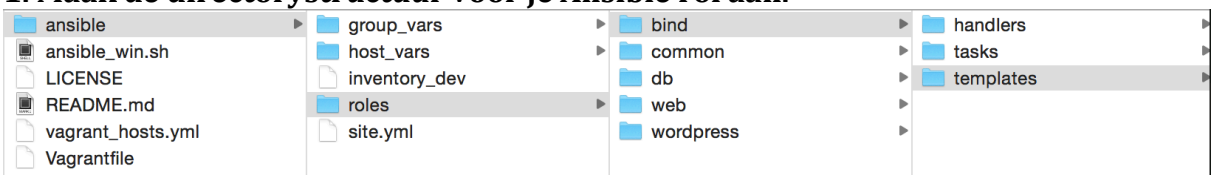
1. Maak de directorystructuur voor je Ansible rol aan.



2. Installeer BIND, zet de service aan, configureer de firewall.

/bind/tasks/main.yml aanmaken;

main.yml

```yaml
# roles/bind/tasks/main.yml
---
- name: install bind packages
  yum: pkg={{ item }} state=installed
  with_items:
    - bind

- name: Start Bind Service
  service: name=named state=running enabled=yes

- name: Add firewall rule for the port 53 (perm)
  firewalld: port=53/udp permanent=true state=enabled

- name: Add firewall rule for the port 53 (non-perm)
  firewalld: port=53/udp permanent=false state=enabled

- name: named.conf zone file
  template:
    src=named.conf.j2
    dest=/etc/named.conf
    owner=root
    group=named
    mode=0640
    setype=named_conf_t
    validate="named-checkconf %s"
  notify: Restart named

- name: linuxlab.net zone file
  template:
    src=linuxlab.net.j2
    dest=/var/named/{{bind_zone_name}}
    owner=root
    group=named
    mode=0640
    setype=named_zone_t
    validate="named-checkzone {{bind_zone_name}} %s"
  notify: Restart named

- name: 2.0.192.in-addr.arpa reverse lookup zone file
  template:
    src=2.0.192.in-addr.arpa.j2
    dest=/var/named/{{reverse_bind_zone_name}}
    owner=root
    group=named
    mode=0640
    setype=named_zone_t
  notify: Restart named
```

3. Maak ansible/host_vars/pu001 aan

pu001

```
# host_vars/pu001
# vi: ft=yaml
---
bind_listen_ipv4:
  - "any"
bind_listen_ipv6:
  - "any"
bind_allow_query:
  - "192.0.2.0/24"
  - "172.16.0.0/16"

bind_recursion: "no"

bind_zone_name: "linuxlab.net"
bind_zone_networks:
  - ip: "192.0.2"
    reverse: "2.0.192"
  - ip: "172.16"
    reverse: "16.172"

bind_zone_name_servers:
  - "pu001"

bind_zone_mail_servers:
  - name: "mail"
    preference: "10"

bind_zone_hosts:
  - name: pu001
    ip: 192.0.2.2
    aliases:
      - ns1
  - name: pu002
    ip: 192.0.2.3
    aliases:
      - ns2
  - name: pu010
    ip: 192.0.2.10
    aliases:
      - www
  - name: pu020
    ip: 192.0.2.20
    aliases:
      - mail
      - smtp
      - imap
  - name: pr001
    ip: 172.16.0.2
    aliases:
      - dhcp
  - name: pr002
    ip: 172.16.0.3
    aliases:
      - moni
      - nagios
  - name: pr010
    ip: 172.16.0.10
    aliases:
      - intra
      - intranet
  - name: pr011
    ip: 172.16.0.11
    aliases:
      - file
```

4. /etc/named.conf van server halen & aanpassen

```
//
// 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 port 53 { any; };
 listen-on-v6 port port 53 { any; };
 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";
 allow-query     { 192.0.2.0/24;172.16.0.0/16;};

 /*
 - 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;

 dnssec-enable yes;
 dnssec-validation yes;
 dnssec-lookaside auto;

 /* Path to ISC DLV key */
 bindkeys-file "/etc/named.iscdlv.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 "{{ lookupzone }}" {
 type master;
 file "{{ 2.0.192.in-addr.arpa }}";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

5. main.yml in /tasks aanpassen

```
- name: named.conf zone file
  template:
    src=named.conf.j2
    dest=/etc/named.conf
    owner=root
    group=named
    mode=0640
    setype=named_conf_t
    validate="named-checkconf %s"
  notify: Restart named
```

6. In /templates linuxlab.net & 2.0.192.in-addr-arpa aanmaken
Linuxlab.net:

```
; Zone file for linuxlab.net

$ORIGIN {{bind_zone_name}}.
$TTL 1W

; primary NS email address admin

@ IN SOA {{bind_zone_name_server}}.{{bind_zone_name}}.
hostmaster.{{bind_zone_name}}. (
14101813 ; serial
1D ; refresh
1H ; retry
1W ; expire
1D ) ; negative caching TTL
        IN NS {{bind_zone_name_servers}}.{{bind_zone_name}}.
;@       IN MX 10 mail.{{bind_zone_name}}.

{% for host in bind_zone_hosts %}
{{host.name}} IN A {{host.ip}}
{% for alias in host.aliases %}
{{alias}} IN CNAME {{host.name}}
{% endfor %}
{% endfor %}
```

2.0.192.in-addr-arpa:

```
; Reverse zone file for linuxlab.net

$TTL 1W
$ORIGIN {{item.reverse}}.in-addr.arpa.

; primary NS  email address admin
@ IN SOA {{bind_zone_name_servers}}.{{bind_zone_name}}.
hostmaster.{{bind_zone_name}}. (
 14101813 ; serial
 1D ; refresh
 1H ; retry
 1W ; expire
 1D ) ; negative caching TTL

      IN  NS   {{bind_zone_name_servers}}.{{bind_zone_name}}.

{% for host in bind_zone_hosts if host.ip.startswith(item.ip) %}
   {{host.ip.replace(item.ip+'.','').ljust(8)}} IN PTR
{{host.name}}.{{bind_zone_name}}.
{% endfor %}
```

7. main.yml terug aanpassen in /tasks

```
- name: linuxlab.net zone file
 template:
   src=linuxlab.net.j2
   dest=/var/named/{{bind_zone_name}}
   owner=root
   group=named
   mode=0640
   setype=named_zone_t
   validate="named-checkzone {{bind_zone_name}} %s"
 notify: Restart named

- name: 2.0.192.in-addr.arpa reverse lookup zone file
 template:
   src=2.0.192.in-addr.arpa.j2
   dest=/var/named/{{reverse_bind_zone_name}}
   owner=root
   group=named
   mode=0640
   setype=named_zone_t
 notify: Restart named
```

8. In vagrantfile lijn toevoegen:
node.vm.synced_folder 'test/', '/tmp/test'
In de map test het script runbats.sh, verkregen door de lector.