

Administration Linux

M2i Formation –2021

MISE EN PLACE D'UNE INFRASTRUCTURE
RESEAU SOUS LINUX

DNS

INSTALLATION DU SERVEUR DNS

Prérequis : on installe les outils nécessaire au testage du DNS : *apt-get install dnsutils*

Configuration des fichiers

Modification du fichier hostname

```
root@srv-lx01:~# nano /etc/hostname
```

```
GNU nano 3.2 /etc/hostname

srv-lx01.m2i.local
```

On redémarre le serveur

On ajoute les lignes suivantes au fichier /etc/network/interfaces :

dns-nameservers 192.168.200.100

dns-domain m2i.local

```
GNU nano 3.2 /etc/network/interfaces

auto ens33
allow-hotplug ens33
#iface ens33 inet dhcp
iface ens33 inet static
address 192.168.200.100
netmask 255.255.255.0
network 192.168.200.0
broadcast 192.168.200.255
gateway 192.168.200.254
dns-nameservers 192.168.200.100
dns-domain m2i.local
```

On modifie le fichier hosts

```
root@srv-lx01:~# nano /etc/hosts
```

```
GNU nano 3.2 /etc/hosts

127.0.0.1    localhost
127.0.1.1    srv-lx01.m2i.local    srv-lx01
192.168.200.100 srv-lx01.m2i.local    srv-lx01
192.168.200.102 srv-lx02.m2i.local    srv-lx02
192.168.200.103 srv-lx03.m2i.local    srv-lx03
192.168.200.104 srv-lx04.m2i.local    srv-lx04
192.168.200.105 srv-lx05.m2i.local    srv-lx05

# The following lines are desirable for IPv6 capable hosts
::1    localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

On modifie le fichier resolv.conf (Attention ce fichier se réinitialise si on change d'adresse ip)

```
root@srv-lx01:~# nano /etc/resolv.conf
```

```
GNU nano 3.2 /etc/resolv.conf Modifié
domain m2i.local
search m2i.local
nameserver 192.168.200.100
```

Installation du paquet bind9

```
root@srv-lx01:~# apt-get install bind9
```

On modifie le fichier `/etc/bind/named.conf` en commentant la dernière ligne

```
GNU nano 3.2 /etc/bind/named.conf Modifié
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
//include "/etc/bind/named.conf.default-zones";
```

On modifie le fichier `/etc/bind/named.conf.local`

```
root@srv-lx01:~# nano /etc/bind/named.conf.local
```

```
GNU nano 3.2 /etc/bind/named.conf.local Modifié
//
// 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 "m2i.local" IN {
    type master;
    file "/var/cache/bind/db.m2i.local";
    allow-update { 127.0.0.1; };
};

zone "200.168.192.in-addr.arpa" IN {
    type master;
    file "/var/cache/bind/db.200.168.192.in-addr.arpa";
    allow-update { 127.0.0.1; };
};
```

On crée le fichier `db.m2i.local`

```
root@srv-lx01:~# nano /etc/bind/db.m2i.local
```

```

GNU nano 3.2 /etc/bind/db.m2i.local

$TTL      604800
$ORIGIN m2i.local.
@         IN      SOA      srv-lx01.m2i.local. root.m2i.local. (
                                20200324;
                                3h;
                                1h;
                                1w;
                                1h;
                                )
@         IN      NS       srv-lx01.m2i.local.
@         IN      MX       srv-lx03.m2i.local.
@         IN      AAAA     ::1
srv-lx01   IN      A       192.168.200.100
srv-lx02   IN      A       192.168.200.102
srv-lx03   IN      A       192.168.200.103
srv-lx04   IN      A       192.168.200.104
srv-lx05   IN      A       192.168.200.105
www        IN      CNAME    srv-lx02
webmail    IN      CNAME    srv-lx02

```

On crée le fichier db.200.168.192.in-addr.arpa pour la zone reverse

```
root@srv-lx01:~# nano /etc/bind/db.200.168.192.in-addr.arpa
```

```

GNU nano 3.2 db.200.168.192.in-addr.arpa

$TTL      604800
$ORIGIN 200.168.192.in-addr.arpa.
@         IN      SOA      srv-lx01.m2i.local. root.m2i.local. (
                                20200324;
                                3h;
                                1h;
                                1w;
                                1h;
                                )
@         IN      NS       srv-lx01.m2i.local.
100       IN      PTR      srv-lx01.m2i.local.
102       IN      PTR      srv-lx02.m2i.local.
103       IN      PTR      srv-lx03.m2i.local.
104       IN      PTR      srv-lx04.m2i.local.
105       IN      PTR      srv-lx05.m2i.local.

```

On déplace ces 2 fichiers db dans /var/cache/bind

```

root@srv-lx01:/etc/bind# mv db.m2i.local /var/cache/bind
root@srv-lx01:/etc/bind# mv db.200.168.192.in-addr.arpa /var/cache/bind

```

```

-rw-r--r-- 1 root bind 382 mars 27 15:27 db.200.168.192.in-addr.arpa
-rw-r--r-- 1 root bind 620 mars 27 15:36 db.m2i.local
-rw-r--r-- 1 bind bind 821 mars 27 14:51 managed-keys.bind
-rw-r--r-- 1 bind bind 512 mars 27 14:51 managed-keys.bind.jnl

```

On modifie le propriétaire sur ces 2 fichiers de façon à ce que bind soit le nouveau propriétaire

```
root@srv-lx01:/var/cache/bind# chown bind db.m2i.local
root@srv-lx01:/var/cache/bind# chown bind db.200.168.192.in-addr.arpa
```

```
-rw-r--r-- 1 bind bind 382 mars 27 15:27 db.200.168.192.in-addr.arpa
-rw-r--r-- 1 bind bind 620 mars 27 15:36 db.m2i.local
-rw-r--r-- 1 bind bind 821 mars 27 14:51 managed-keys.bind
-rw-r--r-- 1 bind bind 512 mars 27 14:51 managed-keys.bind.jnl
```

On supprime tous les autres fichiers db.* dans /etc/bind

```
root@srv-lx01:/etc/bind# rm db.*
```

On commente les 2 dernières lignes du fichier /etc/bind/named.conf.options

```
GNU nano 3.2 /etc/bind/named.conf.options Modifié

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 {
    // 0.0.0.0;
    // };

    //=====
    // 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 { all; };
};
```

On modifie le fichier /etc/default/bind9 : ajout de -4 sur la dernière ligne pour supprimer les erreurs

```
root@srv-lx01:~# nano /etc/default/bind9
```

```
GNU nano 3.2 /etc/default/bind9

#
# run resolvconf?
RESOLVCONF=no

# startup options for the server
OPTIONS="-u bind -4"
```

On modifie les lignes suivantes dans le fichier /etc/dhcp/dhcpd.conf :

```
#option domain-name "example.org";
#option domain-name-servers ns1.example.org, ns2.example.org;
# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
#ddns-update-style none;
ddns-updates on;
ddns-update-style interim;
# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
log-facility local7;
ignore client-updates;
update-static-leases on;
allow-unknown-client;
zone m2i.local. {
    primary 127.0.0.1;
}
zone 200.168.192.in-addr.arpa. {
    primary 127.0.0.1;
}
```

On vérifie la configuration avec la commande named-checkconf -z

```
root@srv-lx01:~# named-checkconf -z
zone m2i.local/IN: loaded serial 20200324
zone 200.168.192.in-addr.arpa/IN: loaded serial 20200324
```

On redémarre le service et on vérifie le status

```
root@srv-lx01:~# systemctl stop bind9
root@srv-lx01:~# systemctl start bind9
root@srv-lx01:~# systemctl status bind9
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2020-03-28 15:17:48 CET; 20s ago
     Docs: man:named(8)
  Process: 929 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
 Main PID: 930 (named)
    Tasks: 4 (limit: 1120)
   Memory: 12.1M
   CGroup: /system.slice/bind9.service
           └─930 /usr/sbin/named -u bind -4

mars 28 15:17:48 srv-lx01.m2i.local named[930]: none:106: 'max-cache-size 90%' - setting to 866MB (out of 96
mars 28 15:17:48 srv-lx01.m2i.local named[930]: configuring command channel from '/etc/bind/rndc.key'
mars 28 15:17:48 srv-lx01.m2i.local named[930]: command channel listening on 127.0.0.1#953
mars 28 15:17:48 srv-lx01.m2i.local named[930]: managed-keys-zone: journal file is out of date: removing jou
mars 28 15:17:48 srv-lx01.m2i.local named[930]: managed-keys-zone: loaded serial 6
mars 28 15:17:48 srv-lx01.m2i.local named[930]: zone 200.168.192.in-addr.arpa/IN: loaded serial 20200324
mars 28 15:17:48 srv-lx01.m2i.local named[930]: zone m2i.local/IN: loaded serial 20200324
mars 28 15:17:48 srv-lx01.m2i.local named[930]: all zones loaded
mars 28 15:17:48 srv-lx01.m2i.local systemd[1]: Started BIND Domain Name Server.
mars 28 15:17:48 srv-lx01.m2i.local named[930]: running
```