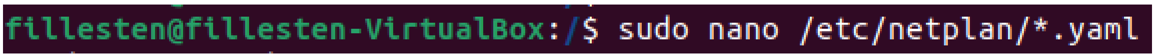
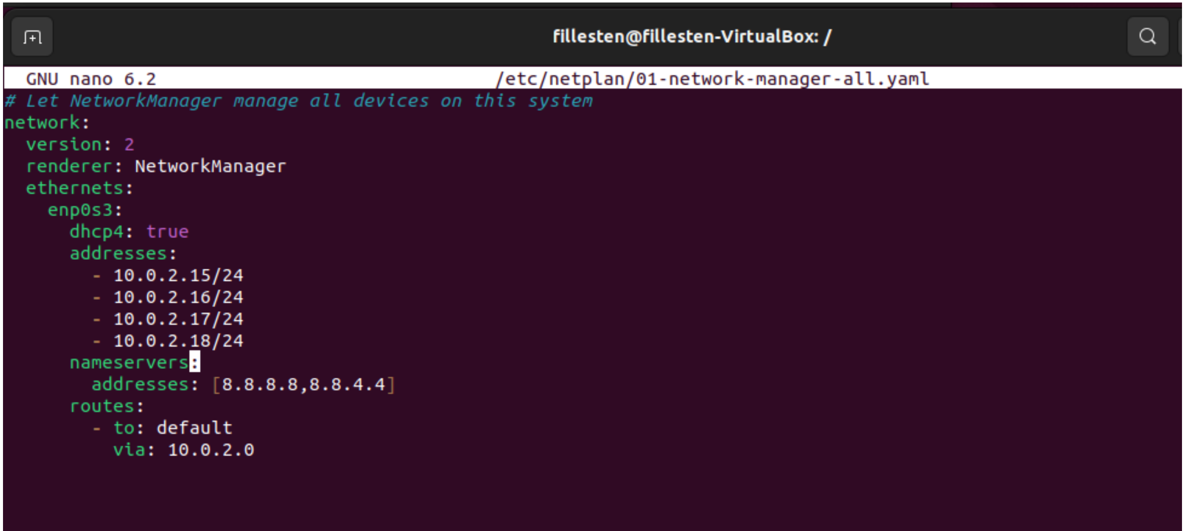
Administration av UNIX lab 4

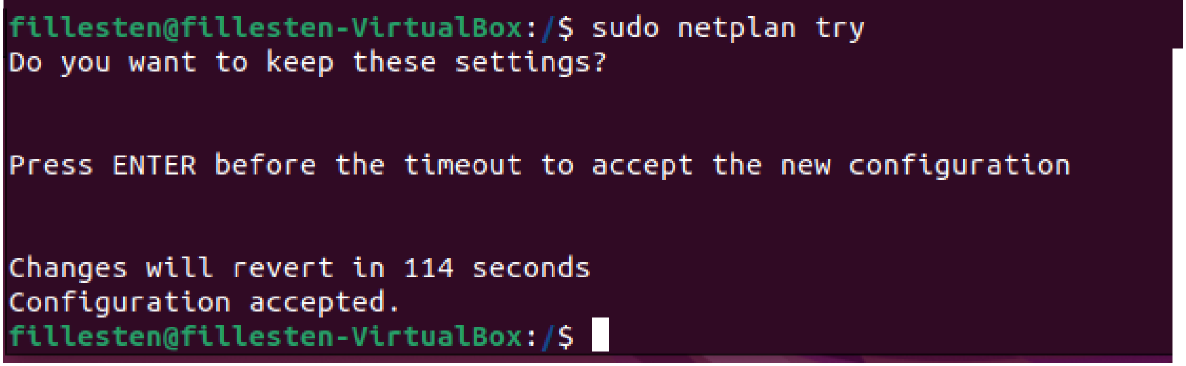
4.1.1 Pre-installation



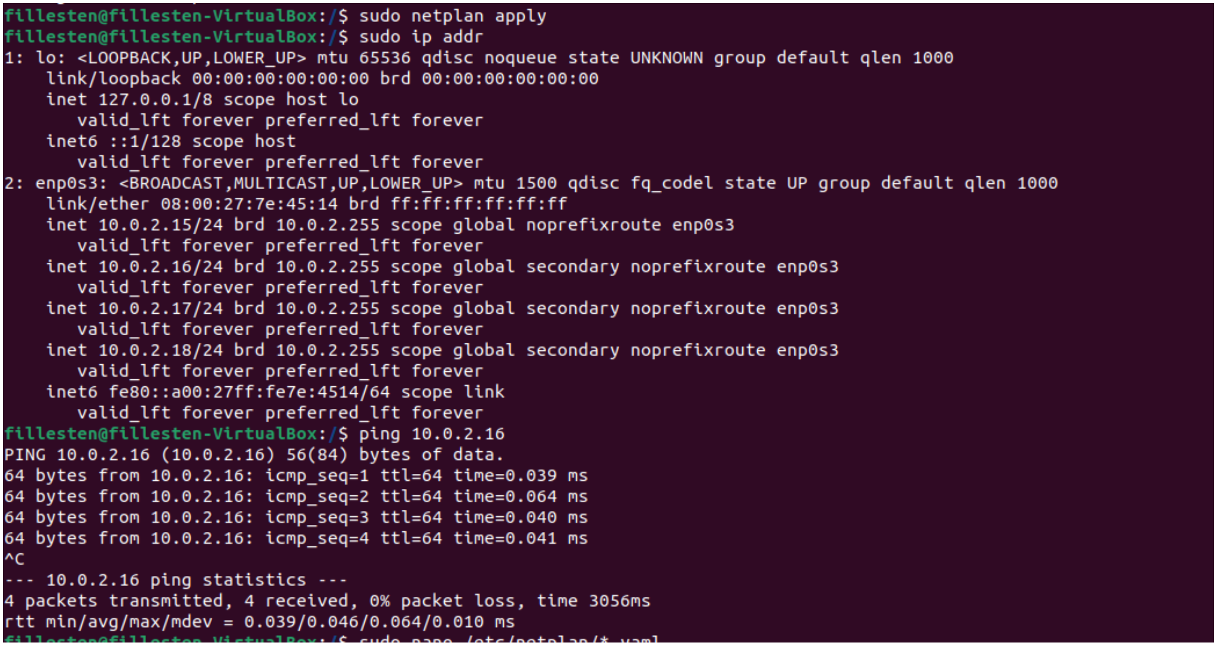
```
fillesten@fillesten-VirtualBox:/$ sudo nano /etc/netplan/*.yaml
```



```
  GNU nano 6.2                           /etc/netplan/01-network-manager-all.yaml
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enp0s3:
      dhcp4: true
      addresses:
        - 10.0.2.15/24
        - 10.0.2.16/24
        - 10.0.2.17/24
        - 10.0.2.18/24
      nameservers:
        addresses: [8.8.8.8,8.8.4.4]
      routes:
        - to: default
          via: 10.0.2.0
```



```
fillesten@fillesten-VirtualBox:/$ sudo netplan try
Do you want to keep these settings?


Press ENTER before the timeout to accept the new configuration


Changes will revert in 114 seconds
Configuration accepted.
fillesten@fillesten-VirtualBox:/$ 
```



```
fillesten@fillesten-VirtualBox:/$ sudo netplan apply
fillesten@fillesten-VirtualBox:/$ sudo ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:7e:45:14 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet 10.0.2.16/24 brd 10.0.2.255 scope global secondary noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet 10.0.2.17/24 brd 10.0.2.255 scope global secondary noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet 10.0.2.18/24 brd 10.0.2.255 scope global secondary noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe7e:4514/64 scope link
       valid_lft forever preferred_lft forever
fillesten@fillesten-VirtualBox:/$ ping 10.0.2.16
PING 10.0.2.16 (10.0.2.16) 56(84) bytes of data.
64 bytes from 10.0.2.16: icmp_seq=1 ttl=64 time=0.039 ms
64 bytes from 10.0.2.16: icmp_seq=2 ttl=64 time=0.064 ms
64 bytes from 10.0.2.16: icmp_seq=3 ttl=64 time=0.040 ms
64 bytes from 10.0.2.16: icmp_seq=4 ttl=64 time=0.041 ms
^C
--- 10.0.2.16 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3056ms
rtt min/avg/max/mdev = 0.039/0.046/0.064/0.010 ms
fillesten@fillesten-VirtualBox:/$ sudo nano /etc/netplan/*.yaml
```

Pinging a new address works.

4.1.2 Installation

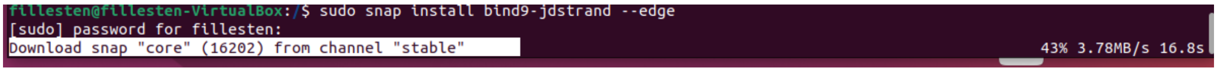
- Discuss the advantages and disadvantages of running containers instead of installing Bind9 with apt.

Running applications within containers has some advantages, like enhanced security and reliability through isolation from other applications and the host system. Containers offer better portability, allowing you to easily move them between various Linux distributions and different operating systems, this makes them a valuable choice for cloud deployments or heterogeneous server environments. Containers are also more resource-efficient, it shares the host systems kernel and enables the operation of multiple containers on a single server which can reduce hardware costs.

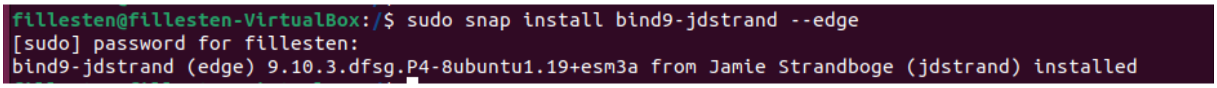
Managing containers can introduce complexity to systems as you need to handle container runtimes and images. This complexity can be mitigated with the help of container management tools like Kubernetes.

When comparing this to the traditional installation method using apt for package management, containers offer greater flexibility and isolation. apt is a package manager for the host system, while containers encapsulate the application and its dependencies, ensuring that it operates consistently regardless of the host's configuration.

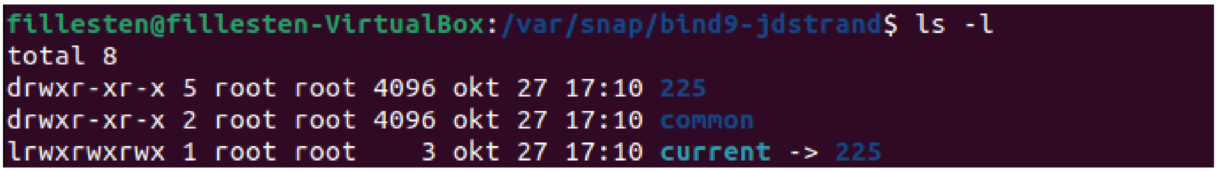
- Describe the installation process of installing with Snap.



```
fillesten@fillesten-VirtualBox:/$ sudo snap install bind9-jdstrand --edge
[sudo] password for fillesten:
Download snap "core" (16202) from channel "stable"                                    43% 3.78MB/s 16.8s
```

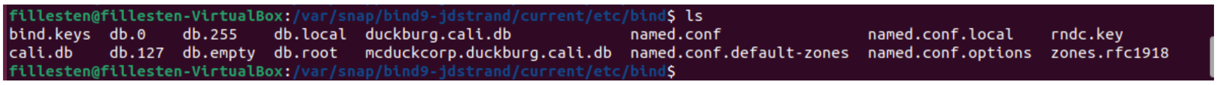


```
fillesten@fillesten-VirtualBox:/$ sudo snap install bind9-jdstrand --edge
[sudo] password for fillesten:
bind9-jdstrand (edge) 9.10.3.dfsg.P4-8ubuntu1.19+esm3a from Jamie Strandboge (jdstrand) installed
```



```
fillesten@fillesten-VirtualBox:/var/snap/bind9-jdstrand$ ls -l
total 8
drwxr-xr-x 5 root root 4096 okt 27 17:10 225
drwxr-xr-x 2 root root 4096 okt 27 17:10 common
lrwxrwxrwx 1 root root    3 okt 27 17:10 current -> 225
```

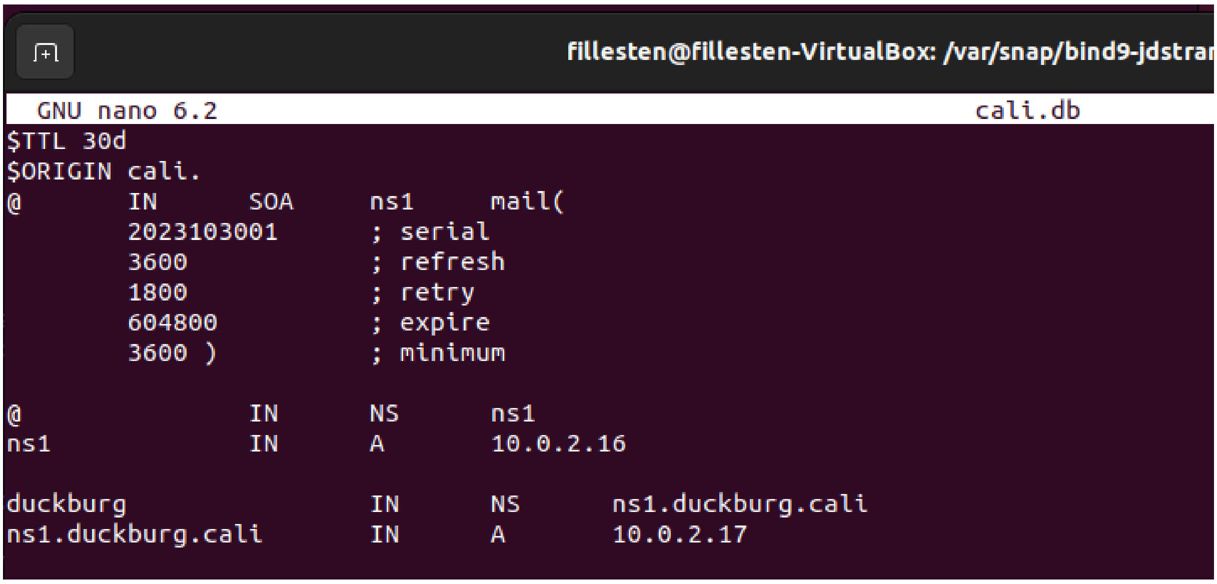
Current is a symbolic link to 225.



```
fillesten@fillesten-VirtualBox:/var/snap/bind9-jdstrand/current/etc/bind$ ls
bind.keys  db.0    db.255    db.local  duckburg.cali.db           named.conf                 named.conf.local    rndc.key
cali.db    db.127  db.empty  db.root   mcduckcorp.duckburg.cali.db named.conf.default-zones  named.conf.options  zones.rfc1918
fillesten@fillesten-VirtualBox:/var/snap/bind9-jdstrand/current/etc/bind$
```

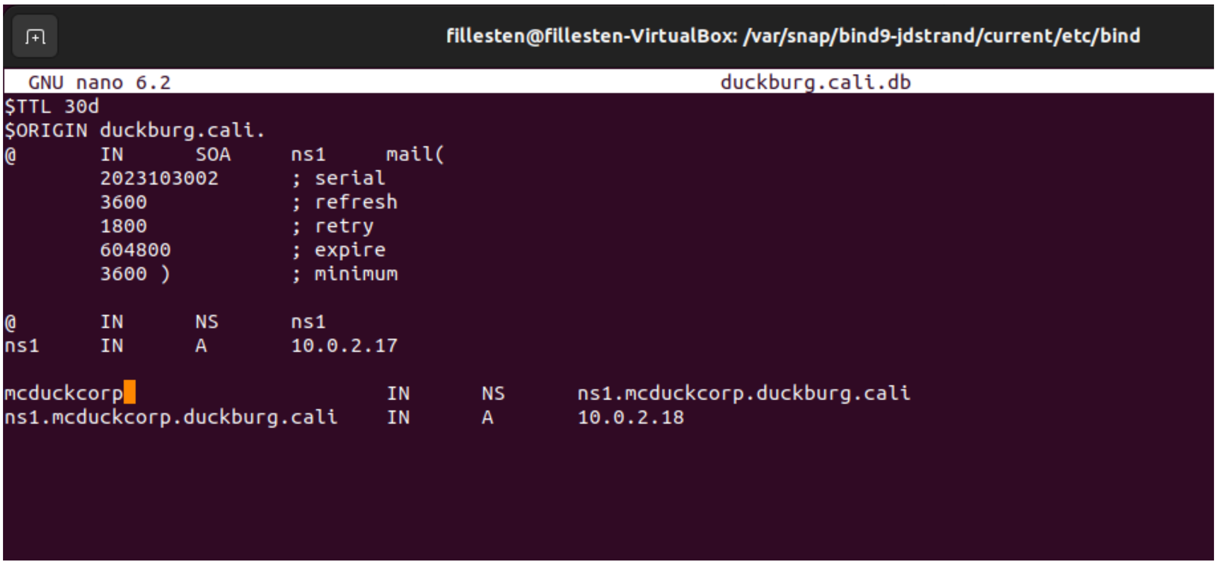
All the domains in the bind directory.

The cali.db file:



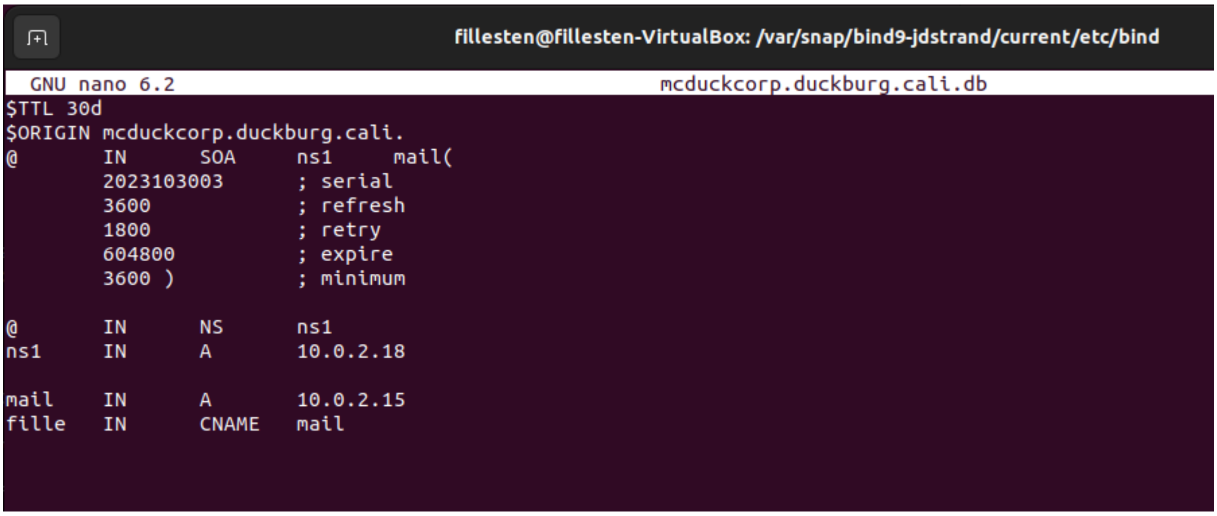
```
fillesten@fillesten-VirtualBox: /var/snap/bind9-jdstra
  GNU nano 6.2                                            cali.db
$TTL 30d
$ORIGIN cali.
@       IN      SOA     ns1     mail(
        2023103001      ; serial
        3600            ; refresh
        1800            ; retry
        604800          ; expire
        3600 )          ; minimum

@               IN      NS      ns1
ns1             IN      A       10.0.2.16

duckburg                IN      NS      ns1.duckburg.cali
ns1.duckburg.cali       IN      A       10.0.2.17
```

The duckburg.cali.db file:



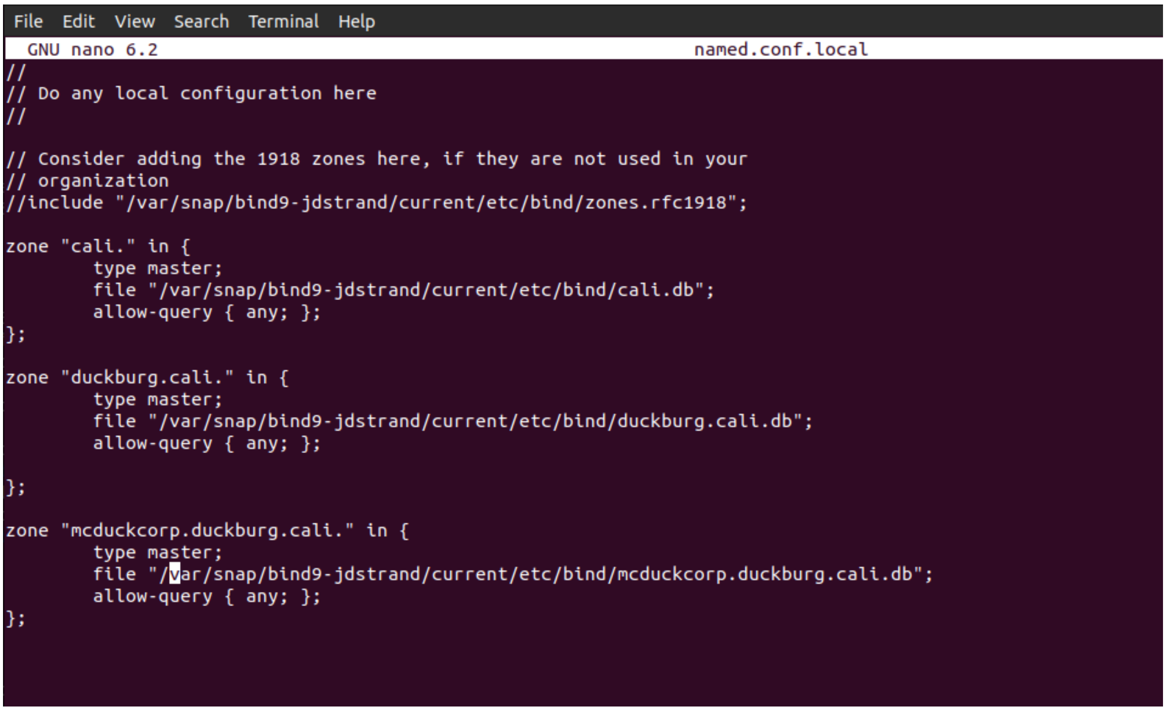
```
fillesten@fillesten-VirtualBox: /var/snap/bind9-jdstrand/current/etc/bind
  GNU nano 6.2                                            duckburg.cali.db
$TTL 30d
$ORIGIN duckburg.cali.
@       IN      SOA     ns1     mail(
        2023103002      ; serial
        3600            ; refresh
        1800            ; retry
        604800          ; expire
        3600 )          ; minimum

@       IN      NS      ns1
ns1     IN      A       10.0.2.17

mcduckcorp                      IN      NS      ns1.mcduckcorp.duckburg.cali
ns1.mcduckcorp.duckburg.cali    IN      A       10.0.2.18
```

The mcduckcorp.duckburg.cali.db file:



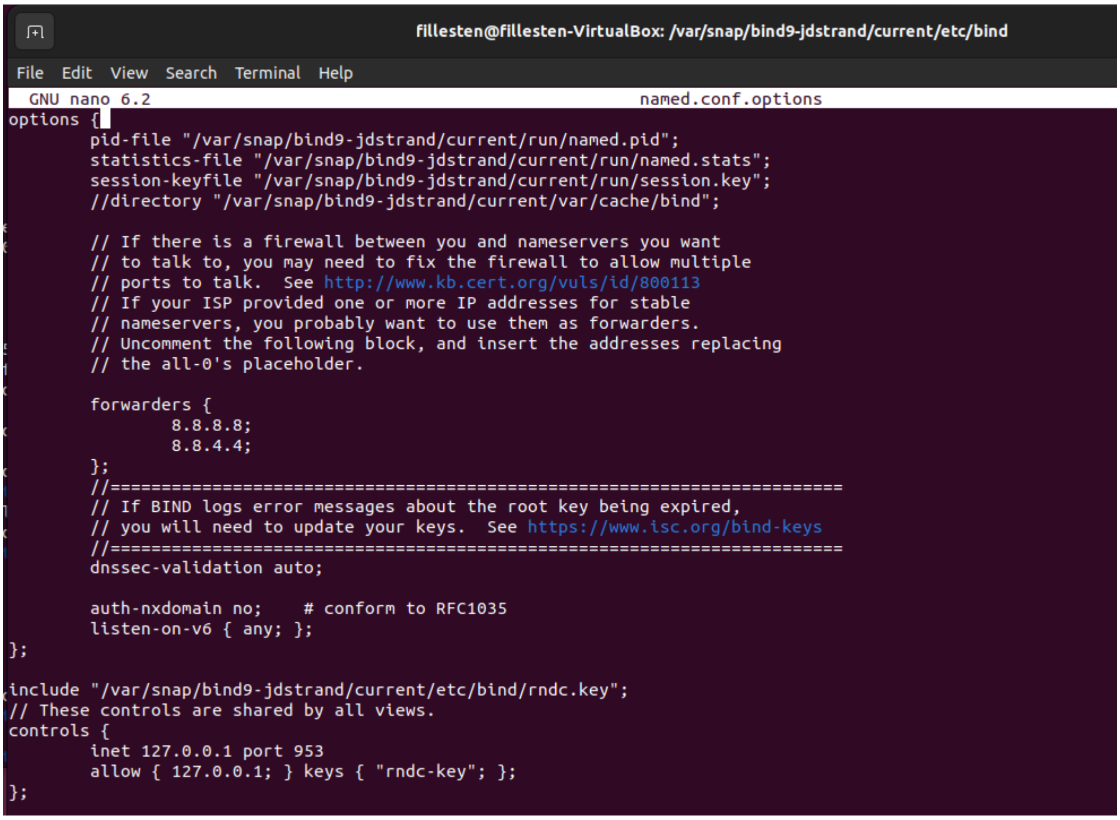
```
fillesten@fillesten-VirtualBox: /var/snap/bind9-jdstrand/current/etc/bind
  GNU nano 6.2                                  mcduckcorp.duckburg.cali.db
$TTL 30d
$ORIGIN mcduckcorp.duckburg.cali.
@       IN      SOA     ns1     mail(
        2023103003      ; serial
        3600            ; refresh
        1800            ; retry
        604800          ; expire
        3600 )          ; minimum

@       IN      NS      ns1
ns1     IN      A       10.0.2.18

mail    IN      A       10.0.2.15
fille   IN      CNAME   mail
```

Configured the named.conf.local file:



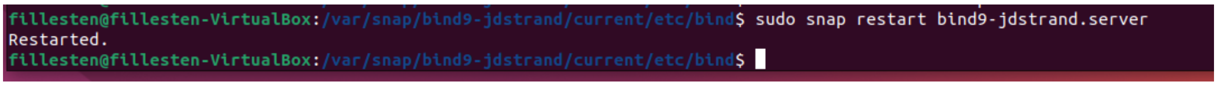
```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/var/snap/bind9-jdstrand/current/etc/bind/zones.rfc1918";

zone "cali." in {
        type master;
        file "/var/snap/bind9-jdstrand/current/etc/bind/cali.db";
        allow-query { any; };
};

zone "duckburg.cali." in {
        type master;
        file "/var/snap/bind9-jdstrand/current/etc/bind/duckburg.cali.db";
        allow-query { any; };

};

zone "mcduckcorp.duckburg.cali." in {
        type master;
        file "/var/snap/bind9-jdstrand/current/etc/bind/mcduckcorp.duckburg.cali.db";
        allow-query { any; };
};
```

Change to google DNS inside of named.conf.options file:


fillesten@fillesten-VirtualBox: /var/snap/bind9-jdstrand/current/etc/bind
File Edit View Search Terminal Help
GNU nano 6.2
named.conf.options

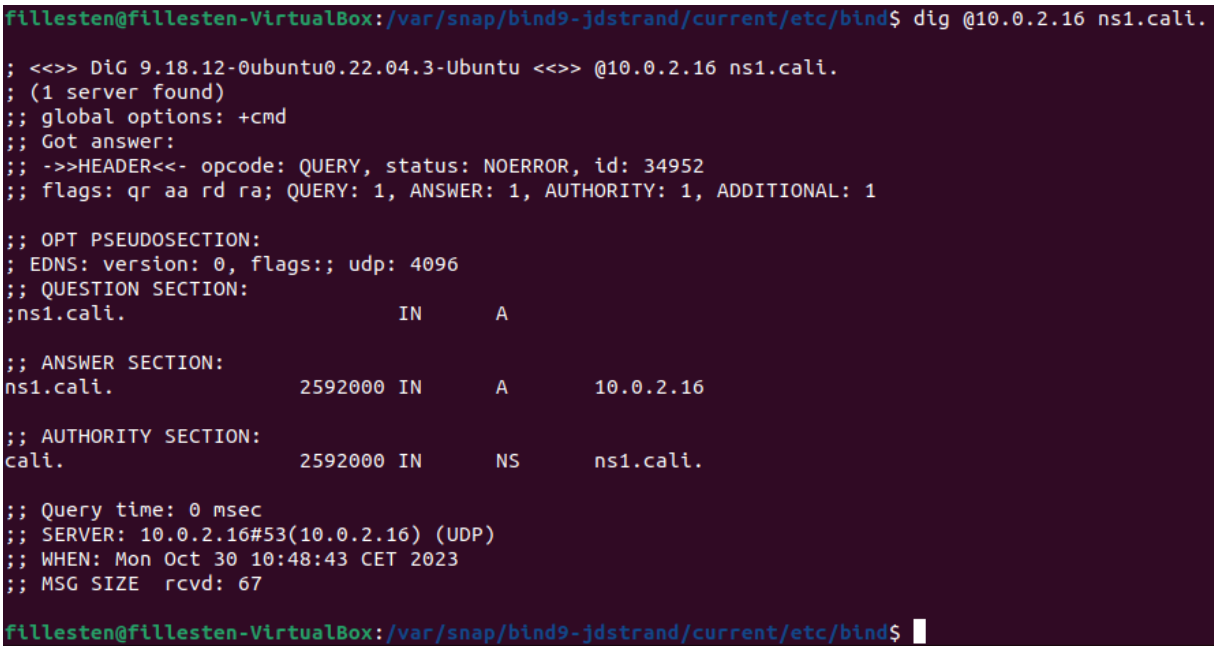
```
options {
        pid-file "/var/snap/bind9-jdstrand/current/run/named.pid";
        statistics-file "/var/snap/bind9-jdstrand/current/run/named.stats";
        session-keyfile "/var/snap/bind9-jdstrand/current/run/session.key";
        //directory "/var/snap/bind9-jdstrand/current/var/cache/bind";

        // 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 {
                8.8.8.8;
                8.8.4.4;
        };
        //========================================================================
        // 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;

        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
};

include "/var/snap/bind9-jdstrand/current/etc/bind/rndc.key";
// These controls are shared by all views.
controls {
        inet 127.0.0.1 port 953
        allow { 127.0.0.1; } keys { "rndc-key"; };
};
```

Restart server to apply new settings:

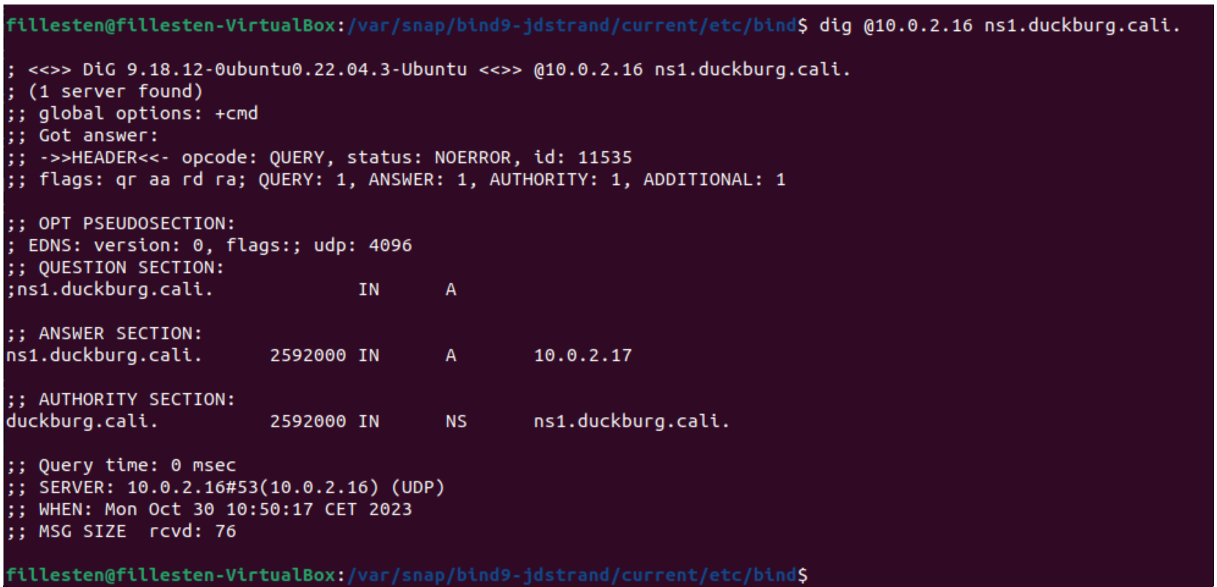


```
fillesten@fillesten-VirtualBox:/var/snap/bind9-jdstrand/current/etc/bind$ sudo snap restart bind9-jdstrand.server
Restarted.
fillesten@fillesten-VirtualBox:/var/snap/bind9-jdstrand/current/etc/bind$
```

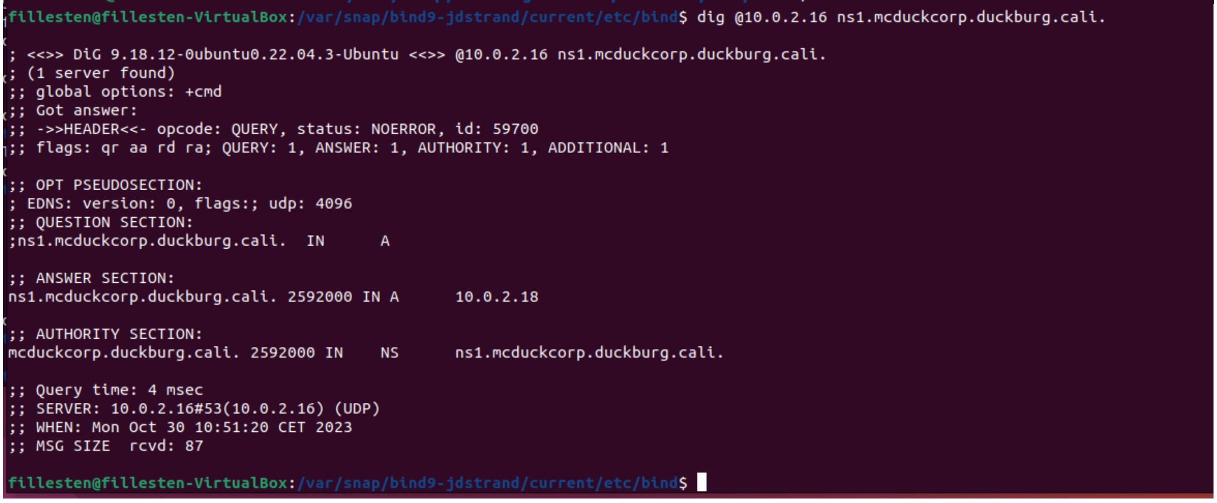
Testing with dig command on each zone:



```
fillesten@fillesten-VirtualBox:/var/snap/bind9-jdstrand/current/etc/bind$ dig @10.0.2.16 ns1.cali.

; <<>> DiG 9.18.12-0ubuntu0.22.04.3-Ubuntu <<>> @10.0.2.16 ns1.cali.
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34952
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ns1.cali.                      IN      A

;; ANSWER SECTION:
ns1.cali.               2592000 IN      A       10.0.2.16

;; AUTHORITY SECTION:
cali.                   2592000 IN      NS      ns1.cali.

;; Query time: 0 msec
;; SERVER: 10.0.2.16#53(10.0.2.16) (UDP)
;; WHEN: Mon Oct 30 10:48:43 CET 2023
;; MSG SIZE  rcvd: 67

fillesten@fillesten-VirtualBox:/var/snap/bind9-jdstrand/current/etc/bind$ 
```

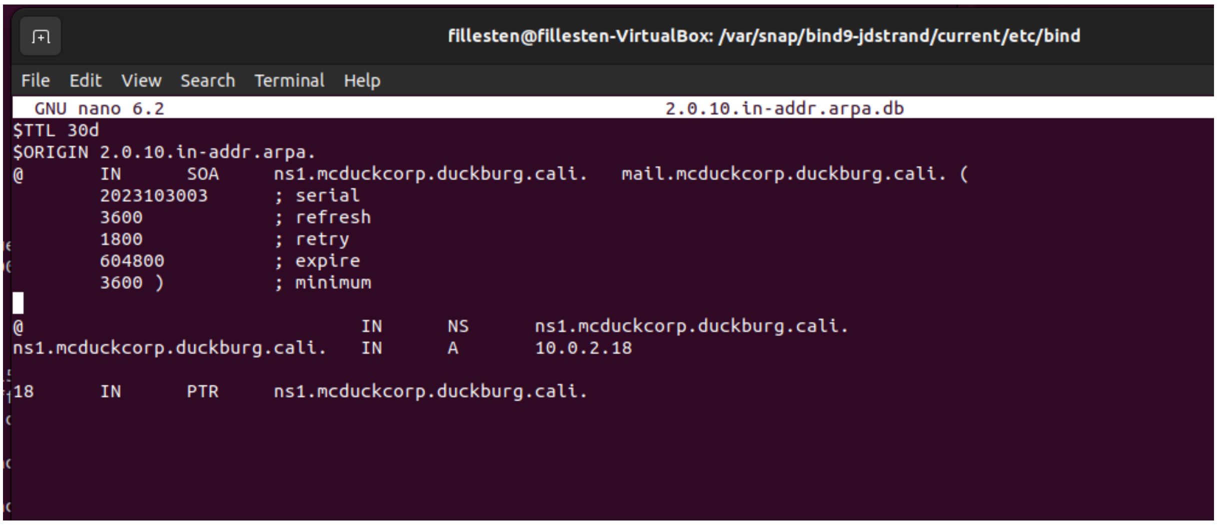


```
fillesten@fillesten-VirtualBox:/var/snap/bind9-jdstrand/current/etc/bind$ dig @10.0.2.16 ns1.duckburg.cali.

; <<>> DiG 9.18.12-0ubuntu0.22.04.3-Ubuntu <<>> @10.0.2.16 ns1.duckburg.cali.
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11535
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ns1.duckburg.cali.             IN      A

;; ANSWER SECTION:
ns1.duckburg.cali.      2592000 IN      A       10.0.2.17

;; AUTHORITY SECTION:
duckburg.cali.          2592000 IN      NS      ns1.duckburg.cali.

;; Query time: 0 msec
;; SERVER: 10.0.2.16#53(10.0.2.16) (UDP)
;; WHEN: Mon Oct 30 10:50:17 CET 2023
;; MSG SIZE  rcvd: 76

fillesten@fillesten-VirtualBox:/var/snap/bind9-jdstrand/current/etc/bind$
```



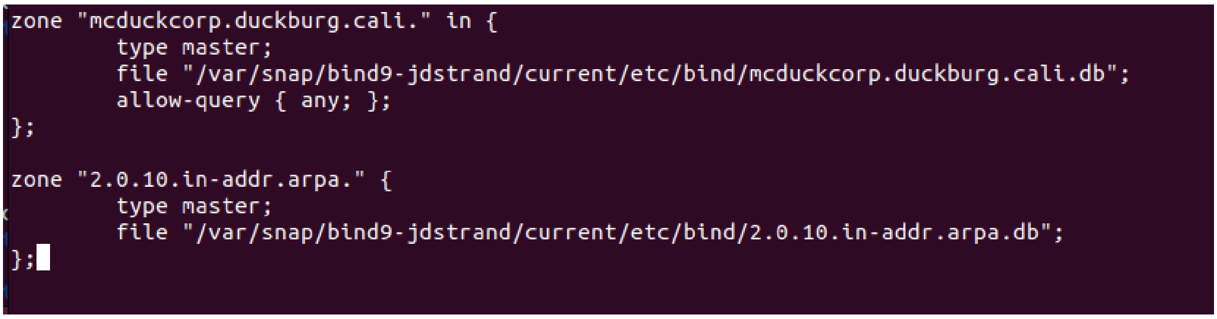
```
fillesten@fillesten-VirtualBox:/var/snap/bind9-jdstrand/current/etc/bind$ dig @10.0.2.16 ns1.mcduckcorp.duckburg.cali.

; <<>> DiG 9.18.12-0ubuntu0.22.04.3-Ubuntu <<>> @10.0.2.16 ns1.mcduckcorp.duckburg.cali.
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59700
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ns1.mcduckcorp.duckburg.cali.  IN      A

;; ANSWER SECTION:
ns1.mcduckcorp.duckburg.cali. 2592000 IN A      10.0.2.18

;; AUTHORITY SECTION:
mcduckcorp.duckburg.cali. 2592000 IN    NS      ns1.mcduckcorp.duckburg.cali.

;; Query time: 4 msec
;; SERVER: 10.0.2.16#53(10.0.2.16) (UDP)
;; WHEN: Mon Oct 30 10:51:20 CET 2023
;; MSG SIZE  rcvd: 87

fillesten@fillesten-VirtualBox:/var/snap/bind9-jdstrand/current/etc/bind$ 
```

Now for configuring the reverse lookup. Normal dns maps letters/names to ip. This however maps ip to letters/names.


fillesten@fillesten-VirtualBox: /var/snap/bind9-jdstrand/current/etc/bind
File Edit View Search Terminal Help

```
  GNU nano 6.2                                          2.0.10.in-addr.arpa.db
$TTL 30d
$ORIGIN 2.0.10.in-addr.arpa.
@       IN      SOA     ns1.mcduckcorp.duckburg.cali.   mail.mcduckcorp.duckburg.cali. (
        2023103003      ; serial
        3600            ; refresh
        1800            ; retry
        604800          ; expire
        3600 )          ; minimum

@                               IN      NS      ns1.mcduckcorp.duckburg.cali.
ns1.mcduckcorp.duckburg.cali.   IN      A       10.0.2.18

18      IN      PTR     ns1.mcduckcorp.duckburg.cali.
```

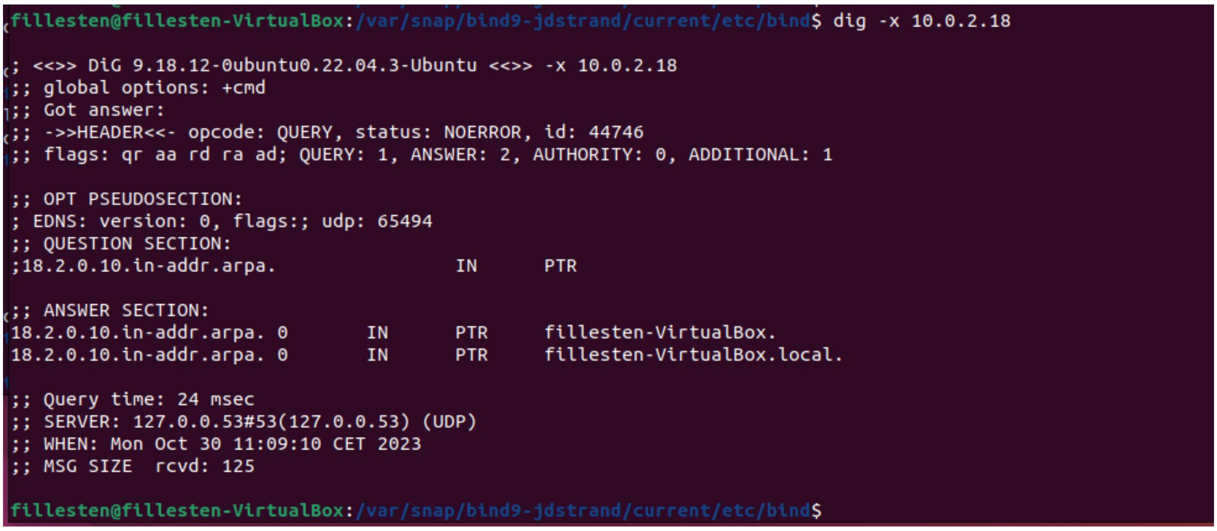
Also need to update named.conf.local to add the reverse zone.:



```
zone "mcduckcorp.duckburg.cali." in {
        type master;
        file "/var/snap/bind9-jdstrand/current/etc/bind/mcduckcorp.duckburg.cali.db";
        allow-query { any; };
};

zone "2.0.10.in-addr.arpa." {
        type master;
        file "/var/snap/bind9-jdstrand/current/etc/bind/2.0.10.in-addr.arpa.db";
};
```

The file looks the same above the mcduckcorp.duckburh.cali. clause.

Testing the reverse zone with dig:

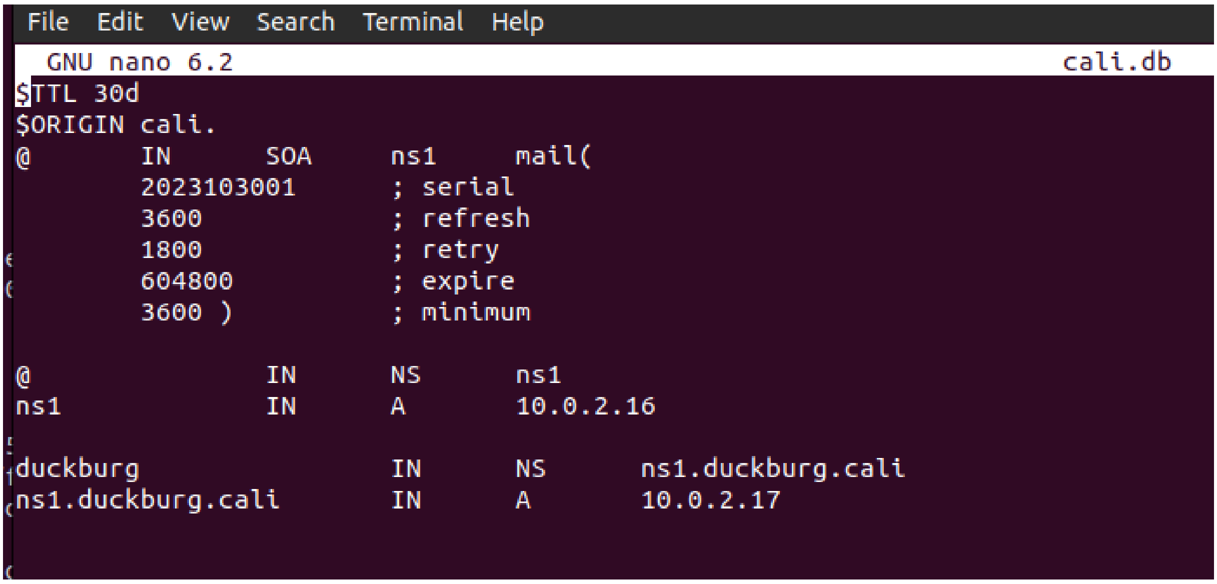


```
fillesten@fillesten-VirtualBox:/var/snap/bind9-jdstrand/current/etc/bind$ dig -x 10.0.2.18

; <<>> DiG 9.18.12-0ubuntu0.22.04.3-Ubuntu <<>> -x 10.0.2.18
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44746
;; flags: qr aa rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;18.2.0.10.in-addr.arpa.                IN      PTR

;; ANSWER SECTION:
18.2.0.10.in-addr.arpa. 0       IN      PTR     fillesten-VirtualBox.
18.2.0.10.in-addr.arpa. 0       IN      PTR     fillesten-VirtualBox.local.

;; Query time: 24 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Oct 30 11:09:10 CET 2023
;; MSG SIZE  rcvd: 125

fillesten@fillesten-VirtualBox:/var/snap/bind9-jdstrand/current/etc/bind$
```

To answer in my report:

- Screenshots of my domains are in the report
- Need for GLUE-record:
  GLUE records are a crucial part of the DNS system, they are used to avoid circular dependencies when resolving domain names. They are included in NS records and provide the IP addresses of authoritative name servers for delegated subdomains. Without GLUE records, DNS resolvers can have trouble finding the necessary name servers, particularly at top-level domains and complex domain hierarchies. GLUE-records stop infinite loops from occurring.
- Discuss the SOA-values that you set. What do we need to consider when deciding these values?

From cali.db:



```
$TTL 30d
$ORIGIN cali.
@       IN      SOA     ns1     mail(
        2023103001      ; serial
        3600            ; refresh
        1800            ; retry
        604800          ; expire
        3600 )          ; minimum

@               IN      NS      ns1
ns1             IN      A       10.0.2.16

duckburg                IN      NS      ns1.duckburg.cali
ns1.duckburg.cali       IN      A       10.0.2.17
```

serial = 2023103001. The serial number can be any arbitrary number however using yyyymmddxx is somewhat standard and often seen/used.

Refresh = 3600 seconds or 1h. how often secondary / slave name servers checks the master name server for updates. Cant be too high to “miss” important updates and cant be too low to avoid creating unnecessary traffic and load to the DNS servers.

Retry = 1800 seconds or 30minutes. This value defines how long secondary DNS servers should wait before retrying a failed zone transfer request. Same here as Refresh with regards to time, to avoid traffic but do not want to wait for too long to retry the request.

Expire = 604800 seconds or 1 week. This determines the maximum time a secondary server will consider its data to be valid of it fails to refresh from the primary server. This value should be significantly greater than the refresh and retry values.

Minimum = 3600 seconds or 1h. determines the default Time to live (TTL) for resource records in the zone. It specifies how long other DNS servers and caches should consider data to be valid. A reasonable time for this is around 1h. where the same principles as refresh apply here too.

- Screenshot of named.conf.local is in report
- DIG can do successful lookups on all domains, pictures are in report
- Explain how reverse zone file works:

A reverse zone file is a component of the Domain Name System (DNS) that maps IP addresses to domain names. It is used for reverse DNS lookups and contains PTR (Pointer) records that associate IP addresses with domain names in a hierarchical, in-addr.arpa domain. When an IP address is queried, the DNS server checks the reverse zone file to provide the corresponding domain name.

- Move the mcduckcorp domain to global dns tree

I would have to change the mcduckcorp domain to be a slave or secondary server instead of a master. Additionally I need to enable allow-transfer. I add a master server to the new slave domain which can be done with the allow-transfer {x.x.x.x;}; with the public ip address of the new master dns server.