Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Ministerie van BZK
Operatie BRP

Turfmarkt 147
2511 HC Den Haag

www.operatiebrp.nl
contact@operatiebrp.nl

Configuratie proeftuinen

Versie 1.0
Aan Tbv intern gebruik Operatie BRP
Van Operatie BRP

Datum
26 juli 2017

Inhoudsopgave

1 Inleiding

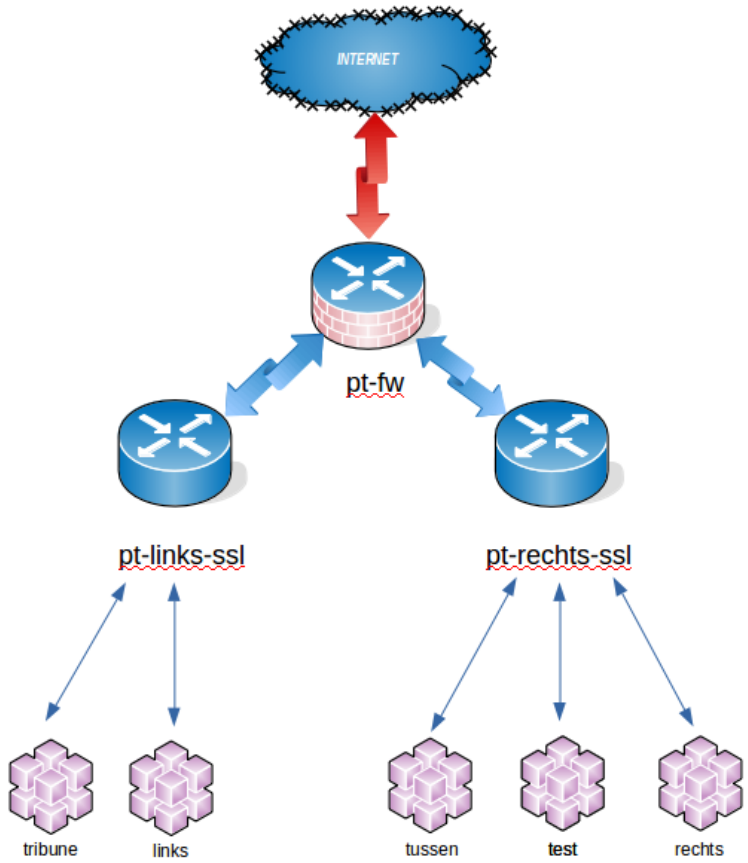
In dit document wordt beschreven hoe de proeftuinen op de modernodam omgeving worden opgezet en ingericht.

2 Proeftuin netwerk

Modernodam Proeftuin bestaat uit een aantal servers die zorgen voor de infra, zoals: firewall, reverse proxy e.d., en de servers waar de BRP applicatie op draait. De servers waar de applicatie op draait zijn standaard docker servers die middels de Docker puppet module (zie bijlage A) worden ingericht.

Aan de buitenkant luistert de server genaamd **pt-fw** met de interfaces die beschreven staan in /etc/network/interfaces (zie Bijlage B). De firewall regels zijn te vinden op /etc/network/iptables (zie Bijlage C).

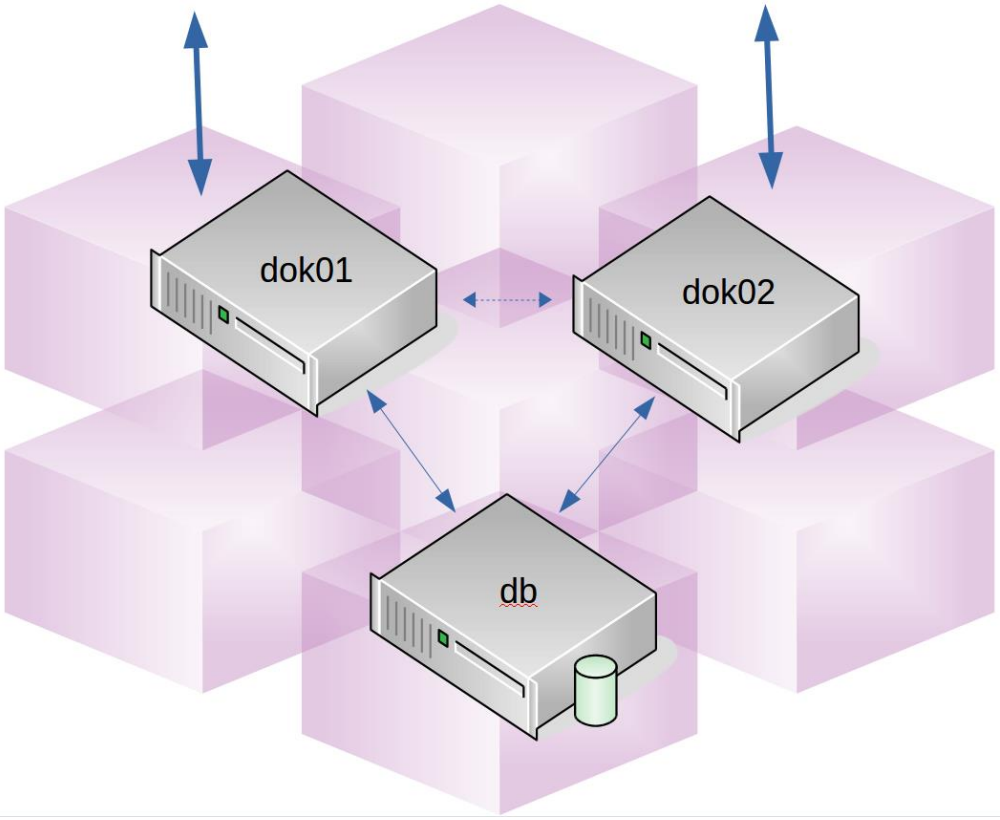
Hieronder vind je het schema van de proeftuinen.



pt-links-ssl en **pt-rechts-ssl** hebben allebei gelijke iptables die zich op /etc/network/iptables (zie Bijlage D) bevinden. Hier wordt ook de toegang geregeld voor specifieke partijen. Op beide servers bevinden zich de apache configuraties. Gezien het feit dat op deze servers Ubuntu 16.04 draait staat deze zowel voor pt-links-ssl (zie Bijlage E) en pt-rechts-ssl (zie Bijlage F) op /etc/apache2/sites-enabled/default-ssl.conf. Zoals te zien is in het bovenstaande

schema routeren de pt-rechts-ssl en pt-links-ssl naar verschillende omgevingen. pt-rechts-ssl heeft ook 1 omgeving meer dan dat pt-links-ssl heeft. Om de reverse proxy op beide servers goed te laten werken moet op pt-links-ssl en pt-rechts-ssl de /etc/network/interfaces zoals in bijlages G en H ingericht worden.

De proeftuinen zelf bestaan uit 2 docker servers en en database server. De database servers worden net als de docker servers ingericht met een aantal puppet modules waarvan de postgres (zie Bijlage I) het belangrijkst is.



1.1 Testen

Testen gebeurt aan de functionele kant door een test team en de externen: leveranciers en afnemers. Op het technische vlak kunnen bijvoorbeeld de apache access logs bekeken worden of de netwerkstroom kan getest worden bijvoorbeeld met tcpdump of netcat.

1.2 Certificaten

Voor de certificaten is er een PKI ingericht die nu in een .tgz bestand te vinden is op https://www.modernodam.nl/svn/brp-release/trunk/OA release/03 Testrapport/02 OA release/02 Proeftuin/02 Technisch beheer/CA/ca.tgz.

Hieronder vind je het LEESMIJ en de 2 handleidingen die het gebruik hiervan beschrijven:

LEESMIJ:

Dit is de ca / PKI infra voor de BRP omgeving.
Deze folder bevat de scripts, directory structuur en configuratie bestanden t.b.v. het aanmaken van certificaten. De scripts gaan er van uit dat deze folder wordt gekopieerd naar /opt/ca. Indien deze folder en onderliggende folders ergens anders dan in /opt/ca staan, dan dienen de scripts aangepast te worden en dient de $BASEDIR in alle scripts naar het juiste pad gezet te worden.

Voor meer info, lees de installatie handleidingen van de BRP Service en de instructie bestanden in deze folder.

INSTRUCTIES_NIEUWE_CLIENT:

INSTALLATIE KLANT CERTIFICAAT

Aanmaken certificaat

- Login op de server waar de certificaten worden beheerd.
- cd naar '/opt/ca/bin' (of waar het certificaten materiaal is geinstalleerd)
- Executeer het 'new_client.sh' script met als argument de naam can de klant (zonder spaties)
- In '/opt/ca/distrib' staat nu het nieuwe certificaat materiaal voor de klant. Dit kan naar de klant toegestuurd worden.
- Zorg er voor dat de data zoals gemeld in het script onder 'The following data is required...' bij de hand blijft, want deze data is nodig voor het toevoegen van het certificaat aan de database.

Toevoegen certificaat aan de BRP

- cd naar '/opt/ca/var'
- scp het '<klant>_client.crt' bestand naar de applicatie server
- Ga naar de server waar de applicatie server op draait.
- Ga naar de folder waar het '<klant>_client.crt' naar toe is gekopieerd.
- Executeer het volgende command:

```
keytool -import -alias <klant> -file ./<klant>_client.crt -keystore /opt/tomcat/lib/brpserver_publicstore.jks
```

- Ga naar de server waar de database op draait.
- Open een connectie naar de BRP database.
- Executeer het volgende SQL commando voor het toevoegen van het certificaat aan de BRP database, hierbij uiteraard gebruik makend van de eerder gemelde waardes:

INSERT INTO autaut.certificaat (id, subject, serial, signature) VALUES ((select coalesce(max(id), 0) + 1 from autaut.certificaat), '<DB SUBJECT>', <DB SERIAL>, '<DB SIGNATURE>');

- Executeer het volgende SQL commando voor het toevoegen van de nieuwe klant met zijn certificaat, hierbij dient voor de partij een specifiek id te worden gebruikt welke overeen dient te komen met de id van de partij/gemeente waaraan de klant gekoppeld dient te worden:

INSERT INTO autaut.authenticatiemiddel (id, partij, rol, functie, certificaattbvondertekening, authenticatiemiddelstatushis) VALUES ((select coalesce(max(id), 0) + 1 from autaut.authenticatiemiddel), <PARTIJ ID>, 1, 1, (select max(id) from autaut.certificaat), 'A');

INSTRUCTIES_NIEUWE_CA_OF_SERVER:

INSTALLATIE CA EN/OF SERVER CERTIFICAAT

Aanmaken CA

- Wijzig 'req_distinguished_name' in CA certificaat configuratie in /opt/ca/etc/ca-ssl.conf
- Wijzig eventueel de alias van het CA certificaat in het script /opt/ca/bin/ca-setup.sh, wijzig hierin 'staat_der_mgba_root_ca' in het gewenste alias.
- Maak CA certificaat aan door nu het 'ca-setup' script uit te voeren met 'ca' als argument /opt/ca/bin/ca-setup.sh ca
- In /opt/ca/var vind je nu het CA key materiaal.

Aanmaken Server

- Wijzig 'req_distinguished_name' in server SSL certificaat configuratie in /opt/ca/etc/server-ssl.conf
- Maak Server certificaat aan door nu het 'ca-setup' script uit te voeren met 'server' als argument /opt/ca/bin/ca-setup.sh server
- Run het 'privatestore' script om aan de hand van het server certificaat een private keystore te maken: /opt/va/bin/privatestore.sh
- In /opt/ca/var vind je nu het server key materiaal.

Bijlage A Docker puppet module

```
class docker::1_12 {

  file { "docker-sysctl":
    path   => "/etc/sysctl.d/10-sysctl.conf",
    ensure => "file",
    owner  => "root",
    group  => "root",
    mode   => "0644",
    source => "puppet:///modules/docker/10-sysctl.conf",
    notify => Exec["sysctl"],
  }

  exec { "sysctl":
    command     => "/sbin/sysctl --system",
    subscribe   => File["docker-sysctl"],
    refreshonly => true
  }

  package { "policycoreutils-python":
    ensure => "installed",
  }

  package { "libseccomp.x86_64":
    ensure => "installed",
  }

  package { "libtool-ltdl":
    ensure => "installed",
    before => Package["docker-engine-selinux-1.12.1-
1.el7.centos.noarch"],
  }

  file { "docker-compose":
    path   => "/bin/docker-compose",
    ensure => "file",
    owner  => "root",
    group  => "root",
    mode   => "0755",
    source => "puppet:///modules/docker/docker-compose-1.8.0-
Linux-x86_64",
    before => Package["libtool-ltdl"],
  }

  file { "docker-profile":
    path   => "/etc/profile.d/docker.sh",
    ensure => "file",
    owner  => "root",
    group  => "root",
    mode   => "0755",
    source => "puppet:///modules/docker/docker_profile",
  }
```

```
  package { "docker-engine-selinux-1.11.1-1.el7.centos.noarch":
    ensure => "absent",
  }

  package { "docker-engine-1.11.1-1.el7.centos.x86_64":
    ensure => "absent",
  }

  package { "docker-engine-selinux-1.12.1-1.el7.centos.noarch":
    provider => "rpm",
    ensure   => "installed",
    source   =>
"http://192.168.202.13/software/centos7/docker-engine-selinux-
1.12.1-1.el7.centos.noarch.rpm",
    require  => Package["policycoreutils-python"],
  }

  package { "docker-engine-1.12.1-1.el7.centos.x86_64":
    provider => "rpm",
    ensure   => "installed",
    source   =>
"http://192.168.202.13/software/centos7/docker-engine-1.12.1-
1.el7.centos.x86_64.rpm",
    require  => Package["docker-engine-selinux-1.12.1-
1.el7.centos.noarch"],
  }

  file { "docker.service.d":
    path   => "/etc/systemd/system/docker.service.d",
    ensure => "directory",
    owner  => "root",
    group  => "root",
    mode   => "0755",
  }

  exec { "reload_docker":
    command     => "/bin/systemctl daemon-reload",
    refreshonly => "true",
    notify      => Service["docker.service"],
  }

  file { "docker_service":
    path    => "/etc/systemd/system/docker.service.d/docker-
service.conf",
    ensure  => "file",
    owner   => "root",
    group   => "root",
    mode    => "0644",
    source  => "puppet:///modules/docker/docker-service-
1.12.conf",
    require => File["docker.service.d"],
    notify  => Exec["reload_docker"],
  }
```

```
  file { "http_proxy":
    path    => "/etc/systemd/system/docker.service.d/http-
proxy.conf",
    ensure  => "file",
    owner   => "root",
    group   => "root",
    mode    => "0644",
    source  => "puppet:///modules/docker/http-
proxy_1.12.conf",
    require => File["docker.service.d"],
    notify  => Exec["reload_docker"],
  }

  service { "docker.service":
    ensure  => "running",
    enable  => "true",
    require => Package["docker-engine-1.12.1-
1.el7.centos.x86_64"],
  }

}
```

Bijlage B Interfaces pt-fw

```
# This file describes the network interfaces available on your
system
# and how to activate them. For more information, see
interfaces(5).
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 172.19.2.72
    netmask 255.255.255.224
    gateway 172.19.2.65
    up route add -net 192.168.212.0/24 gw 172.19.2.69 dev eth0
        up route add -net 192.168.202.0/24 gw 172.19.2.69 dev
eth0
        up route add -net 192.168.206.0/24 gw 172.19.2.69 dev
eth0
    down route del -net 192.168.212.0/24 gw 172.19.2.69 dev
eth0
    down route del -net 192.168.202.0/24 gw 172.19.2.69 dev
eth0

## v interface voor BRP proeftuin links
auto eth0:1
iface eth0:1 inet static
    address 172.19.2.74
    netmask 255.255.255.224

auto eth3
iface eth3 inet static
    address 192.168.208.1
    netmask 255.255.255.0

auto eth2
iface eth2 inet static
    address 192.168.209.1
    netmask 255.255.255.0

auto eth1
iface eth1 inet static
    address 192.168.210.1
    netmask 255.255.255.0

auto eth4
iface eth4 inet static
    address 192.168.217.1
    netmask 255.255.255.0

auto eth5
iface eth5 inet static
    address 192.168.216.1
    netmask 255.255.255.0
```

Bijlage C Iptables pt-fw

```
# Generated by iptables-save v1.4.21 on Mon Aug  7 12:09:21 2017
*nat
:PREROUTING ACCEPT [2582480:189869069]
:INPUT ACCEPT [95176:6037914]
:OUTPUT ACCEPT [194147:14045442]
:POSTROUTING ACCEPT [1921256:124478194]
-A PREROUTING -d 172.19.2.72/32 -p tcp -m tcp --dport 443 -j
DNAT --to-destination 192.168.208.100:443
-A PREROUTING -d 172.19.2.74/32 -p tcp -m tcp --dport 443 -j
DNAT --to-destination 192.168.216.10:443
-A POSTROUTING -s 192.168.216.10/32 ! -d 192.168.0.0/16 -o eth0
-j SNAT --to-source 172.19.2.74
-A POSTROUTING -s 192.168.216.30/32 -o eth0 -j SNAT --to-source
172.19.2.74
-A POSTROUTING ! -d 192.168.0.0/16 -o eth0 -j SNAT --to-source
172.19.2.72
COMMIT
# Completed on Mon Aug  7 12:09:21 2017
# Generated by iptables-save v1.4.21 on Mon Aug  7 12:09:21 2017
*filter
:INPUT DROP [1611:58032]
:FORWARD DROP [423053:44919018]
:OUTPUT DROP [0:0]
:BRP-DEMO - [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -s 192.168.202.50/32 -p tcp -m tcp --dport 8086 -j
ACCEPT
-A INPUT -s 192.168.202.100/32 -p tcp -m tcp --dport 22 -j
ACCEPT
-A INPUT -s 192.168.202.200/32 -p tcp -m tcp --dport 8086 -j
ACCEPT
-A FORWARD -d 192.168.202.140/32 -p udp -m udp --dport 12201 -m
comment --comment "Graylog2 logging host" -j ACCEPT
-A FORWARD -s 192.168.0.0/16 -d 192.168.202.206/32 -p tcp -m
multiport --dports 9200,9300,9301,9302,9303,9304,9305 -m
comment --comment "Doorvoer naar fac-proeftuinlog" -j ACCEPT
-A FORWARD -d 192.168.202.200/32 -p tcp -m tcp --dport 8140 -j
ACCEPT
-A FORWARD -d 192.168.202.50/32 -p tcp -m tcp --dport 8140 -j
ACCEPT
-A FORWARD -s 192.168.206.68/32 -p tcp -m tcp --dport 22 -m
comment --comment "Toegang pat-db01 naar de proeftuin" -j
ACCEPT
-A FORWARD -s 192.168.212.0/24 -m comment --comment "Sta alle
VPN toe, zirkoon regelt individueel toegang" -j ACCEPT
-A FORWARD -p icmp -j ACCEPT
-A FORWARD -s 192.168.202.200/32 -p tcp -m tcp --dport 8086 -m
comment --comment "Nagios monitoring van FAC-CON01" -j ACCEPT
-A FORWARD -s 192.168.202.200/32 -p icmp -m comment --comment
"ping van FAC-CON01 voor nagios" -j ACCEPT
-A FORWARD -s 192.168.202.50/32 -p icmp -j ACCEPT
-A FORWARD -s 192.168.202.100/32 -p icmp -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
-A FORWARD -s 192.168.202.50/32 -p tcp -m tcp --dport 8086 -m
comment --comment "Nagios monitoring" -j ACCEPT
-A FORWARD -s 192.168.202.50/32 -p tcp -m tcp --dport 4949 -m
comment --comment "Munin monitoring" -j ACCEPT
-A FORWARD -s 192.168.0.0/16 -p tcp -m tcp --dport 22 -j ACCEPT
-A FORWARD -s 192.168.202.100/32 ! -o eth0 -p tcp -m tcp --
dport 22 -j ACCEPT
-A FORWARD ! -i eth0 -p tcp -m multiport --dports 53,80,443 -j
ACCEPT
-A FORWARD ! -i eth0 -p udp -m multiport --dports 53,123 -j
ACCEPT
-A FORWARD -d 192.168.208.100/32 -p tcp -m tcp --dport 443 -j
ACCEPT
-A FORWARD -d 192.168.216.10/32 -p tcp -m tcp --dport 443 -j
ACCEPT
-A FORWARD -d 192.168.216.60/32 -p tcp -m tcp --dport 443 -m
comment --comment "RHEL based reverse proxy PT links" -j ACCEPT
-A FORWARD -d 192.168.208.60/32 -p tcp -m tcp --dport 443 -m
comment --comment "RHEL based reverse proxy PT rechts" -j
ACCEPT
-A FORWARD -s 192.168.208.0/24 -d 192.168.209.0/24 -p tcp -m
tcp --dport 5432 -m comment --comment "postgres access for PT
rechts AP servers" -j ACCEPT
-A FORWARD -s 192.168.216.0/24 -d 192.168.217.0/24 -p tcp -m
tcp --dport 5432 -m comment --comment "postgres access for ap
servers" -j ACCEPT
-A FORWARD -d 192.168.202.13/32 ! -i eth0 -p tcp -m tcp --dport
3128 -m comment --comment "http proxy access" -j ACCEPT
-A FORWARD -d 192.168.202.33/32 -p tcp -m tcp --dport 25 -m
comment --comment "mail relay" -j ACCEPT
-A FORWARD -s 192.168.208.80/32 -p tcp -m multiport --dports
80,443 -m comment --comment "afnemersverkeers prap02" -j ACCEPT
-A FORWARD -s 192.168.216.30/32 -p tcp -m multiport --dports
80,443 -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -p icmp -j ACCEPT
-A OUTPUT -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT
COMMIT
# Completed on Mon Aug  7 12:09:21 2017
```

Bijlage D Iptables pt-links-ssl en pt-rechts-ssl

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
:BRP_SVC_ACCESS - [0:0]
-A INPUT -m comment --comment "000 INPUT allow related and
established" -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m comment --comment "001 accept all icmp
requests" -j ACCEPT
-A INPUT -i lo -p tcp -m comment --comment "002 INPUT allow
TCP loopback" -j ACCEPT
-A INPUT -i lo -p udp -m comment --comment "0021 INPUT allow
UDP loopback" -j ACCEPT
-A INPUT -s 192.168.202.100/32 -p tcp -m multiport --dports 22
-m comment --comment "100 allow ssh" -m state --state NEW -j
ACCEPT
-A INPUT -s 192.168.202.50/32 -p udp -m multiport --dports 123
-m comment --comment "101 allow NAGIOS ntp-check" -m state --
state NEW -j ACCEPT
-A INPUT -s 192.168.202.50/32 -p tcp -m multiport --dports 8086
-m comment --comment "101 allow nagios mon / nrpe" -m state --
state NEW -j ACCEPT
-A INPUT -s 192.168.202.200/32 -p tcp -m multiport --dports
8086 -m comment --comment "101a allow NAGIOS ntp-check" -m
state --state NEW -j ACCEPT
-A INPUT -s 192.168.202.50/32 -p tcp -m multiport --dports 4949
-m comment --comment "109 allow munin polling" -m state --state
NEW -j ACCEPT
-A INPUT -s 192.168.202.0/24 -p tcp -m multiport --dports 22 -m
comment --comment "210 allow ssh from facilitybox" -m state --
state NEW -j ACCEPT
-A INPUT -s 188.200.160.225/32 -p tcp -m multiport --dports 443
-m comment --comment "440 allow vicrea" -m state --state NEW -j
ACCEPT
-A INPUT -s 95.96.7.128/32 -p tcp -m multiport --dports 443 -m
comment --comment "441 allow Maljaars IT" -m state --state NEW
-j ACCEPT
-A INPUT -s 94.242.198.151/32 -p tcp -m multiport --dports 443
-m comment --comment "441a allow Maljaars IT monitoring LU" -m
state --state NEW -j ACCEPT
-A INPUT -s 144.43.249.0/24 -p tcp -m multiport --dports 443 -m
comment --comment "442 allow WIFI netwerk JUBI toren" -m state
--state NEW -j ACCEPT
-A INPUT -s 192.168.212.0/24 -p tcp -m multiport --dports 443 -
m comment --comment "443 allow OpenVPN clients" -m state --
state NEW -j ACCEPT
-A INPUT -s 37.153.235.7/32 -p tcp -m multiport --dports 443 -m
comment --comment "444 allow Gemmboxx" -m state --state NEW -j
ACCEPT
-A INPUT -s 80.89.238.224/27 -p tcp -m multiport --dports 443 -
m comment --comment "445 allow SNG testomgeving" -m state --
state NEW -j ACCEPT
-A INPUT -s 31.223.163.78/32 -p tcp -m multiport --dports 443 -
m comment --comment "446 allow T&T kantoor" -m state --state
NEW -j ACCEPT
```

```
-A INPUT -s 188.202.26.81/32 -p tcp -m multiport --dports 443 -
m comment --comment "447 allow Procura" -m state --state NEW -j
ACCEPT
-A INPUT -s 171.33.133.144/29 -p tcp -m multiport --dports 443
-m comment --comment "448 allow Centric" -m state --state NEW -
j ACCEPT
-A INPUT -s 212.61.158.8/29 -p tcp -m multiport --dports 443 -m
comment --comment "449 allow PinkRoccade #1" -m state --state
NEW -j ACCEPT
-A INPUT -s 92.70.53.0/27 -p tcp -m multiport --dports 443 -m
comment --comment "450 allow PinkRoccade #2" -m state --state
NEW -j ACCEPT
-A INPUT -s 87.250.154.0/24 -p tcp -m multiport --dports 443 -m
comment --comment "455 allow eLABBS" -m state --state NEW -j
ACCEPT
-A INPUT -s 159.46.196.105/32 -p tcp -m multiport --dports 443
-m comment --comment "457 allow JustID/IND" -m state --state
NEW -j ACCEPT
-A INPUT -s 193.177.160.99/32 -p tcp -m multiport --dports 443
-m comment --comment "456 allow Centrc 2" -m state --state NEW
-j ACCEPT
-A INPUT -s 159.46.196.106/32 -p tcp -m multiport --dports 443
-m comment --comment "458 allow JustID/IND" -m state --state
NEW -j ACCEPT
-A INPUT -s 198.211.119.11/32 -p tcp -m multiport --dports 443
-m comment --comment "459 allow JustID/IND" -m state --state
NEW -j ACCEPT
-A INPUT -s 192.168.212.107/32 -p tcp -m multiport --dports 22
-m comment --comment "667 allow arkra-vpn ssh" -m state --state
NEW -j ACCEPT
-A INPUT -s 192.168.212.6/32 -p tcp -m multiport --dports 22 -m
comment --comment "678 allow jawin2-vpn ssh" -m state --state
NEW -j ACCEPT
-A INPUT -s 192.168.212.116/32 -p tcp -m multiport --dports 22
-m comment --comment "777 allow saeer-vpn ssh" -m state --state
NEW -j ACCEPT
-A INPUT -m comment --comment "998 deny all other requests" -j
DROP
-A FORWARD -m comment --comment "999 deny all other requests" -
j DROP
-A OUTPUT -m comment --comment "000 OUTPUT allow related and
established" -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT
COMMIT
# Completed on Tue Aug  8 07:54:03 2017
```

Bijlage E Apache configuratie pt-links-ssl

```
<IfModule mod_ssl.c>
<VirtualHost *:443>

DocumentRoot /var/www

<Directory />
  Require all denied
</Directory>

<Directory /var/www>
  Require all granted
  Options None
</Directory>


        ProxyRequests Off
        ProxyPreserveHost On

        ProxyPass /bijhouding http://pl-
dok02.modernodam.nl:8780/bijhouding
        ProxyPass /bevraging http://pl-
dok01.modernodam.nl:8080/bevraging
        ProxyPass /afnemerindicaties http://pl-
dok02.modernodam.nl:8480/afnemerindicaties
        ProxyPass /synchronisatie http://pl-
dok02.modernodam.nl:8380/synchronisatie

        RequestHeader set X-SSL-SSL_CLIENT_S_DN
"%{SSL_CLIENT_S_DN}s"
        SSLOptions +StdEnvVars +ExportCertData

        <Proxy http://pl-dok02.modernodam.nl:8780>
              Require all granted
        </Proxy>

        <Proxy http://pl-dok02.modernodam.nl:8480>
              Require all granted
        </Proxy>

        <Proxy http://pl-dok02.modernodam.nl:8380>
              Require all granted
        </Proxy>

        <Proxy http://pl-dok01.modernodam.nl:8080>
            Require all granted
        </Proxy>

RewriteEngine on
RewriteRule
^/brp/bijhouding/BijhoudingService(.+)              /bijhoudin
g/BijhoudingService$1 [PT]
```

```
RewriteRule
^/brp/bijhouding/DocumentarchiefService(.+)         /documenta
rchief/DocumentarchiefService$1 [PT]
RewriteRule
^/brp/bijhouding/BevragingService(.+)               /bevraging
/BijhoudingBevragingService$1 [PT]
RewriteRule
^/brp/levering/BevragingService(.+)                 /bevraging
/LeveringBevragingService$1 [PT]
RewriteRule
^/brp/levering/BevragingBulkService(.+)             /bevraging
/LeveringBevragingBulkService$1 [PT]
RewriteRule
^/brp/levering/SynchronisatieService(.+)            /synchroni
satie/SynchronisatieService$1 [PT]
RewriteRule
^/brp/levering/AfnemerindicatiesService(.+)         /afnemerin
dicaties/AfnemerindicatiesService$1 [PT]
RewriteRule
^/brp/terugmelding/TerugmeldingService(.+)          /terugmeld
ing/TerugmeldingService$1 [PT]
RewriteRule
^/brp/vrijeberichten/VrijeBerichtenService(.+)      /vrijeberi
chten/VrijeBerichtenService$1 [PT]
RewriteRule
^/brp/levering/BevragingService(.+)                 /bevraging
/LeveringBevragingService$1 [PT]

ServerAdmin support@modernodam.nl
ServerName brp-proeftuin-links.modernodam.nl
ErrorLog /var/log/apache2/ssl_error.log
LogLevel info
CustomLog /var/log/apache2/ssl_access.log combined
SSLEngine on
SSLCertificateFile /etc/ssl/brp-server.crt
SSLCertificateKeyFile /etc/ssl/brp-server.key
SSLCACertificateFile /etc/ssl/brp-ca.crt
SSLVerifyClient require
SSLVerifyDepth 10
SSLProxyCipherSuite
TLS_DHE_RSA_WITH_AES_128_CBC_SHA:TLS_RSA_WITH_AES_128_CBC_SHA:
TLS_RSA_WITH_AES_256_CBC_SHA:TLS_DHE_RSA_WITH_AES_256_CBC_SHA:
SSL_RSA_WITH_AES_128_CBC_SHA:TLS_RSA_WITH_3DES_EDE_CBC_SHA

</VirtualHost>
<VirtualHost *:443>
DocumentRoot /var/www

<Directory />
  Require all denied
</Directory>

<Directory /var/www>
  Require all granted
  Options None
</Directory>
```

```
        ProxyRequests Off
        ProxyPreserveHost On


        ProxyPass /bijhouding http://pd-
dok02.modernodam.nl:8780/bijhouding
        ProxyPass /bevraging http://pd-
dok02.modernodam.nl:8980/bevraging
        ProxyPass /afnemerindicaties http://pd-
dok02.modernodam.nl:8480/afnemerindicaties
        ProxyPass /synchronisatie http://pd-
dok02.modernodam.nl:8380/synchronisatie

        RequestHeader set X-SSL-SSL_CLIENT_S_DN
"%{SSL_CLIENT_S_DN}s"
        SSLOptions +StdEnvVars +ExportCertData

        <Proxy http://pd-dok02.modernodam.nl:8780>
              Require all granted
        </Proxy>

        <Proxy http://pd-dok02.modernodam.nl:8480>
              Require all granted
        </Proxy>

        <Proxy http://pd-dok02.modernodam.nl:8380>
              Require all granted
        </Proxy>

        <Proxy http://pd-dok01.modernodam.nl:8080>
              Require all granted
        </Proxy>

RewriteEngine on
RewriteRule
^/brp/bijhouding/BijhoudingService(.+)              /bijhoudin
g/BijhoudingService$1 [PT]
RewriteRule
^/brp/bijhouding/DocumentarchiefService(.+)         /documenta
rchief/DocumentarchiefService$1 [PT]
RewriteRule
^/brp/bijhouding/BevragingService(.+)               /bevraging
/BijhoudingBevragingService$1 [PT]
RewriteRule
^/brp/levering/BevragingService(.+)                 /bevraging
/LeveringBevragingService$1 [PT]
RewriteRule
^/brp/levering/BevragingBulkService(.+)             /bevraging
/LeveringBevragingBulkService$1 [PT]
RewriteRule
^/brp/levering/SynchronisatieService(.+)            /synchroni
satie/SynchronisatieService$1 [PT]
```

```
RewriteRule
^/brp/levering/AfnemerindicatiesService(.+)         /afnemerin
dicaties/AfnemerindicatiesService$1 [PT]
RewriteRule
^/brp/terugmelding/TerugmeldingService(.+)          /terugmeld
ing/TerugmeldingService$1 [PT]
RewriteRule
^/brp/vrijeberichten/VrijeBerichtenService(.+)      /vrijeberi
chten/VrijeBerichtenService$1 [PT]
RewriteRule
^/brp/levering/BevragingService(.+)                 /bevraging
/LeveringBevragingService$1 [PT]

ServerAdmin support@modernodam.nl
ServerName brp-proeftuin-tribune.modernodam.nl
ErrorLog /var/log/apache2/ssl_error.log
LogLevel info
CustomLog /var/log/apache2/ssl_access.log combined
SSLEngine on
SSLCertificateFile /etc/ssl/brp-tribune-server.crt
SSLCertificateKeyFile /etc/ssl/brp-tribune-server.key
SSLCACertificateFile /etc/ssl/brp-ca.crt
SSLVerifyClient require
SSLVerifyDepth 10
SSLProxyCipherSuite
TLS_DHE_RSA_WITH_AES_128_CBC_SHA:TLS_RSA_WITH_AES_128_CBC_SHA:
TLS_RSA_WITH_AES_256_CBC_SHA:TLS_DHE_RSA_WITH_AES_256_CBC_SHA:
SSL_RSA_WITH_AES_128_CBC_SHA:TLS_RSA_WITH_3DES_EDE_CBC_SHA

</VirtualHost>
</IfModule>
```

Bijlage F Apache configuratie pt-rechts-ssl

```
<IfModule mod_ssl.c>

<VirtualHost *:443>

ServerAdmin support@modernodam.nl
ServerName brp-proeftuin.modernodam.nl
ErrorLog /var/log/apache2/ssl_error.log
LogLevel info
CustomLog /var/log/apache2/ssl_access.log combined
SSLEngine on
SSLCertificateFile /etc/ssl/brp-server.crt
SSLCertificateKeyFile /etc/ssl/brp-server.key
SSLCACertificateFile /etc/ssl/brp-ca.crt
SSLVerifyClient require
SSLVerifyDepth 10
SSLProxyCipherSuite
TLS_DHE_RSA_WITH_AES_128_CBC_SHA:TLS_RSA_WITH_AES_128_CBC_SHA:
TLS_RSA_WITH_AES_256_CBC_SHA:TLS_DHE_RSA_WITH_AES_256_CBC_SHA:
SSL_RSA_WITH_AES_128_CBC_SHA:TLS_RSA_WITH_3DES_EDE_CBC_SHA

SetEnv nokeepalive ssl-unclean-shutdown

DocumentRoot /var/www

<Directory />
  Require all denied
</Directory>

<Directory /var/www>
  Require all granted
  Options None
</Directory>

        ProxyRequests Off
        ProxyPreserveHost On

        ProxyPass /bijhouding http://pt-
dok02.modernodam.nl:8780/bijhouding
        ProxyPass /bevraging http://pt-
dok02.modernodam.nl:8980/bevraging
        ProxyPass /afnemerindicaties http://pt-
dok02.modernodam.nl:8480/afnemerindicaties
        ProxyPass /synchronisatie http://pt-
dok02.modernodam.nl:8380/synchronisatie

        RequestHeader set X-SSL-SSL_CLIENT_S_DN
"%{SSL_CLIENT_S_DN}s"
        SSLOptions +StdEnvVars +ExportCertData

        <Proxy http://pt-dok02.modernodam.nl:8780>
              Require all granted
        </Proxy>
```

```
        <Proxy http://pt-dok02.modernodam.nl:8480>
              Require all granted
        </Proxy>

        <Proxy http://pt-dok01.modernodam.nl:8980>
              Require all granted
        </Proxy>

        <Proxy http://pt-dok02.modernodam.nl:8380>
              Require all granted
        </Proxy>
RewriteEngine on
RewriteRule
^/brp/bijhouding/BijhoudingService(.+)              /bijhoudin
g/BijhoudingService$1 [PT]
RewriteRule
^/brp/levering/BevragingService(.+)                 /bevraging
/LeveringBevragingService$1 [PT]
RewriteRule
^/brp/levering/AfnemerindicatiesService(.+)         /afnemerin
dicaties/AfnemerindicatiesService$1 [PT]
RewriteRule
^/brp/synchronisatie/SynchronisatieService(.+)      /synchroni
satie/SynchronisatieService$1 [PT]

</VirtualHost>

<VirtualHost *:443>

ServerAdmin support@modernodam.nl
ServerName brp-proeftuin-rechts.modernodam.nl
ErrorLog /var/log/apache2/ssl_error.log
LogLevel info
CustomLog /var/log/apache2/ssl_access.log combined
SSLEngine on
SSLCertificateFile /etc/ssl/brp-rechts-server.crt
SSLCertificateKeyFile /etc/ssl/brp-rechts-server.key
SSLCACertificateFile /etc/ssl/brp-ca.crt
SSLVerifyClient require
SSLVerifyDepth 10
SSLProxyCipherSuite
TLS_DHE_RSA_WITH_AES_128_CBC_SHA:TLS_RSA_WITH_AES_128_CBC_SHA:
TLS_RSA_WITH_AES_256_CBC_SHA:TLS_DHE_RSA_WITH_AES_256_CBC_SHA:
SSL_RSA_WITH_AES_128_CBC_SHA:TLS_RSA_WITH_3DES_EDE_CBC_SHA

SetEnv nokeepalive ssl-unclean-shutdown

DocumentRoot /var/www

<Directory />
  Require all denied
</Directory>

<Directory /var/www>
  Require all granted
```

```
  Options None
</Directory>

        ProxyRequests Off
        ProxyPreserveHost On

        ProxyPass /bijhouding http://pr-
dok02.modernodam.nl:8780/bijhouding
        ProxyPass /bevraging http://pr-
dok02.modernodam.nl:8980/brp-delivery-bevraging
        ProxyPass /afnemerindicaties http://pr-
dok02.modernodam.nl:8480/brp-delivery-afnemerindicatie
        ProxyPass /synchronisatie http://pr-
dok02.modernodam.nl:8380/brp-delivery-synchronisatie

        RequestHeader set X-SSL-SSL_CLIENT_S_DN
"%{SSL_CLIENT_S_DN}s"
        SSLOptions +StdEnvVars +ExportCertData

        <Proxy http://pr-dok02.modernodam.nl:8780>
              Require all granted
        </Proxy>

        <Proxy http://pr-dok02.modernodam.nl:8480>
              Require all granted
        </Proxy>

        <Proxy http://pr-dok01.modernodam.nl:8980>
              Require all granted
        </Proxy>

        <Proxy http://pr-dok02.modernodam.nl:8380>
              Require all granted
        </Proxy>

RewriteEngine on
RewriteRule
^/brp/bijhouding/BijhoudingService(.+)              /bijhoudin
g/BijhoudingService$1 [PT]
RewriteRule
^/brp/levering/BevragingService(.+)                 /bevraging
/LeveringBevragingService$1 [PT]
RewriteRule
^/brp/levering/AfnemerindicatiesService(.+)         /afnemerin
dicaties/AfnemerindicatiesService$1 [PT]
RewriteRule
^/brp/synchronisatie/SynchronisatieService(.+)      /synchroni
satie/SynchronisatieService$1 [PT]

</VirtualHost>

<VirtualHost *:443>

ServerAdmin support@modernodam.nl
ServerName brp-proeftuin-test.modernodam.nl
```

```
ErrorLog /var/log/apache2/ssl_error.log
LogLevel info
CustomLog /var/log/apache2/ssl_access.log combined
SSLEngine on
SSLCertificateFile /etc/ssl/brp-test-server.crt
SSLCertificateKeyFile /etc/ssl/brp-test-server.key
SSLCACertificateFile /etc/ssl/brp-ca.crt
SSLVerifyClient require
SSLVerifyDepth 10
SSLProxyCipherSuite
TLS_DHE_RSA_WITH_AES_128_CBC_SHA:TLS_RSA_WITH_AES_128_CBC_SHA:
TLS_RSA_WITH_AES_256_CBC_SHA:TLS_DHE_RSA_WITH_AES_256_CBC_SHA:
SSL_RSA_WITH_AES_128_CBC_SHA:TLS_RSA_WITH_3DES_EDE_CBC_SHA

SetEnv nokeepalive ssl-unclean-shutdown

DocumentRoot /var/www

<Directory />
  Require all denied
</Directory>

<Directory /var/www>
  Require all granted
  Options None
</Directory>

        ProxyRequests Off
        ProxyPreserveHost On

        ProxyPass /bijhouding http://pt-
dok02.modernodam.nl:8780/bijhouding
        ProxyPass /bevraging http://pt-
dok01.modernodam.nl:8980/bevraging
        ProxyPass /afnemerindicaties http://pt-
dok02.modernodam.nl:8480/afnemerindicaties
        ProxyPass /synchronisatie http://pt-
dok02.modernodam.nl:8380/synchronisatie

        RequestHeader set X-SSL-SSL_CLIENT_S_DN
"%{SSL_CLIENT_S_DN}s"
        SSLOptions +StdEnvVars +ExportCertData

        <Proxy http://pt-dok02.modernodam.nl:8780>
              Require all granted
        </Proxy>

        <Proxy http://pt-dok02.modernodam.nl:8480>
              Require all granted
        </Proxy>

        <Proxy http://pt-dok01.modernodam.nl:8980>
              Require all granted
        </Proxy>
```

```
        <Proxy http://pt-dok02.modernodam.nl:8380>
              Require all granted
        </Proxy>

RewriteEngine on
RewriteRule
^/brp/bijhouding/BijhoudingService(.+)              /bijhoudin
g/BijhoudingService$1 [PT]
RewriteRule
^/brp/levering/BevragingService(.+)                 /bevraging
/LeveringBevragingService$1 [PT]
RewriteRule
^/brp/levering/AfnemerindicatiesService(.+)         /afnemerin
dicaties/AfnemerindicatiesService$1 [PT]
RewriteRule
^/brp/synchronisatie/SynchronisatieService(.+)      /synchroni
satie/SynchronisatieService$1 [PT]

</VirtualHost>

<VirtualHost *:443>

ServerAdmin support@modernodam.nl
ServerName brp-proeftuin-tussen.modernodam.nl
ErrorLog /var/log/apache2/ssl_error.log
LogLevel info
CustomLog /var/log/apache2/ssl_access.log combined
SSLEngine on
SSLCertificateFile /etc/ssl/tussen/brp-server.crt
SSLCertificateKeyFile /etc/ssl/tussen/brp-server.key
SSLCACertificateFile /etc/ssl/tussen/brp-ca.crt
SSLVerifyClient require
SSLVerifyDepth 10
SSLProxyCipherSuite
TLS_DHE_RSA_WITH_AES_128_CBC_SHA:TLS_RSA_WITH_AES_128_CBC_SHA:
TLS_RSA_WITH_AES_256_CBC_SHA:TLS_DHE_RSA_WITH_AES_256_CBC_SHA:
SSL_RSA_WITH_AES_128_CBC_SHA:TLS_RSA_WITH_3DES_EDE_CBC_SHA

SetEnv nokeepalive ssl-unclean-shutdown

DocumentRoot /var/www

<Directory />
  Require all denied
</Directory>

<Directory /var/www>
  Require all granted
  Options None
</Directory>

        ProxyRequests Off
        ProxyPreserveHost On
```

```
        ProxyPass /bijhouding http://ptt-
dok02.modernodam.nl:8780/bijhouding
        ProxyPass /bevraging http://ptt-
dok02.modernodam.nl:8980/bevraging
        ProxyPass /afnemerindicaties http://ptt-
dok02.modernodam.nl:8480/afnemerindicaties
        ProxyPass /synchronisatie http://ptt-
dok02.modernodam.nl:8380/synchronisatie

        RequestHeader set X-SSL-SSL_CLIENT_S_DN
"%{SSL_CLIENT_S_DN}s"
        SSLOptions +StdEnvVars +ExportCertData

        <Proxy http://ptt-dok02.modernodam.nl:8780>
              Require all granted
        </Proxy>

        <Proxy http://ptt-dok02.modernodam.nl:8480>
              Require all granted
        </Proxy>

        <Proxy http://ptt-dok01.modernodam.nl:8980>
              Require all granted
        </Proxy>

        <Proxy http://ptt-dok02.modernodam.nl:8380>
              Require all granted
        </Proxy>

RewriteEngine on
RewriteRule
^/brp/bijhouding/BijhoudingService(.+)              /bijhoudin
g/BijhoudingService$1 [PT]
RewriteRule
^/brp/levering/BevragingService(.+)                 /bevraging
/LeveringBevragingService$1 [PT]
RewriteRule
^/brp/levering/AfnemerindicatiesService(.+)         /afnemerin
dicaties/AfnemerindicatiesService$1 [PT]
RewriteRule
^/brp/synchronisatie/SynchronisatieService(.+)      /synchroni
satie/SynchronisatieService$1 [PT]

</VirtualHost>
</IfModule>
```

Bijlage G Interfaces voor pt-links-ssl

```
# This file describes the network interfaces available on your
system
# and how to activate them. For more information, see
interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens32
iface ens32 inet static
  address 192.168.216.10
  netmask 255.255.255.0
  gateway 192.168.216.1
```

Bijlage H Interfaces voor pt-rechts-ssl

```
# This file describes the network interfaces available on your
system
# and how to activate them. For more information, see
interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens32
iface ens32 inet static
        address 192.168.208.100
        netmask 255.255.255.0
        gateway 192.168.208.1
```

Bijlage I Postgres modules

```
class postgres::server94 {

  group { "postgres":
    ensure => "present",
    gid    => "26",
    before => User['postgres'],
  }

  user { "postgres":
    ensure => "present",
    home   => "/var/lib/pgsql/",
    uid    => "26",
    gid    => "26",
    before => Package['postgresql94-server'],
  }



  package { "postgresql94-server":
    ensure => installed,
    before => Package['postgresql94-contrib'],
  }

  package { "postgresql94-contrib":
    ensure => installed,
    before => Package['nagios-plugins-pgsql'],
  }
  package { "nagios-plugins-pgsql":
    ensure => installed,
    before => File['/opt/sa/bin/postgres_init.sh'],
  }

  file { "/opt/sa/bin/postgres_init.sh":
    owner   => postgres,
    group   => root,
    mode    => 0540,
    before  => File['/opt/sa/bin/postgres_udb_creator.sh'],
    content =>
template("postgres/server94/postgres_init.sh.erb");
  }

  file { "/opt/sa/bin/postgres_udb_creator.sh":
    owner   => postgres,
    group   => postgres,
    mode    => 0540,
    before  => File['/etc/profile.d/postgres.sh'],
    content =>
template("postgres/server94/postgres_udb_creator.sh.erb");
  }



  file { "/etc/profile.d/postgres.sh":
    owner   => root,
```

```
    group   => root,
    mode    => 0555,
    before  => File['/etc/sysctl.conf'],
    content =>
template("postgres/server94/postgres_profile.sh.erb");
  }

  file { "/etc/sysctl.conf":
    owner   => root,
    group   => root,
    mode    => 0444,
    before  => File['/opt/sa/bin/postgres_grant_select.sh'],
    content => template("postgres/server94/sysctl.conf.erb");
  }

  file { "/opt/sa/bin/postgres_grant_select.sh":
    owner   => postgres,
    group   => root,
    mode    => 0540,
    before  => Exec['postgres-initdb'],
    content =>
template("postgres/server94/postgres_grant_select.sh.erb");
  }

  exec { postgres-initdb:
    command   => "/opt/sa/bin/postgres_init.sh",
    logoutput => true,
    unless    => "/bin/test -f
/var/lib/pgsql/9.3/data/PG_VERSION",
    before    => File['/var/lib/pgsql/9.4/data/pg_hba.conf'],
  }

  file { "/var/lib/pgsql/9.4/data/pg_hba.conf":
    owner   => postgres,
    group   => postgres,
    mode    => 0444,
    before  =>
File['/var/lib/pgsql/9.4/data/postgresql.conf'],
    content => template("postgres/server94/pg_hba.conf.erb");
  }

 file { "/var/lib/pgsql/9.4/data/postgresql.conf":
    owner   => postgres,
    group   => postgres,
    mode    => 0444,
    content =>
template("postgres/server94/postgresql.conf.erb");
  }

  exec { restart-postgres:
    command     => "/bin/systemctl restart postgresql-9.4",
    logoutput   => true,
    refreshonly => true,
    require     => Exec['postgres-initdb'],
    subscribe   =>
File["/var/lib/pgsql/9.4/data/postgresql.conf"],
```

```
  }


  exec { subscribe-sysctl:
    command     => "/usr/sbin/sysctl -p",
    logoutput   => true,
    subscribe   => File["/etc/sysctl.conf"],
    require     => Exec['postgres-initdb'],
    refreshonly => true,
  }

}
```