

TD DNS

Valentin Benard – 10/09/2024

Mise en place d'un serveur DNS à partir d'une machine Debian 12.

Machine proxmox :

Tout d'abord, une machine virtuelle Debian 12 est créée sur **Proxmox**.

Un utilisateur « admin » est créé avec les permissions sudoers car il n'est pas possible de se connecter au compte root via ssh.

Adduser admin

Ajout des permissions sudo :

adduser admin sudo

Il faut en suite installer sudo sur le compte root

apt install sudo

Il est désormais possible de se connecter au compte admin via ssh avec les permissions sudo.

Les paquets suivants sont installés :

apt install bind9 dnsutils bind9-doc

Sur le serveur client, le fichier config /etc/bind/named.conf.options est modifié de cette manière :

```
GNU nano 7.2                                named.conf.options
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        192.168.104.254;
        172.16.0.254;
    };
    recursion yes;
    forward only;
    dnssec-validation yes;

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys.  See https://www.isc.org/bind-keys
    //=====
    //
    dnssec-validation auto;
}

[ Read 28 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo     M-A Set r
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/_ Go To Line M-E Redo     M-6 Copy
```

Le service bind9 avec **systemctl restart bind9** est en suite redémarré afin d'appliquer les changements.

Le serveur DNS 192.168.63.151 est en suite interrogé depuis la machine client 192.168.63.152 avec la commande :

dig ac-lille.fr @192.168.63.151

Création de notre propre zone DNS

Modification du fichier named.conf.local :

```
GNU nano 7.2                                named.conf.local
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "benard.btssiojb.local" {
    type master;
    file "/etc/bind/benard.btssiojb.local.ian";
};

[ Read 12 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location  M-U Undo     M-A Set f
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line M-E Redo     M-6 Copy
```

Création du fichier /etc/bind/benard.btssiojb.local.ian à partir du fichier, en le copiant, db.local :

```

GNU nano 7.2 /etc/bind/benard.btssiojb.local.1an
;
; BIND data file for local loopback interface
;
$TTL 604800
@ IN SOA ns.benard.btssiojb.local. benard.localhost. (
    2020409101 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS ns
@ IN A 127.0.0.1
@ IN AAAA ::1
ns IN A 192.168.63.151
nagios IN A 192.168.104.250

```

Read 16 lines

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set M
 ^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line M-E Redo M-G Copy

Résultat :

```

;; Query time: 25 msec
;; SERVER: 192.168.63.151#53(192.168.63.151) (UDP)
;; WHEN: Tue Sep 10 14:53:55 UTC 2024
;; MSG SIZE rcvd: 84

root@vb-debian-dns-client:~# dig ns.benard.btssiojb.local @192.168.63.151

; <<>> DiG 9.18.28-1~deb12u2-Debian <<>> ns.benard.btssiojb.local @192.168.63.151
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33536
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: 14b14ead686f346b0100000066e05e0068bb2a04e57f53d8 (good)
;; QUESTION SECTION:
ns.benard.btssiojb.local. IN A

;; ANSWER SECTION:
ns.benard.btssiojb.local. 604800 IN A 192.168.63.151

;; Query time: 0 msec
;; SERVER: 192.168.63.151#53(192.168.63.151) (UDP)
;; WHEN: Tue Sep 10 14:56:00 UTC 2024
;; MSG SIZE rcvd: 97

root@vb-debian-dns-client:~#

```

Configuration d'un DNS reverse :

Configuration du fichier named.conf.local

Copie du fichier benard.btssiojb.local.lan en 192.168.63.lan

```
GNU nano 7.2 /etc/bind/192.168.63.lan
;
; BIND data file for local loopback interface
;
$TTL 604800
@ IN SOA ns.benard.btssiojb.local. benard.localhost. (
    2020409101 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS ns
ns IN A 192.168.63.151
151 IN PTR ns.benard.btssiojb.local.
250 IN PTR nagios.benard.btssiojb.local.

// Organization
//include "/etc/bind/zones.rfc1918";

zone "benard.btssiojb.local" {
    type master;
    file "/etc/bind/benard.btssiojb.local.lan";
};

zone "63.168.192.in-addr.arpa" {
    type master;
    notify no;
    file "/etc/bind/192.168.63.lan";
};
```

Résultat :

```
in-addr.arpa.      517      IN      SOA      b.in-addr-servers.arpa. nstld.iana.org. 2022095034 1800 900 604800 3600

;; Query time: 1 msec
;; SERVER: 192.168.104.254#53(192.168.104.254) (UDP)
;; WHEN: Tue Sep 10 15:35:24 UTC 2024
;; MSG SIZE rcvd: 121

root@vb-debian-dns-client:~# dig -x 192.168.63.151 @192.168.63.151

;<<>> DiG 9.18.28-1~deb12u2-Debian <<>> -x 192.168.63.151 @192.168.63.151
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25893
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: 2f6969367e977e0d0100000066e06751a17115b048bcbbfc (good)
;; QUESTION SECTION:
;151.63.168.192.in-addr.arpa.      IN      PTR

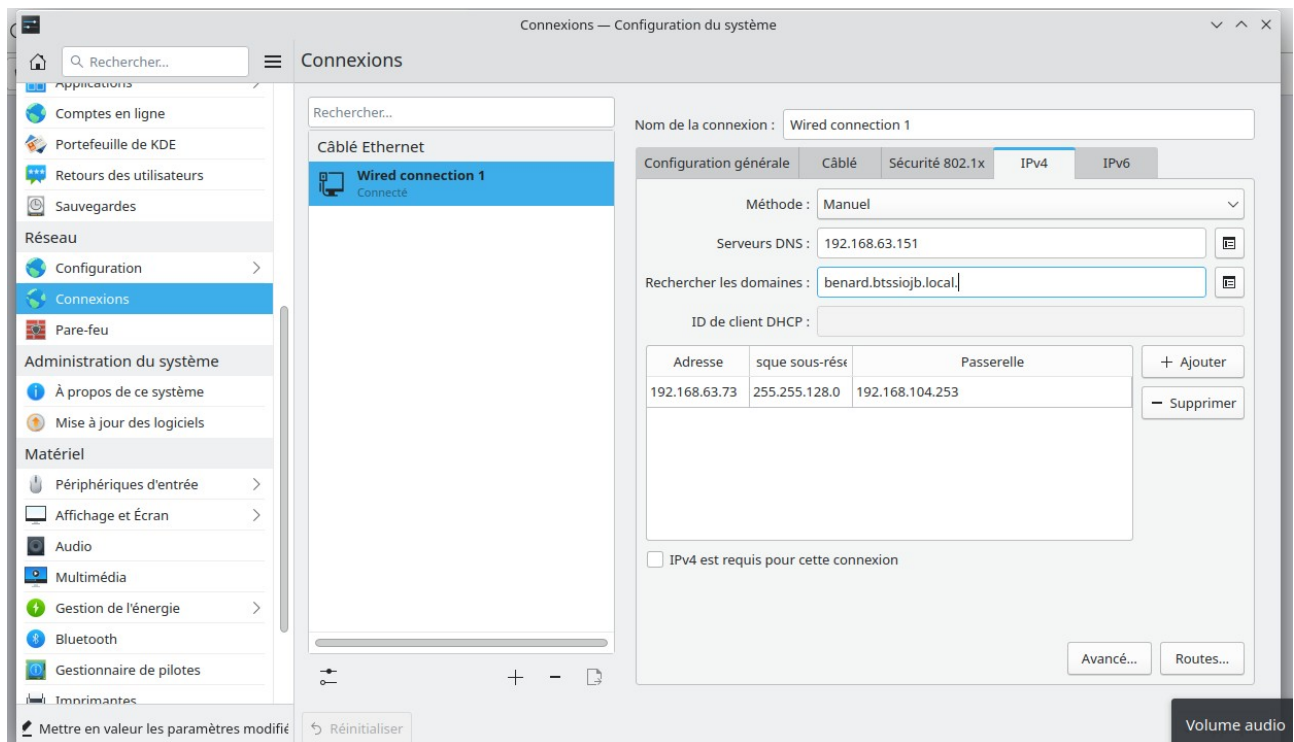
;; ANSWER SECTION:
151.63.168.192.in-addr.arpa. 604800 IN PTR      ns.benard.btssiojb.local.

;; Query time: 1 msec
;; SERVER: 192.168.63.151#53(192.168.63.151) (UDP)
;; WHEN: Tue Sep 10 15:35:45 UTC 2024
;; MSG SIZE rcvd: 122

root@vb-debian-dns-client:~#
```

Une machine Kubuntu est mise en place comme client.

Configuration ipv4



(PAS DE PROXY POUR FIREFOX)

Interrogation de www.benard.btssiojb.local via la machine Kubuntu

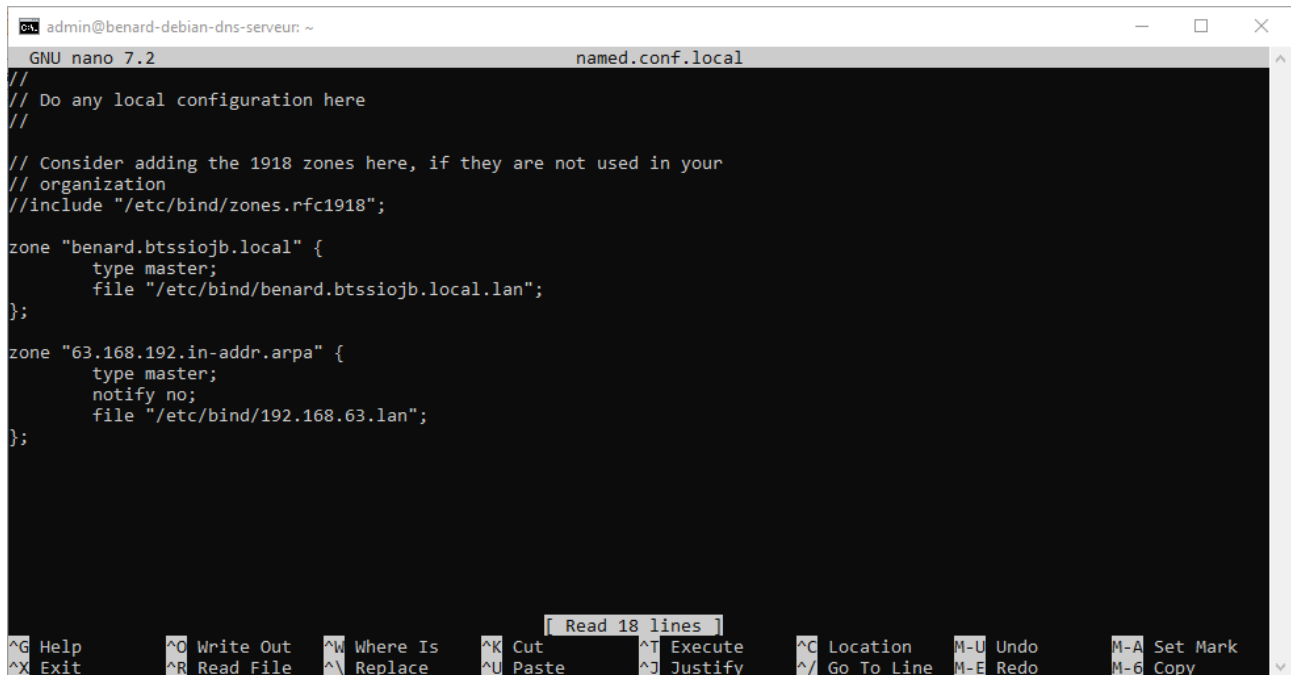
Ajout des enregistrements pour www dans les fichiers suivants

(fichier 63.168.192)

(fichier benard)

/ etc / bind

systemctl restart bind9

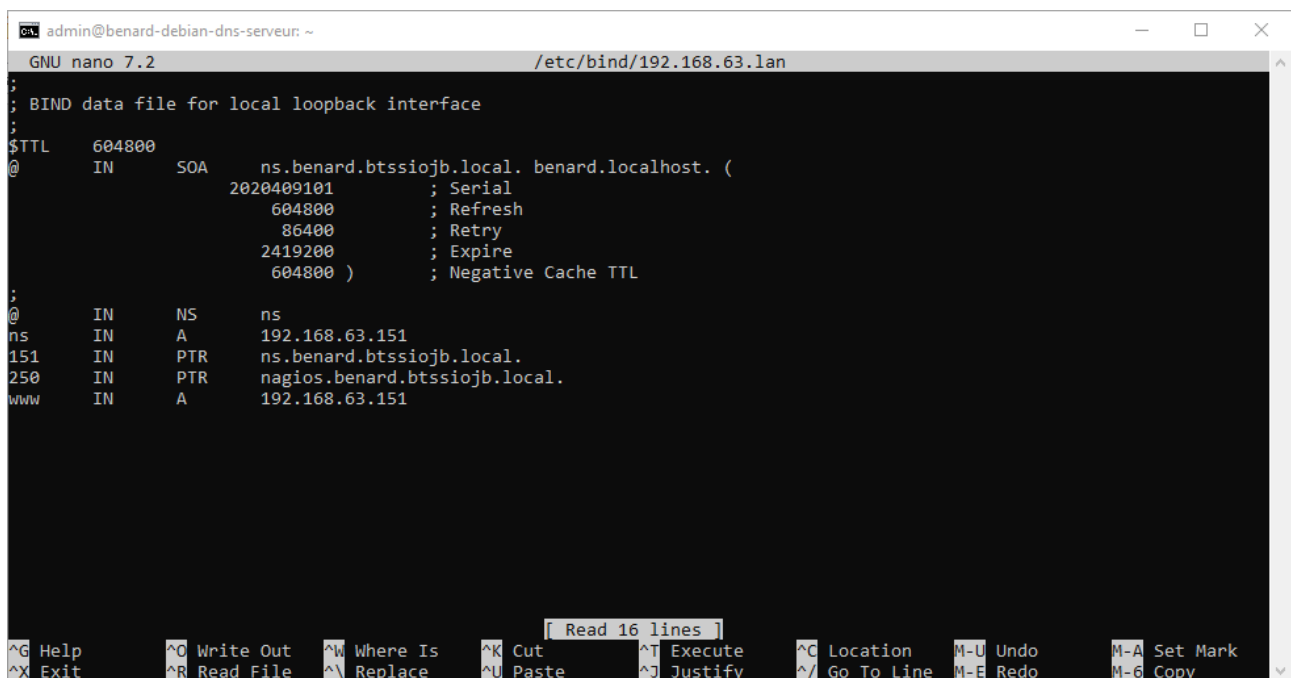


```
admin@benard-debian-dns-serveur: ~
GNU nano 7.2 named.conf.local
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "benard.btssiojb.local" {
    type master;
    file "/etc/bind/benard.btssiojb.local.1an";
};

zone "63.168.192.in-addr.arpa" {
    type master;
    notify no;
    file "/etc/bind/192.168.63.1an";
};

[ Read 18 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo     M-A Set Mark
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line M-E Redo     M-6 Copy
```



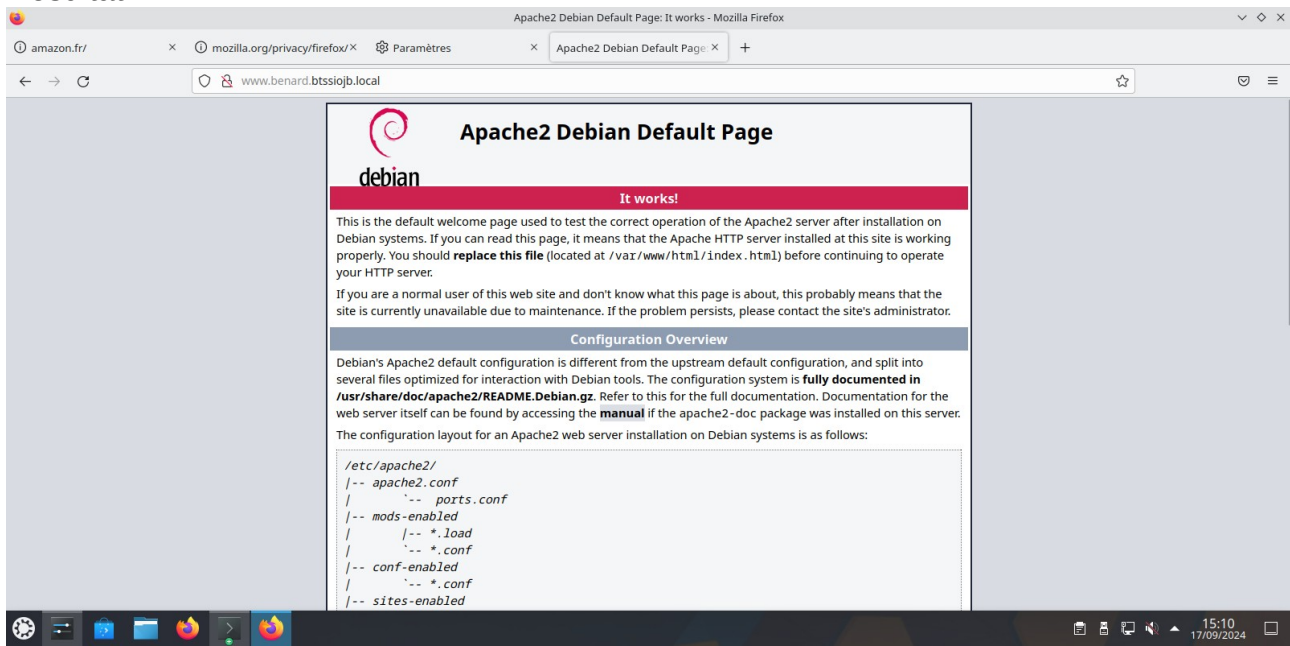
```
admin@benard-debian-dns-serveur: ~
GNU nano 7.2 /etc/bind/192.168.63.1an
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA     ns.benard.btssiojb.local. benard.localhost. (
        2020409101      ; Serial
        604800          ; Refresh
        86400           ; Retry
        2419200         ; Expire
        604800 )        ; Negative Cache TTL
;
@         IN      NS      ns
ns        IN      A       192.168.63.151
151       IN      PTR     ns.benard.btssiojb.local.
250       IN      PTR     nagios.benard.btssiojb.local.
www       IN      A       192.168.63.151

[ Read 16 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo     M-A Set Mark
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line M-E Redo     M-6 Copy
```

```
admin@benard-debian-dns-seveur: ~
GNU nano 7.2                                benard.btssiojb.local.lan
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      ns.benard.btssiojb.local. benard.localhost. (
; Serial
        2020409101      ; Refresh
        604800          ; Retry
        86400           ; Expire
        2419200         ; Negative Cache TTL
        )
;
@         IN      NS       ns
@         IN      A        127.0.0.1
@         IN      AAAA     ::1
ns        IN      A        192.168.63.151
nagios    IN      A        192.168.104.250
www       IN      A        192.168.63.151

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/_ Go To Line  M-E Redo      M-6 Copy
```

Résultat :



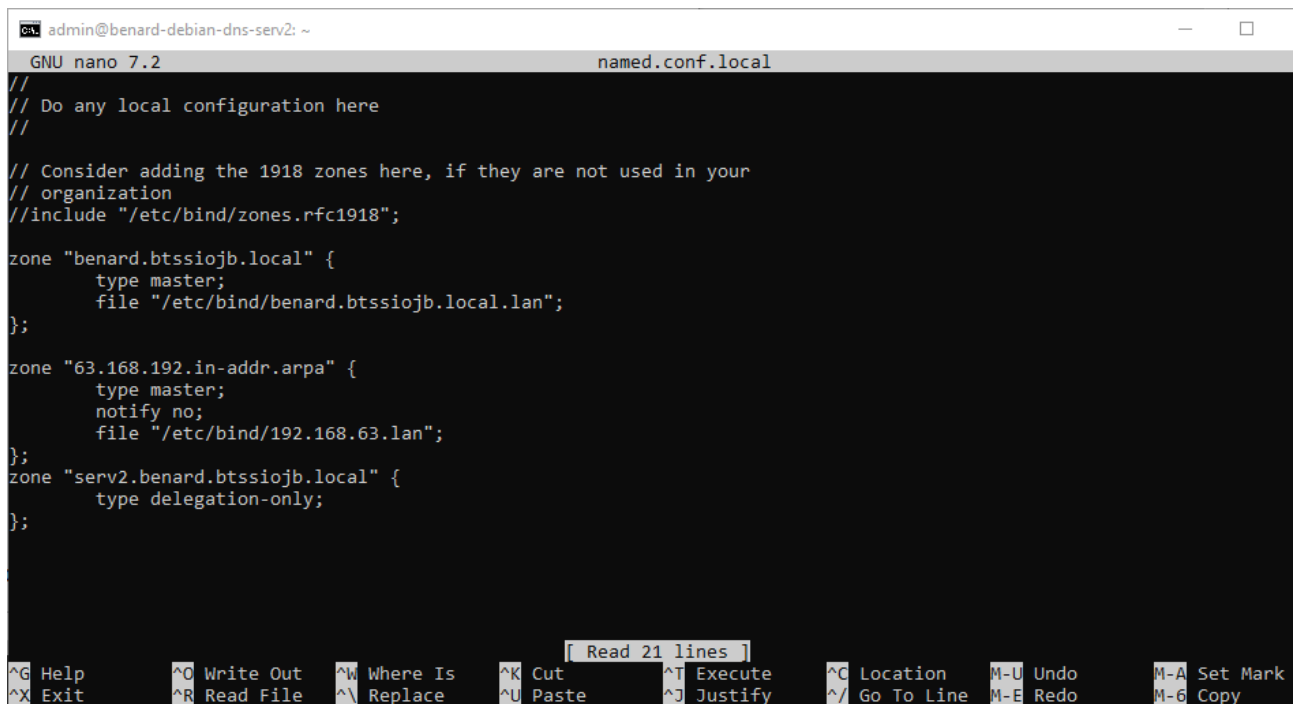
Ajout d'un serveur de delegation

Modification du fichier benard.btssiojb.local.lan

```
admin@benard-debian-dns-serv2: ~
GNU nano 7.2 benard.btssiojb.local.lan
;
; BIND data file for local loopback interface
;
$TTL 604800
@ IN SOA ns.benard.btssiojb.local. benard.localhost. (
    2020409101 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS ns
@ IN A 127.0.0.1
@ IN AAAA ::1
ns IN A 192.168.63.155
nagios IN A 192.168.104.250
www IN A 192.168.63.155
serv2 IN A ns2.benard.btssiojb.local.
ns2 IN A 192.168.104.231

Read 19 lines
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line M-E Redo M-6 Copy
```

Modification du fichier named.conf.local



```
admin@benard-debian-dns-serv2: ~
GNU nano 7.2 named.conf.local
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

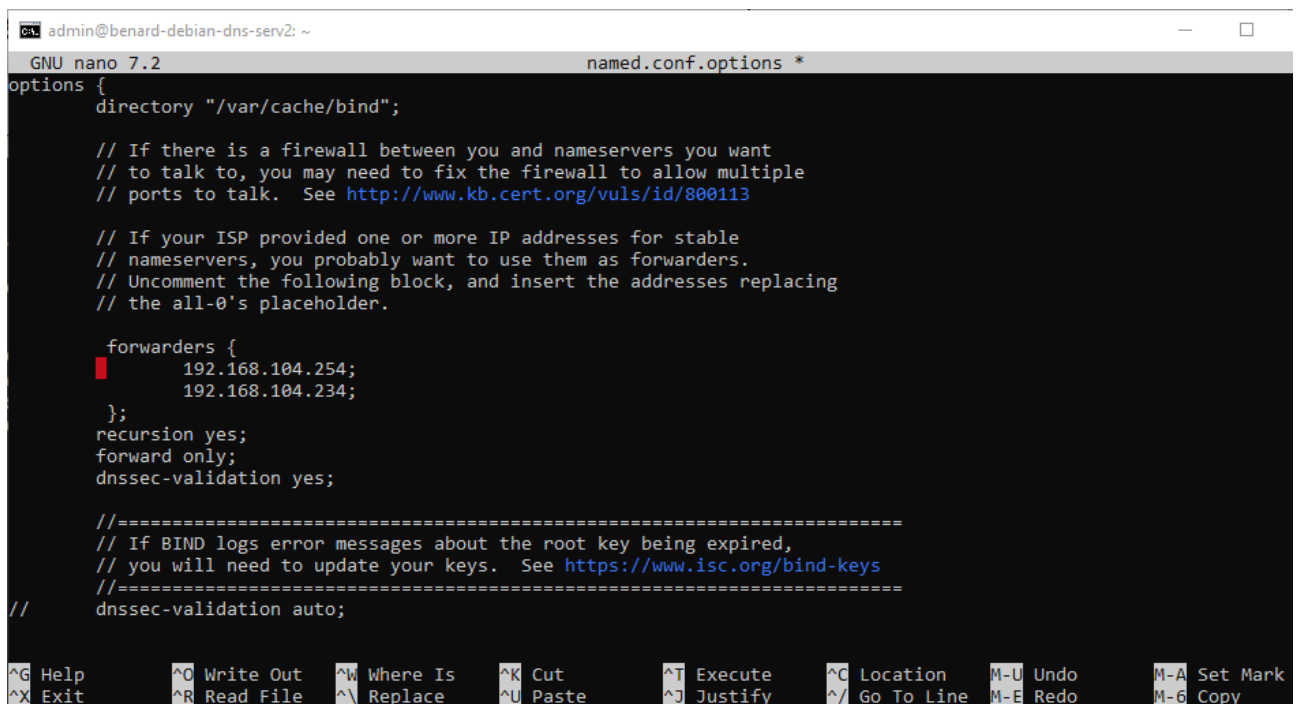
zone "benard.btssiojb.local" {
    type master;
    file "/etc/bind/benard.btssiojb.local.ian";
};

zone "63.168.192.in-addr.arpa" {
    type master;
    notify no;
    file "/etc/bind/192.168.63.ian";
};

zone "serv2.benard.btssiojb.local" {
    type delegation-only;
};

Read 21 lines
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark
^X Exit      ^R Read File  ^_ Replace    ^U Paste      ^J Justify    ^/ Go To Line  M-E Redo      M-6 Copy
```

Modification du fichier named.conf.options



```
admin@benard-debian-dns-serv2: ~
GNU nano 7.2 named.conf.options *
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        192.168.104.254;
        192.168.104.234;
    };
    recursion yes;
    forward only;
    dnssec-validation yes;

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys.  See https://www.isc.org/bind-keys
    //=====
    dnssec-validation auto;
}

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark
^X Exit      ^R Read File  ^_ Replace    ^U Paste      ^J Justify    ^/ Go To Line  M-E Redo      M-6 Copy
```

Création du fichier serv2.benard.btssiojb.local.ian via cp

```
admin@benard-debian-dns-serv2: ~
GNU nano 7.2 serv2.benard.btssiojb.local.lan
;
; BIND data file for local loopback interface
;
$ORIGIN serv2.benard.btssiojb.local.
$TTL 604800
@ IN SOA ns2.serv2.benard.btssiojb.local. benard.localhost. (
    2020409101 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS ns2.serv2.benard.btssiojb.local.
@ IN A 127.0.0.1
@ IN AAAA ::1
ns2 IN A 192.168.63.155
155 IN PTR ns2.serv2.benard.btssiojb.local.
client IN A 192.168.63.156
Read 18 lines
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line M-E Redo M-6 Copy
```

Maintenant édition de ce fichier :

```
admin@benard-debian-dns-serv2: ~
GNU nano 7.2 named.conf.local
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "benard.btssiojb.local" IN {
    type slave;
    file "/etc/bind/benard.btssiojb.local.lan";
    masters {192.168.63.155;};
};
zone "63.168.192.in-addr.arpa" {
    type slave;
    file "/var/cache/bind/192.168.63.lan";
    masters {192.168.63.155;};
};
zone "serv2.benard.btssiojb.local" IN {
    type master;
    file "/etc/bind/serv2.benard.btssiojb.local.lan";
};
Wrote 23 lines
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line M-E Redo M-6 Copy
```

Maintenant édition du fichier named.conf.options

```
admin@benard-debian-dns-serv2: ~
GNU nano 7.2 named.conf.options
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        192.168.63.155;
    };
    recursion yes;
    forward only;
    dnssec-validation yes;

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys.  See https://www.isc.org/bind-keys
    //=====
    // dnssec-validation auto;

    listen-on-v6 { any; };
}

[ Wrote 27 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo     M-A Set Mark
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo     M-6 Copy
```