Examen Enterprise Linux

Inhoud

1.Algemeen

Hoe best te werk gaan bij troubleshooten?

I. Observatie
II. Hypothese
III. Voorspelling
IV. Test
V. Analyse
VI. Repeat

Checklist gaan maken via bottem up structuur

Applicatie
Transport
Internet
Netwerkinterface
Hardware

Gebruik maken van de logfiles :

- Sudo journalctl -f -u xx.service
- Openen apart terminal venster met journalctl -f
- selinux log: /var/log/audit/audit.log (en in /var/log/messages of journalctl | grep "preventing" om te zien wat selinux blokkeert en hoe het op te lossen)

Oude locaties van logs

- /var/log/messages
- /var/log/(naamrol)

Hardware:

- Check interface aangesloten
- Check correcte interface

Netwerkinterface

- Check ip addressering (/etc/sysconfig/network-scripts/ifcfg-"interface-name")
- check firewall
  - systemctl status firewalld (om te testen als het firewall probleem is: systemctl stop firewalld)
  - firewall-cmd --get-service (--permanent)
  - firewall-cmd --list-ports
  - firewall-cmd --permanent --add-service=http
  - firewall-cmd --add-port=80/tcp
  - firewall-cmd --reload
-

Klaarzetten van Vagrant

Indien er probleem is met box kan je box verwijderen adhv vagrant box -c

Voor een nieuwe box toe te voegen doe het volgende :

vagrant box add /home/karim/Documenten/centos70-nocm.box --name *CentOS*

In de vagrantfile dit veranderen : config.vm.box = *'CentOS'*

Niet opstarten van Server

- Is de servernaam ingevuld in de vagrant_host file?
- Is de server opgenomen in de inventory_dev?
- Krijgt de server rollen in de site.yml bestand?
- Vagrant provision foutmelding lezen!!!!

2.Webserver

Apache

Uitzicht van web/tasks/main.yml

```
---
# file web/tasks/main.yml
- name: Install Apache
  yum: pkg={{item}} state=installed
  with_items:
    - httpd
    - mod_ssl
    - php
    - php-xml
    - php-mysql

- name: Start Apache service
  service: name=httpd state=running enabled=yes

- name: Apply Firewall rules
  firewalld:
    zone=public
    service={{ item[0] }}
    state=enabled
    permanent={{ item[1] }}
  with_nested:
    - [ http, https ]
    - [ true, false ]
  tags: web
```

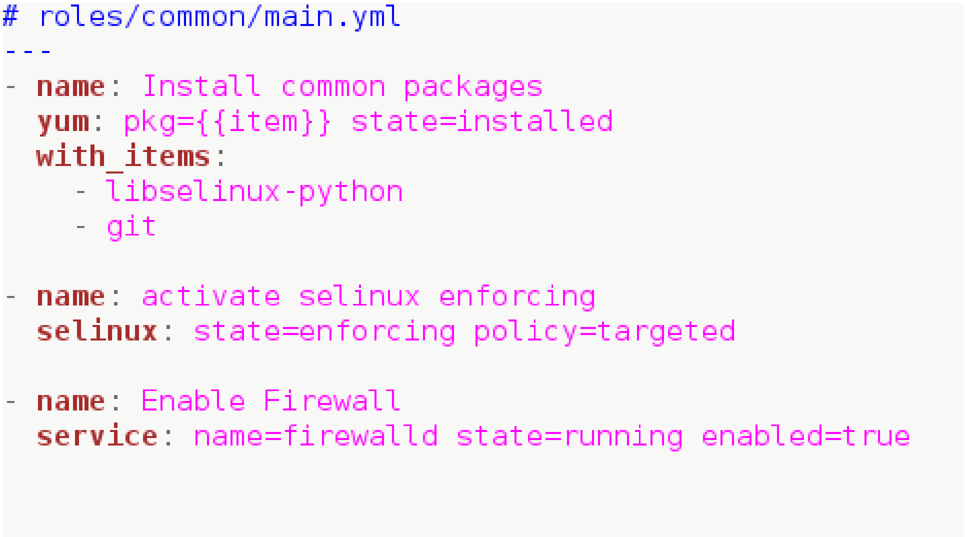
Check : runt de service?

Check : krijg je juiste IP adres?

Check : staat de firewall juist?

Check : kan de website bezocht worden op een andere computer in hetzelfde netwerk?

Zorg ervoor dat de firewall zeker ingeschakeld staat



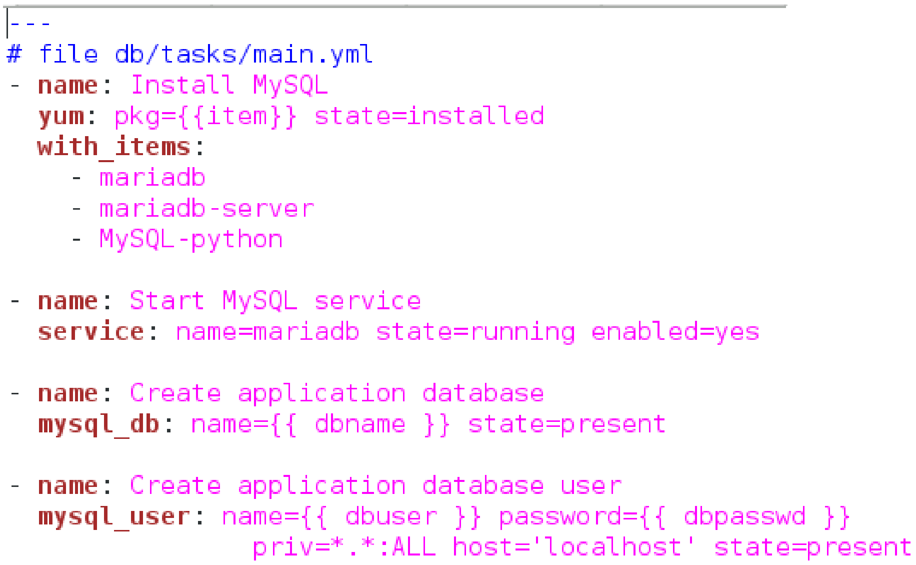
```
# roles/common/main.yml
---
- name: Install common packages
  yum: pkg={{item}} state=installed
  with_items:
    - libselinux-python
    - git

- name: activate selinux enforcing
  selinux: state=enforcing policy=targeted

- name: Enable Firewall
  service: name=firewalld state=running enabled=true
```

Config files van httpd bevinden zich hier : /etc/httpd/conf/httpd.conf

als je httpd processen wil zien doe het volgende :

ps -eZ | grep httpd

Database



```
---
# file db/tasks/main.yml
- name: Install MySQL
  yum: pkg={{item}} state=installed
  with_items:
    - mariadb
    - mariadb-server
    - MySQL-python

- name: Start MySQL service
  service: name=mariadb state=running enabled=yes

- name: Create application database
  mysql_db: name={{ dbname }} state=present

- name: Create application database user
  mysql_user: name={{ dbuser }} password={{ dbpasswd }}
              priv=*.*:ALL host='localhost' state=present
```

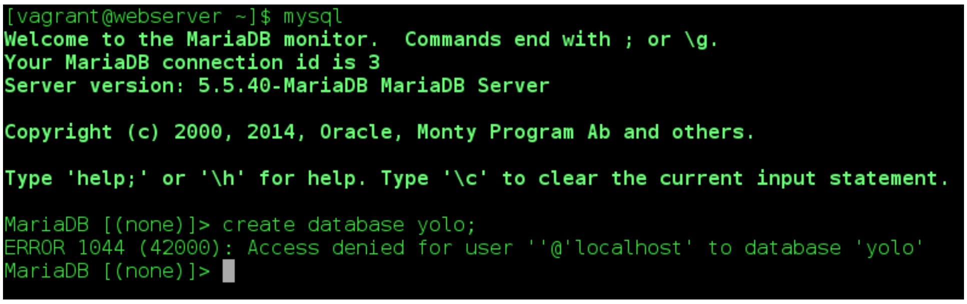
Check: runt de service?

Check : kan je aan de databank?

Check : kan je een tabel aanmaken? --> nog niet, iets mis met gebruiker

Check : moet er rekening gehouden worden met de firewall? (poort 3306)

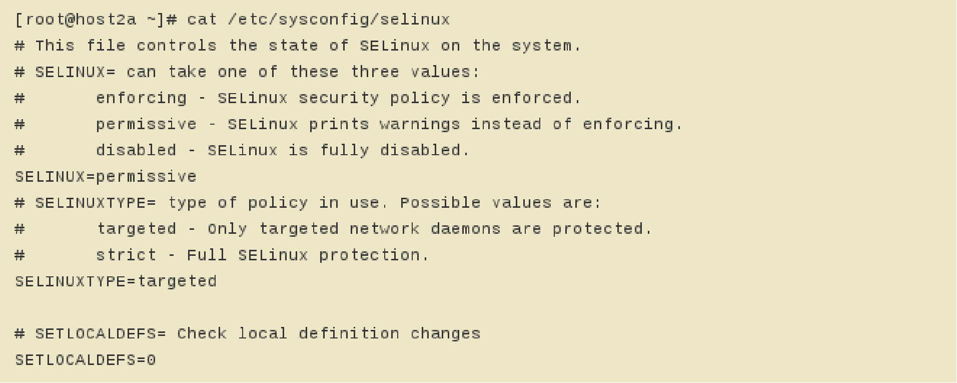
Check : users, moeten die later van tijd de user rechten hebben zoals in de samba en FTP?



```
[vagrant@webserver ~]$ mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 3
Server version: 5.5.40-MariaDB MariaDB Server

Copyright (c) 2000, 2014, Oracle, Monty Program Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database yolo;
ERROR 1044 (42000): Access denied for user ''@'localhost' to database 'yolo'
MariaDB [(none)]>
```

SeLinux

https://www.centos.org/docs/5/html/5.1/Deployment_Guide/sec-sel-enable-disable.html



```
[root@host2a ~]# cat /etc/sysconfig/selinux
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - SELinux is fully disabled.
SELINUX=permissive
# SELINUXTYPE= type of policy in use. Possible values are:
#       targeted - Only targeted network daemons are protected.
#       strict - Full SELinux protection.
SELINUXTYPE=targeted

# SETLOCALDEFS= Check local definition changes
SETLOCALDEFS=0
```

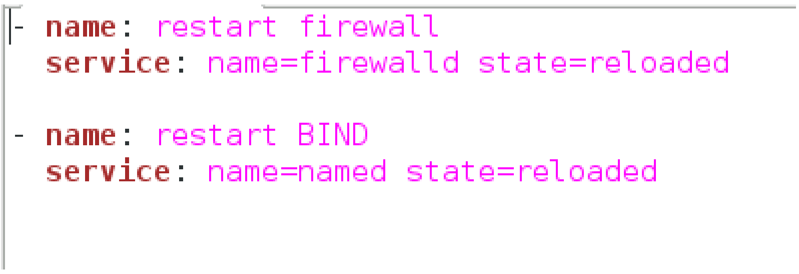
Om te kijken of SeLinux is ingeschakeld : sestatus

3.DNS

main.yml bestand

```
- name: install bind packages
  yum: pkg={{ item }} state=installed
  with_items:
  - bind
  - bind-utils


- name: activate bind service
  service: name=named state=running enabled=true


- name: apply firewall rules
  firewalld:
    port=53/tcp
    state=enabled
    permanent=true
  notify: restart firewall


- name: Copy config file
  template:
    src=named.conf
    dest=/etc/named.conf
    owner=root
    group=named
    mode=640
 #   validate='sudo named-checkconf /etc/named.conf'
#   notify: restart BIND

- name: Copy forward lookup zone
  template:
    src=linuxlab.net
    dest=/var/named/linuxlab.net
    owner=root
    group=named
    mode=640
#   notify: restart BIND
- name: Copy reverse lookup zone
  template:
    src={{item}}
    dest=/var/named/{{item}}
    owner=root
    group=named
    mode=640
  with_items:
    - 2.0.192.in-addr.arpa
    - 16.172.in-addr.arpa
  notify: restart BIND
```

Check : ben je zeker dat de methodes dat je oproept bij notify in de handler staan?



```
- name: restart firewall
  service: name=firewalld state=reloaded

- name: restart BIND
  service: name=named state=reloaded
```

Check : indien je wil troubleshooten, best **bind-utils** mee installeren

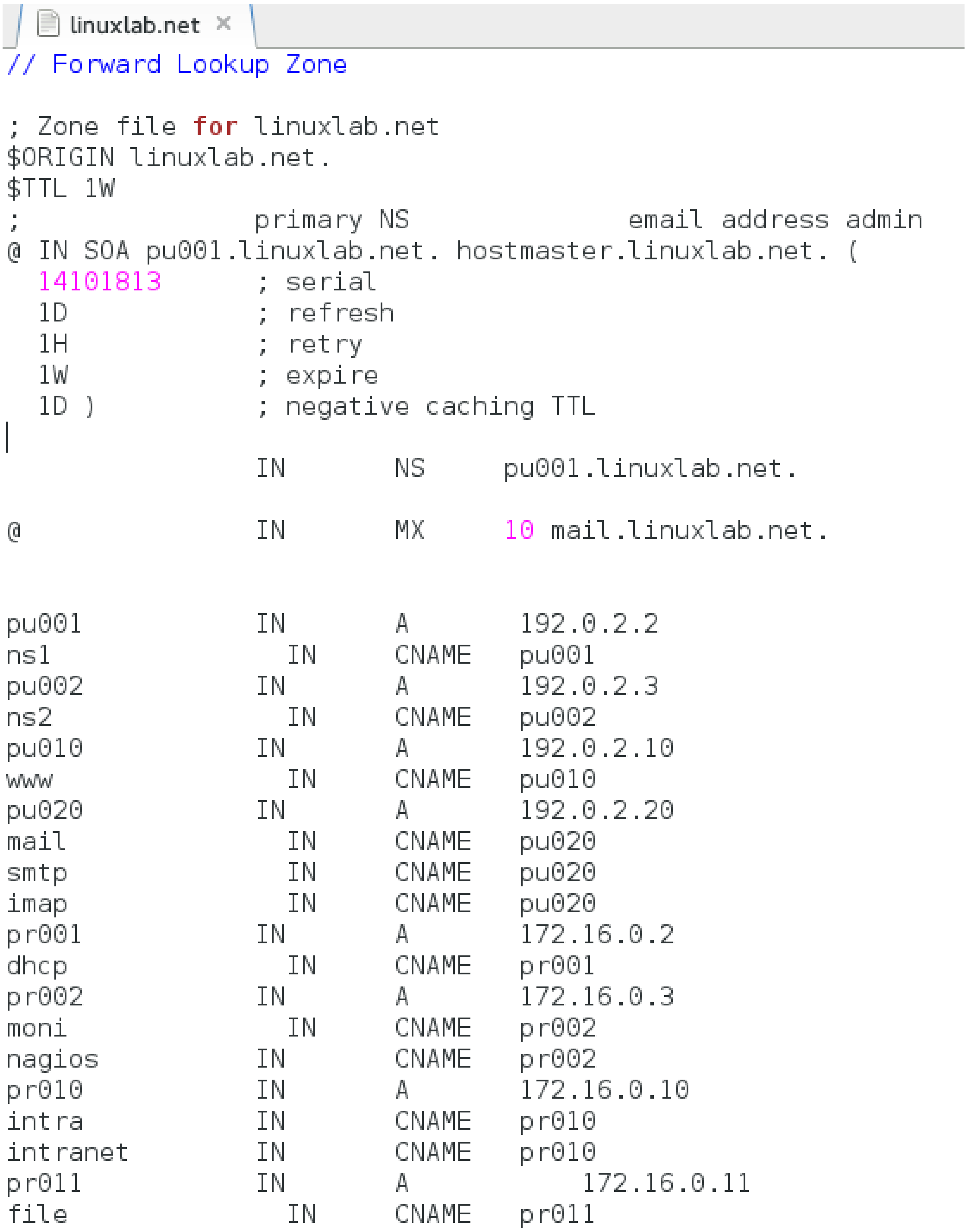
Check : zijn alle template doorgegeven? Dit zijn de volgende

- **Named.conf**
- **Forward Lookup Zone**
- **Reverse Lookup Zone**

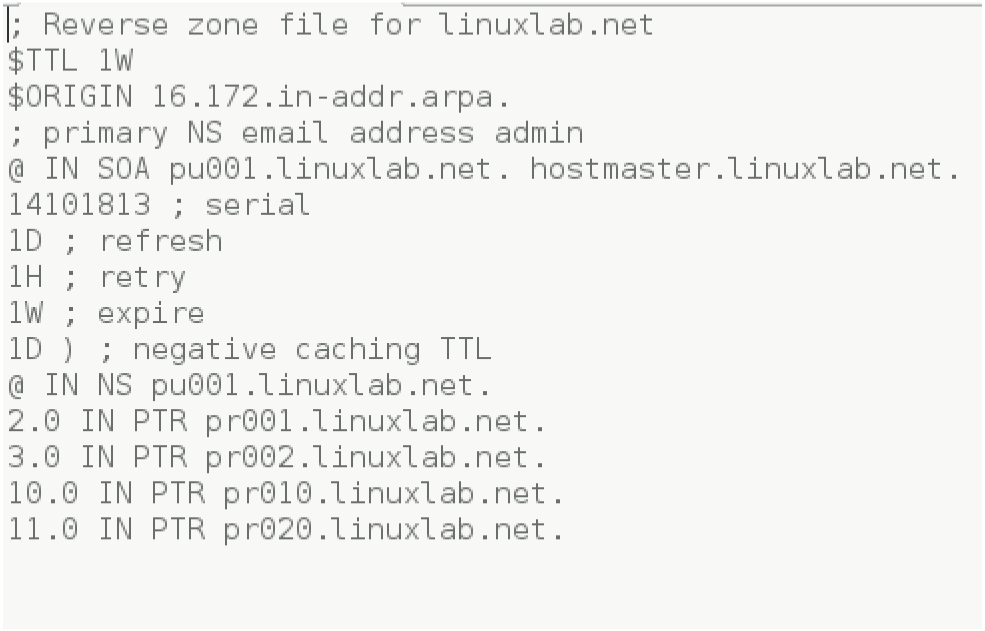
Check : worden deze gekopieerd naar de machine?

Check : zijn de juiste rechten toegekend?

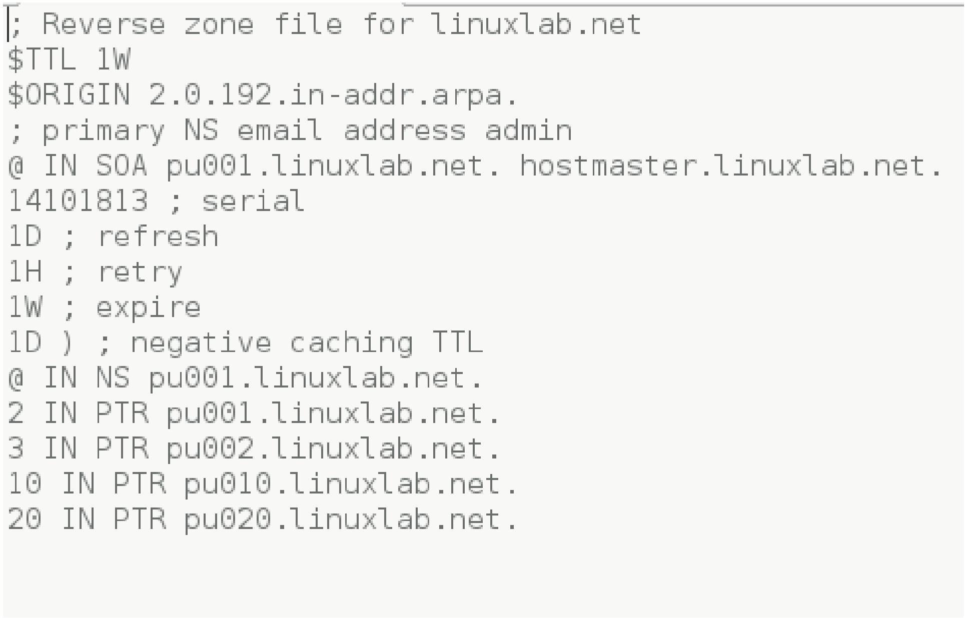
```
 //
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
    listen-on port 53 {any;};
#    listen-on-v6 port 53 { ::1; };
    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     { {{bind_allow_query}} };

    /*
     - 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 {{bind_recursion}};

    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 "." IN {
    type hint;
    file "named.ca";
};
zone "{{bind_zone_name}}" IN {
    type master;
    file "{{bind_zone_file}}";
    allow-update { none;};
};

zone "{{bind_rev_zone1}}" IN {
    type master;
    file "{{bind_rev_zone1_file}}";
    allow-update { none;};
};
zone "{{bind_rev_zone2}}" IN {
    type master;
    file "{{bind_rev_zone2_file}}";
    allow-update { none;};
};


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



```
// Forward Lookup Zone

; Zone file for linuxlab.net
$ORIGIN linuxlab.net.
$TTL 1W
;                primary NS              email address admin
@ IN SOA pu001.linuxlab.net. hostmaster.linuxlab.net. (
  14101813       ; serial
  1D             ; refresh
  1H             ; retry
  1W             ; expire
  1D )           ; negative caching TTL

                IN      NS     pu001.linuxlab.net.

@               IN      MX     10 mail.linuxlab.net.


pu001           IN      A       192.0.2.2
ns1               IN    CNAME   pu001
pu002           IN      A       192.0.2.3
ns2               IN    CNAME   pu002
pu010           IN      A       192.0.2.10
www               IN    CNAME   pu010
pu020           IN      A       192.0.2.20
mail              IN    CNAME   pu020
smtp              IN    CNAME   pu020
imap              IN    CNAME   pu020
pr001           IN      A       172.16.0.2
dhcp              IN    CNAME   pr001
pr002           IN      A       172.16.0.3
moni              IN    CNAME   pr002
nagios          IN      CNAME   pr002
pr010           IN      A       172.16.0.10
intra           IN      CNAME   pr010
intranet        IN      CNAME   pr010
pr011           IN      A           172.16.0.11
file              IN    CNAME   pr011
```



```
; Reverse zone file for linuxlab.net
$TTL 1W
$ORIGIN 16.172.in-addr.arpa.
; primary NS email address admin
@ IN SOA pu001.linuxlab.net. hostmaster.linuxlab.net.
14101813 ; serial
1D ; refresh
1H ; retry
1W ; expire
1D ) ; negative caching TTL
@ IN NS pu001.linuxlab.net.
2.0 IN PTR pr001.linuxlab.net.
3.0 IN PTR pr002.linuxlab.net.
10.0 IN PTR pr010.linuxlab.net.
11.0 IN PTR pr020.linuxlab.net.
```



```
; Reverse zone file for linuxlab.net
$TTL 1W
$ORIGIN 2.0.192.in-addr.arpa.
; primary NS email address admin
@ IN SOA pu001.linuxlab.net. hostmaster.linuxlab.net.
14101813 ; serial
1D ; refresh
1H ; retry
1W ; expire
1D ) ; negative caching TTL
@ IN NS pu001.linuxlab.net.
2 IN PTR pu001.linuxlab.net.
3 IN PTR pu002.linuxlab.net.
10 IN PTR pu010.linuxlab.net.
20 IN PTR pu020.linuxlab.net.
```

4. Samba

Selinux Booleans

- use_samba_home_dirs
- samba_enable_home_dirs

commando: setsebool -P boolean_name=1

Services

- systemctl start nmb
- systemctl start smb

Firewall

- firewall-cmd --add-service=samba (--permanent)

Config

Locatie: /etc/samba/smb.conf

Validatie: testparm -s /etc/samba/smb.conf

Indeling: (voorbeeld)

```
[vagrant@pr011 ~]$ cat /etc/samba/smb.conf
# Samba configuration, managed by Ansible. Please don't edit manually
# Ansible managed: /home/gianni/Documents/Dropbox/3 Tin/Netwerken &
Systeembeheer/Linux/Ansible/AnsibleStoel/ansible/roles/samba/templates/smb.conf.j2 modified
on 2014-12-12 10:15:39 by gianni on localhost.localdomain
#
# vim: ft=samba

[global]
# Server information
netbios name = FILESRV
workgroup = LINUXLAB
server string = Fileserver pr011

# Logging
syslog only = yes
syslog = 1

# Authentication
security = user
passdb backend = tdbsam
map to guest = bad user

# Name resolution: make sure \\NETBIOS NAME\ works
wins support = yes
local master = yes
domain master = yes
preferred master = yes

## Make home directories accessible
[homes]
comment = Home Directories
browseable = no
writable = yes

[public]
comment = public
path = /srv/shares/public
public = no
write list = @public
force group = public
create mode = 775
force create mode = 775
directory mask = 775
force directory mode = 775

[beheer]
comment = beheer
path = /srv/shares/beheer
public = no
valid users = @beheer
write list = @beheer
force group = beheer
create mode = 770
force create mode = 770
```

```
directory mask = 770
force directory mode = 770

[directie]
comment = directie
path = /srv/shares/directie
public = no
valid users = @staf
write list = @directie
force group = directie
create mode = 775
force create mode = 775
directory mask = 775
force directory mode = 775
```

Shares

ls -aZ: setype moet `public_content_rw_t` zijn voor de map om bereikbaar via samba én ftp te zijn.

commando: `sudo chcon -t public_content_rw_t mapnaam`

owner & group: root groupname (die van toepassing is)

Overige

- Maak de juiste groepen aan (groupadd)
- Maak de samba root share directory aan (mkdir)
- Resterende dingen die ik over het hoofd zie => main.yml in Samba role

Checklist (gemaakt fouten door mij)

- Check : Firewalld en SeLinux moeten toegevoegd worden bij common/tasks
- Error : this module requires key=value arguments
  - users werden niet toegevoegd aan de server
  - draaien de rollen?
    - SMB active --> Ja
    - NMB active --> ja
  - gebruikers worden aangemaakt dmv de hostvars, geen typfouten?
  - Worden de shares aangemaakt? --> Ja : ls/srv/shares
    - Zijn de juiste rechten toegekend? --> JA
    - Leest file van Host Vars wel in? --> ja
  - Probleem met encryptie? --> Ja : passwdhash.py
    - Opgelost : filter_plugins moesten meegenomen worden
- Check : hoe laadt hij de filter plugins in?

5. FTP

Installatie

sudo yum install vsftpd

Firewall

add-service=ftp

Selinux Booleans

- ftp_home_dir
- ftpd_full_access

Configuration

Locatie: /etc/vsftpd/vsftpd.conf

owner & group: root & root

Voorbeeld inhoud:

```
# Vsftpd configuration

# Vsftpd configuration/managament

# Anonymous login
anonymous_enable=NO
anon_root=/srv/shares

# Registered user access
local_enable=YES
local_root=/srv/shares
local_umask=022
userlist_deny=YES

write_enable=YES

# Server port settings
connect_from_port_20=YES
listen=YES
listen_ipv6=NO

pam_service_name=vsftpd
```

pam_service_name=vsftpd

Checklist

- Check : is de rol geinstalleerd?
- Check : wordt de poort opengezet in de firewall?
- Check : wordt het configuratiebestand gekopieerd naar de machine?
- Check : Zijn alle variabelen aangevuld in de host_vars
- Check : Zijn de SELinux attributen aangevuld?
- Check : zijn er geen typfouten?./

6. DHCP

Package

Installeer "dhcp"

Config Voorbeeld

```
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.example
#   see dhcpd.conf(5) man page
#

subnet 172.16.0.0 netmask 255.255.0.0 {
        option routers                  172.16.255.254;
        option subnet-mask              255.255.0.0;
        option domain-search            "linuxlab.net";
        option domain-name-servers      192.0.2.2;
range 172.16.100.1 172.16.255.253;
}

host pr001 {
option host-name "pr001.linuxlab.net";
hardware ethernet 08:00:27:E7:3C:0E;
fixed-address 172.16.0.2;
}

host pr010 {
option host-name "pr010.linuxlab.net";
hardware ethernet 07:05:06:04:09:00;
fixed-address 172.16.0.10;
}

host pr011 {
option host-name "pr011.linuxlab.net";
hardware ethernet 08:00:27:65:4E:E0;
fixed-address 172.16.0.11;
}
```

7.Routering

VyOS box toevoegen via vagrant add box … --name name

Commandos in bert’s cheatsheet

Config file op root zetten van ansible folder

```
#!/bin/vbash

source /opt/vyatta/etc/functions/script-template

configure

# Fix for error "INIT: Id "TO" respawning too fast: disabled for 5 minutes"

delete system console device ttyS0

# Commands here

set system host-name router

set system gateway-address 10.0.2.2

set system name-server 192.0.2.2

set service dns forwarding listen-on eth2

set service dns forwarding name-server 192.0.2.2
set service ssh listen-address 0.0.0.0

set interfaces ethernet eth0 address dhcp

set interfaces ethernet eth1 address 192.0.2.254/24

set interfaces ethernet eth2 address 172.16.255.254/16

commit

save
```