 요청했을 경우에 반환해주는 역할도 수행한다.

DNS Server 종류

- **Primary Name Server**
  - 사용하는 도메인을 관리하기 위해 필수적으로 구성하는 서버
- **Secondary Name Server**
  - Primary Name Server의 zone 파일을 백업하는 역할을 수행
- **Caching Name Server**
  - 관리하는 도메인 없이 이름 풀이만을 제공하기 위해 구성하는 서버

DNS Server 프로그램: BIND(Berkeley Internet Name Domain)

/etc/named.conf

- DNS 서버의 전반적 환경 설정을 담당하는 파일

/var/named

- 루트 도메인 서버에 대한 정보를 담고 있는 named.ca를 비롯하여 사용자가 선언하는 zone 파일 등이 위치하는 디렉터리

/etc/named.conf 파일

- 파일의 구성과 특징

    - 파일의 구성은 크게 주석문과 구문으로 구성되어 있다.
    - 주석은 C에서 사용하는 /* */, C++에서 사용하는 //, 유닉스 계열에서 사용하는 # 등 모두 사용 가능하다.
    - 구문에는 options, loggin, controls, zone, acl, view, key, masters, server 등이 존재한다.
    - **각 구문은 중괄호{}로 둘러싸고 끝날 때는 세미콜론(;)을 사용한다.**
    - **include 지시자를 선언하여 별도의 파일에 추가 정의할 수 있다.**
- 주요 구문
    - **options 구문**: DNS 서버의 동작 및 제어와 관련된 여러 가지 설정을 하는 영역으로 존 파일이 위치하는 디렉터리명은 반드시 명기해야 한다.
        - directory "/var/named";
        - listen-on port 53 { any; };
        - allow-query { any; };
        - query-source port 53;
    - **acl 구문**: 여러 호스트를 하나의 명칭으로 지정할 때 사용한다.
    - **zone 구문**: 도메인을 관리하는 데이터베이스 파일인 zone 파일을 지정한다.
        - CentOS 7에서는 /etc/named.conf 파일의 복잡해지는 것을 막기 위해 include 지시자를 사용해서 root zone 파일 관련한 설정을 제어한 zone 구문 자체를 /etc/named.rfc1912.zones라는 별도의 파일에서 설정하도록 권장하고 있다.
        - 기본 형식
            - zone "도메인명" IN {
                - type {master | slave | hint};
                - file "존파일명";
            - };
- /etc/named.conf 파일의 분할
    - CentOS 7 버전에서는 root zone 파일 관련된 설정을 제외한 다른 zone 파일 관련 설정은 **/etc/named.rfc1912.zones**에서 설정하도록 권장한다.
    - 도메인별로 사용한 존 파일과 리버스 존 파일 선언은 named.rfc1912.zones에 설정해야 한다.

zone 파일

- zone 파일 개요
    - zone 파일은 /etc/named.cnf 파일에 지정된 디렉터리에 지정된 파일명으로 생성해야 한다.
    - 기본 설정 디렉터리는 /var/named 디렉터리이므로 이 디렉터리에 생성하면 되고,

최근에 zone 파일명은 /etc/named.rfc1912.zones에 설정하므로 이 파일에 설정한 이름대로 생성한다.

- zone 파일의 구조: 크게 SOA 레코드와 자원 레코드로 나눌 수 있다.
    - $TTL 1D
    - @ IN SOA nameserver contact-email-address {
        - serial_namer ; serial
        - refresh_number ; refresh
        - retry_number ; retry
        - expire_number ; expire
        - minimum number ; minimum
    - 도메인 TTL class type Rdata

1단계: bind 설치

- **yum install bind**

2단계: Server 설정

/etc/named.conf

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

/etc/named.rfc1912.zones

- vi /etc/named.rfc1912.zones
    - **zone “linux.or.kr” IN {**
        - **type master;**
        - **file “linux.zone”;**
    - **};**

zone 파일 생성

- **cd /var/named**
- **cp -p named.localhost linux.zone**
- vi linux.zone

    - $TTL ID
    - @ IN SOA ns.linux.or.kr. itserver.linux.or.kr. (
    - …
        - NS ns.linux.or.kr.
        - A 192.168.111.10
        - MX 10 linux.or.kr.
    - ns A 192.168.111.10
    - itserver A 192.168.111.10
    - www CNAME itserver
    - ftp CNAME itserver

3단계: DNS 서비스 활성화 및 부팅시 자동 시작

- **systemctl restart named.service**
    - **텔넷 시작**
- **systemctl enable named.service**
    - **부팅시 자동 시작**
- **systemctl status named.service**
    - named 서비스 확인

4단계: 방화벽 설정(서비스/포트 열기)

- **firewall-cmd --permanent --zone=public --add-service=dns**
    - **Telnet Port 열기**
- **firewall-cmd --reload**
    - **방화벽 설정 저장**
- **firewall-cmd --zone=public --list-service**
    - **방화벽 열린 포트 확인**

5단계: SELinux

- **관련 설정 없음**
- **getenforce**
    - **SELinux 설정 상태 확인**

DNS 관련 유틸리티

named-checkconf

- /etc/named.conf 파일의 문법적 오류를 찾아주는 명령이다.
- **named-checkconf 파일명**
    - 사용 예
        - **named-checkconf**
        - named-checkconf /backup/etc/named.conf
            - 해당 파일의 문법적 오류를 검사

named-checkzone

- zone 파일의 문법적 오류를 찾아주는 명령이다.
- **named-checkzone 도메인명 존파일경로**
    - 사용 예
        - **named-checkzone linux.or.kr /var/named/linux.zone**