



Computer Systems Administration (IE2060)  
2<sup>nd</sup> Year, 2<sup>nd</sup> Semester

Assignment

**Firewall Installation**

Submitted to  
Sri Lanka Institute of Information Technology

Student Registration Number	Student Name with Initials
IT21042706	Mendis H.R.R

In partial fulfillment of the requirements for the  
Bachelor of Science Special Honors Degree in Information Technology

22.10.2022

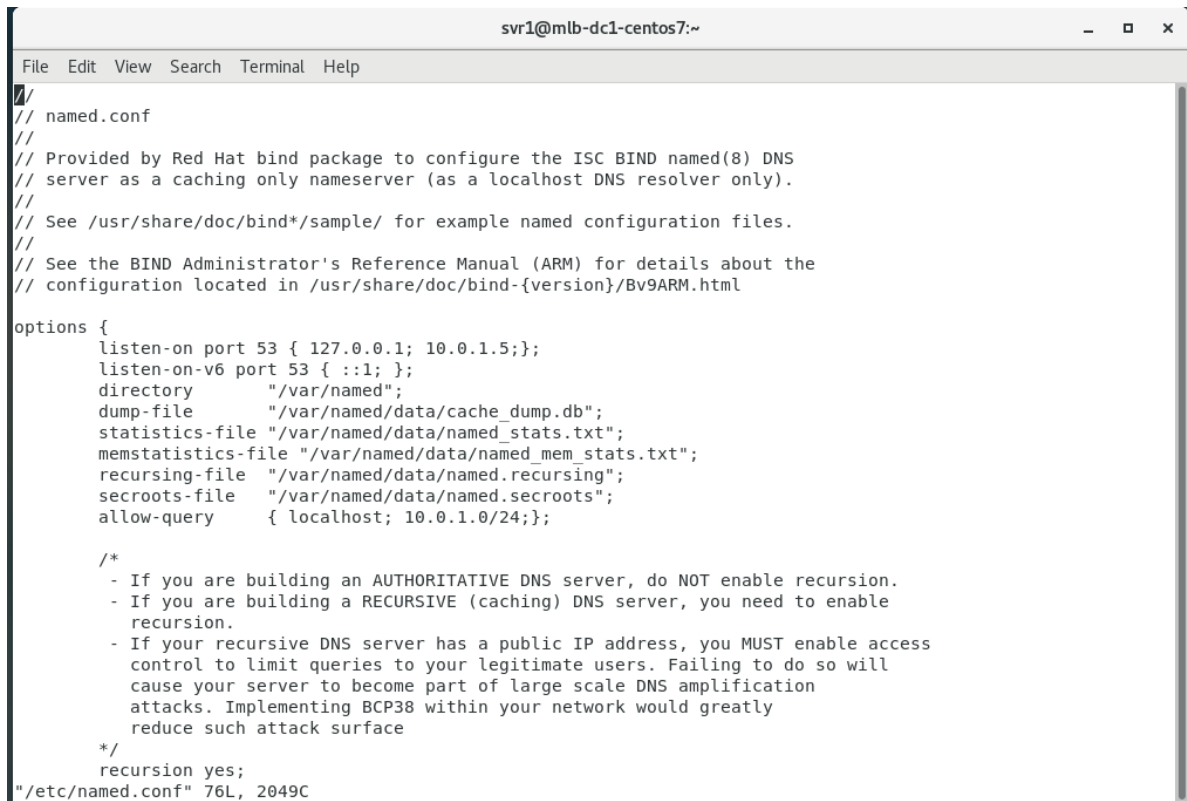
## Table of Contents

1 . DNS Installation.....	3
2 . Zones.....	5
2.1 Creating Zones .....	5
2.1.1 Forward Lookup Zone .....	5
2.1.2 Reverse Lookup Zone .....	5
2.2 Checking the Added zones.....	5
3 . Firewall Installation .....	6
4 . Adding Zone Files to the Firewall list .....	6
5 . Adding given ports to the Firewall list .....	7
6 . Allowing the https service through the Firewall.....	7
7 . Checking the added Ports and Services .....	7

## Table of Figures

Figure 1.1 Named.conf file - I .....	3
Figure 1.2 Named.conf file - II .....	3
Figure 1.3 DNS server active status.....	4
Figure 1.4 Testing the DNS server .....	4
Figure 2.1 Adding forward lookup zone inside the named.conf file .....	5
Figure 2.2 Adding reverse lookup zone inside the named.conf file .....	5
Figure 2.3 Command to check the added zones .....	5
Figure 3.1 Enabling & checking the firewall state .....	6
Figure 3.2 Firewall is already installed.....	6
Figure 4.1 Renaming the older zone files & adding them to the firewall list.....	6
Figure 5.1 Adding the ports 636, 161 & 50000 to the Firewall list.....	7
Figure 6.1 Command to allow the https service through the firewall.....	7
Figure 7.1 Command to check the added ports and services .....	7

# 1 . DNS Installation



```
svr1@mlb-dc1-centos7:~  
File Edit View Search Terminal Help  
//  
// 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.  
//  
// See the BIND Administrator's Reference Manual (ARM) for details about the  
// configuration located in /usr/share/doc/bind-{version}/Bv9ARM.html  
  
options {  
    listen-on port 53 { 127.0.0.1; 10.0.1.5;};  
    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";  
    recursing-file "/var/named/data/named.recursing";  
    secroots-file "/var/named/data/named.secroots";  
    allow-query { localhost; 10.0.1.0/24;};  
  
    /*  
    - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.  
    - If you are building a RECURSIVE (caching) DNS server, you need to enable  
    recursion.  
    - If your recursive DNS server has a public IP address, you MUST enable access  
    control to limit queries to your legitimate users. Failing to do so will  
    cause your server to become part of large scale DNS amplification  
    attacks. Implementing BCP38 within your network would greatly  
    reduce such attack surface  
    */  
    recursion yes;  
};  
/etc/named.conf" 76L, 2049C
```

Figure 1.1 Named.conf file - I



```
svr1@mlb-dc1-centos7:~  
File Edit View Search Terminal Help  
    dnssec-enable yes;  
    dnssec-validation yes;  
  
    /* Path to ISC DLV key */  
    bindkeys-file "/etc/named.root.key";  
  
    managed-keys-directory "/var/named/dynamic";  
  
    pid-file "/run/named/named.pid";  
    session-keyfile "/run/named/session.key";  
};  
  
logging {  
    channel default_debug {  
        file "data/named.run";  
        severity dynamic;  
    };  
};  
  
zone "." IN {  
    type hint;  
    file "named.ca";  
};  
  
#####forward look up zone  
zone "ns" IN {  
    type master;  
    file "forwardcsalk";  
    allow-update { none; };  
};  
  
#####reverse look up zone  
zone "1.0.10.in-addr.arpa" IN {  
    type master;  
    file "reversecsalk";  
    allow-update { none; };  
};  
  
include "/etc/named.rfc1912.zones";  
include "/etc/named.root.key";
```

Figure 1.2 Named.conf file - II

```

[root@mlb-dcl-centos7 ~]# service named status
Redirecting to /bin/systemctl status named.service
● named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.service; disabled; vendor preset: disabled)
   Active: active (running) since Fri 2022-10-21 23:01:44 +0530; 20h ago
   Main PID: 12766 (named)
      Tasks: 4
     CGroup: /system.slice/named.service
             └─12766 /usr/sbin/named -c /etc/named.conf

Oct 22 18:51:27 mlb-dcl-centos7.csa.lk named[12766]: network unreachable resolving 'mlb-dcl-centos7.csa....#53
Oct 22 18:51:27 mlb-dcl-centos7.csa.lk named[12766]: network unreachable resolving 'mlb-dcl-centos7.csa....#53
Oct 22 18:51:27 mlb-dcl-centos7.csa.lk named[12766]: network unreachable resolving 'mlb-dcl-centos7.csa....#53
Oct 22 18:51:27 mlb-dcl-centos7.csa.lk named[12766]: network unreachable resolving 'mlb-dcl-centos7.csa....#53
Oct 22 18:51:27 mlb-dcl-centos7.csa.lk named[12766]: network unreachable resolving 'mlb-dcl-centos7.csa....#53
Oct 22 18:51:27 mlb-dcl-centos7.csa.lk named[12766]: network unreachable resolving 'mlb-dcl-centos7.csa....#53
Oct 22 18:51:27 mlb-dcl-centos7.csa.lk named[12766]: network unreachable resolving 'mlb-dcl-centos7.csa....#53
Oct 22 18:51:27 mlb-dcl-centos7.csa.lk named[12766]: network unreachable resolving 'mlb-dcl-centos7.csa....#53
Oct 22 18:51:27 mlb-dcl-centos7.csa.lk named[12766]: network unreachable resolving 'mlb-dcl-centos7.csa....#53
Oct 22 18:51:27 mlb-dcl-centos7.csa.lk named[12766]: network unreachable resolving 'mlb-dcl-centos7.csa....#53
Hint: Some lines were ellipsized, use -l to show in full.
[root@mlb-dcl-centos7 ~]#

```

Figure 1.3 DNS server active status

```

[root@mlb-dcl-centos7 ~]# dig csa.lk

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9 <<>> csa.lk
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 39596
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;; udp: 4096
;; QUESTION SECTION:
;csa.lk.                                IN      A

;; Query time: 1 msec
;; SERVER: 10.0.1.5#53(10.0.1.5)
;; WHEN: Sun Oct 23 04:22:29 +0530 2022
;; MSG SIZE rcvd: 35

[root@mlb-dcl-centos7 ~]#

```

Figure 1.4 Testing the DNS server

## 2 . Zones

### 2.1 Creating Zones

#### 2.1.1 Forward Lookup Zone

```
#####forward look up zone
zone"ns" IN {
type master;
file "forwardcsalk";
allow-update { none; };
};
```

Figure 2.1 Adding forward lookup zone inside the named.conf file

#### 2.1.2 Reverse Lookup Zone

```
#####reverse look up zone
zone"1.0.10.in-addr.arpa" IN {
type master;
file "reversecsalk";
allow-update { none; };
};
```

Figure 2.2 Adding reverse lookup zone inside the named.conf file

### 2.2 Checking the Added zones

```
[root@mlb-dcl-centos7 ~]# firewall-cmd --reload
success
[root@mlb-dcl-centos7 ~]# firewall-cmd --get-zones
block dmz drop external forwardcsalk home internal public reversecsalk trusted work
[root@mlb-dcl-centos7 ~]# firewall-cmd --zone=public --permanent --add-service=https
success
[root@mlb-dcl-centos7 ~]#
```

Figure 2.3 Command to check the added zones

### 3 . Firewall Installation

```
[root@mlb-dcl-centos7 svr1]# yum install firewalld
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirrors.nxtgen.com
 * extras: mirrors.nxtgen.com
 * updates: mirrors.nxtgen.com
Package firewalld-0.6.3-13.el7_9.noarch already installed and latest version
Nothing to do
```

Figure 3.2 Firewall is already installed

```
[root@mlb-dcl-centos7 ~]# systemctl start firewalld
[root@mlb-dcl-centos7 ~]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2022-10-22 18:58:01 +0530; 3h 32min ago
     Docs: man:firewalld(1)
   Main PID: 27869 (firewalld)
      Tasks: 2
   CGroup: /system.slice/firewalld.service
           └─27869 /usr/bin/python2 -Es /usr/sbin/firewalld --nofork --nopid

Oct 22 19:30:47 mlb-dcl-centos7.csa.lk firewalld[27869]: WARNING: COMMAND_FAILED: '/usr/sbin/iptables -w...?).
Oct 22 19:30:47 mlb-dcl-centos7.csa.lk firewalld[27869]: WARNING: COMMAND_FAILED: '/usr/sbin/iptables -w...?).
Oct 22 19:30:47 mlb-dcl-centos7.csa.lk firewalld[27869]: WARNING: COMMAND_FAILED: '/usr/sbin/iptables -w...?).
Oct 22 19:30:47 mlb-dcl-centos7.csa.lk firewalld[27869]: WARNING: COMMAND_FAILED: '/usr/sbin/iptables -w...me.
Oct 22 19:30:47 mlb-dcl-centos7.csa.lk firewalld[27869]: WARNING: COMMAND_FAILED: '/usr/sbin/iptables -w...me.
Oct 22 19:30:47 mlb-dcl-centos7.csa.lk firewalld[27869]: WARNING: COMMAND_FAILED: '/usr/sbin/iptables -w...?).
Oct 22 19:30:47 mlb-dcl-centos7.csa.lk firewalld[27869]: WARNING: COMMAND_FAILED: '/usr/sbin/iptables -w...?).
Oct 22 19:30:47 mlb-dcl-centos7.csa.lk firewalld[27869]: WARNING: COMMAND_FAILED: '/usr/sbin/iptables -w...?).
Oct 22 19:30:47 mlb-dcl-centos7.csa.lk firewalld[27869]: WARNING: COMMAND_FAILED: '/usr/sbin/iptables -w...?).
Oct 22 19:30:47 mlb-dcl-centos7.csa.lk firewalld[27869]: WARNING: COMMAND_FAILED: '/usr/sbin/iptables -w...?).
Hint: Some lines were ellipsized, use -l to show in full.
[root@mlb-dcl-centos7 ~]# systemctl enable firewalld
[root@mlb-dcl-centos7 ~]# firewall-cmd --state
running
[root@mlb-dcl-centos7 ~]#
```

Figure 3.1 Enabling & checking the firewall state

### 4 . Adding Zone Files to the Firewall list

```
[root@mlb-dcl-centos7 svr1]# cd /var/named
[root@mlb-dcl-centos7 named]# mv forward.csa.lk forwardcsalk
[root@mlb-dcl-centos7 named]# mv reverse.csa.lk reversecsalk
[root@mlb-dcl-centos7 named]# firewall-cmd --permanent --new-zone=forwardcsalk
success
[root@mlb-dcl-centos7 named]# firewall-cmd --permanent --new-zone=reversecsalk
success
[root@mlb-dcl-centos7 named]#
```

Figure 4.1 Renaming the older zone files & adding them to the firewall list

## 5 . Adding given ports to the Firewall list

```
[root@mlb-dc1-centos7 named]# firewall-cmd --add-port=636/tcp --permanent
success
[root@mlb-dc1-centos7 named]# firewall-cmd --add-port=161/tcp --permanent
success
[root@mlb-dc1-centos7 named]# firewall-cmd --add-port=50000/tcp --permanent
success
[root@mlb-dc1-centos7 named]#
```

Figure 5.1 Adding the ports 636, 161 & 50000 to the Firewall list

## 6 . Allowing the https service through the Firewall

```
[root@mlb-dc1-centos7 ~]# firewall-cmd --zone=public --permanent --add-service=https
success
[root@mlb-dc1-centos7 ~]#
```

Figure 6.1 Command to allow the https service through the firewall

## 7 . Checking the added Ports and Services

```
[root@mlb-dc1-centos7 ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens34
  sources:
  services: dhcpv6-client ssh
  ports: 53/udp 80/tcp 443/tcp 636/tcp 161/tcp 50000/tcp
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@mlb-dc1-centos7 ~]#
```

Figure 7.1 Command to check the added ports and services