Это руководство проведет вас через шаги, которые вам потребуются для настройки DNS-сервера BIND в CentOS 8 — Настройка привязки главного DNS-сервера в CentOS 8. Система доменных имен — это иерархическая и децентрализованная система именования для компьютеры, службы или другие ресурсы, подключенные к Интернету или частной сети. Он действует как телефонная книга в Интернете, поскольку дает адрес каждому компьютеру с связанным с ним полным доменным именем.

Как часть прикладного уровня эталонной модели TCP / IP, DNS очень важен в повседневной работе компьютеров по всему миру. Мы собираемся установить авторитетный BIND DNS на CentOS8 и выполнить такие настройки, как добавление записей PTR, A / AAAA среди других.

------------------------------------------------------------------------------------------

1) Conf both machines with in same network.

2) Make pingable to each other.

------------------------------------------------------------------------------------------

1.Выполните следующие команды, чтобы установить пакеты Bind DNS-сервера на сервере CentOS 8.

------------------------------------------------------------------------------------------

1.1 sudo yum -y install bind bind-utils - Выполните следующие команды, чтобы установить пакеты Bind DNS-сервера на сервере

------------------------------------------------------------------------------------------

2.Настройка авторитетного сервера BIND DNS на CentOS 8.

------------------------------------------------------------------------------------------

2.1 infoit.com.ua Зона (Доменное имя)

192.168.154. 0 — управляемая подсеть

192.168.154.94 IP подчиненного сервера

192.168.154.88 — IP главного сервера

2.2 sudo nano /etc/named.conf - конфигурационный файл named.conf.

2.3

//

// 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 { any; }; ## Listen on any since it is an authoritative DNS Publicly available.

listen-on-v6 port 53 { any; }; ## You can also set the same for IPv6

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";

secroots-file "/var/named/data/named.secroots";

recursing-file "/var/named/data/named.recursing";

## Since this will be an authoritative Nameserver, allow query from any host

allow-query { any; }; allow-transfer {192.168.154.94; }; /\* - 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 no; ## Following Advice from above. dnssec-enable yes; dnssec-validation yes; managed-keys-directory "/var/named/dynamic";

pid-file "/run/named/named.pid"; session-keyfile "/run/named/session.key"; /\* https://fedoraproject.org/wiki/Changes/CryptoPolicy \*/

include "/etc/crypto-policies/back-ends/bind.config"; }; logging { channel default\_debug { file "data/named.run"; severity dynamic; }; }; zone "." IN { type hint; file "named.ca"; }; include "/etc/named.rfc1912.zones"; include "/etc/named.root.key"; ## Set your ZONE details as shown below for different domains. Set the forward and reverse details. You can set the names of files as you like zone "infoit.com.ua" IN { type master; file "infoit.forward"; allow-update { none; }; }; ## Make sure you follow the rule for reverse zone (154.168.192.in-addr.arpa). [If your IP is 192.168.10.10, It will be 10.168.192.in-addr.arpa] zone "154.168.192.in-addr.arpa" IN { type master; file "infoit.reverse"; allow-update { none; }; };

Главный сервер 192.168.154.88 . Обратите внимание, что ваш IP-адрес должен быть общедоступным, потому что это авторитетный DNS-сервер.

2.4 После того, как вы установили файлы в named.conf, мы должны создать файлы зоны и разместить все записи, которые вы хотите добавить, такие как A/AAAA, MX, PTR и другие. Создайте файлы в каталоге /var/named/

Sudo nano /var/named/infoit.forward

2.5

$TTL 86400

@ IN SOA dns1.infoit.com.ua. root.infoit.com.ua. (

# You can use any numerical values for serial number but it is recommended to use [YYYYMMDDnn]

2019112201 ;Serial

3600 ;Refresh

1800 ;Retry

604800 ;Expire

86400 ;Minimum TTL

)

# Set your Name Servers here

IN NS dns1.infoit.com.ua.

IN NS dns2.infoit.com.ua.

# define Name Server's IP address

IN A 192.168.154.88

# Set your Mail Exchanger (MX) Server here

IN MX 10 dns1.infoit.com.ua.

# Set each IP address of a hostname. Sample A records.

dns1 IN A 192.168.154.88

dns2 IN A 192.168.154.94

mail1 IN A 192.168.154.97

2.6 Создайте соответствующие обратные записи для того же домена, который мы определили в конфигурационном файле named.conf.

2.7 sudo vim /var/named/infoit.reverse

------------------------------------------------------------------------------------------

3. Изменить настройки DNS на главном сервере.

------------------------------------------------------------------------------------------

3.1 Сделайте наш новый DNS-сервер сервером имен по умолчанию. Откройте файл /etc/resolv.conf и добавьте строки ниже. Обязательно замените IP-адрес в соответствии с вашей средой.

3.2 sudo nano /etc/resolv.conf

3.3 nameserver 192.168.154.88 – ip главного сервера.

------------------------------------------------------------------------------------------

### 4. Разрешить службу DNS на брандмауэре.

------------------------------------------------------------------------------------------

4.1 Настройте брандмауэр, чтобы разрешить службу DNS.

4.2 sudo firewall-cmd --add-service=dns --permanent sudo firewall-cmd –reload

------------------------------------------------------------------------------------------

### 5. Убедитесь, что ваши конфигурации в порядке, запустите и включите привязку

------------------------------------------------------------------------------------------

5.1 sudo named-checkconf

sudo systemctl start named

sudo systemctl enable named