Virtuelle Multiserverumgebung mit dedizierten Web & MySQL, Email & DNS Servern unter Debian Squeeze mit ISPConfig 3

Version 1.0

Autor: Michel Käser <info [at] rackster [dot] ch>
Übersetzt: Christian Schmalfeld <c [dot] schmalfeld [at] projektfarm [dot] de>
Letzte Änderung 05/30/2012

Dieses Tutorial beschreibt, wie Sie unter Debian Squeeze mit OpenVZ einen einzelnen dedizierten Server als virtuelle Multiserverumgebung mit dedizierten Web, Mail, MySQL und DNS Servern aufsetzen. Außerdem wird gezeigt, wie Sie all diese Server verwalten. Zusätzlich erfahren Sie, wie Sie einige nützliche Pakete installieren, die Ihre Server schützen und helfen, sie zu überwachen.

Am Ende des Tutorials haben Sie eine vollfunktionale, virtuelle Multiserverumgebung.

Für die Richtigkeit der Inhalte des Tutorials gebe ich keinerlei Garantie!

1 Anforderungen

Um diesem Tutorial zu folgen benötigen Sie folgendes:
einen dedizierten Server
mindestens fünf IPs
eine Menge Zeit

2 Vorbemerkung

In diesem Tutorial benutze ich den dedizierten Server http://www.hetzner.de/hosting/produkte_rootserver/ex4 mit Flexi-Pack und einem zusätzlichen /28 Subnetz (14 IPs).

Das Ziel ist es, die folgenden Server aufzusetzen:
Typ: Node
Hardware: Dediziert
Hostname: *root.example.tld*
192.168.1.1
Typ: Container
Hardware: Virtuell
Hostname: *web.example.tld*
192.168.1.2
Typ: Container
Hardware: Virtuell
Hostname: *mail.example.tld*
192.168.1.3
Typ: Container
Hardware: Virtuell
Hostname: *ns1.example.tld*
192.168.1.4
Typ: Container
Hardware: Virtuell

Hostname: *ns2.example.tld*

192.168.1.5

3 Das Basissystem

Ich nehme im folgenden an, dass Sie den selben dedizierten Server gewählt haben wie ich. Die Hetzner Web-Oberfläche erlaubt Ihnen eine Reihe von Distributionen zu installieren. Wählen Sie die minimale Debian 6.0 64-bit Installation.

Das Basissystem wird dadurch für Sie installiert und Sie brauchen es nicht selbst zu konfigurieren. Auch das root Passwort werden Sie bekommen.

4 Installation von OpenVZ + OVZ Web Panel

Sobald der Server fertig ist, melden Sie sich mit den erhaltenen Daten an. Führen Sie zunächst ein Update, gefolgt von einem Upgrade aus

```
apt-get update && apt-get -y upgrade && apt-get -y dist-upgrade
```

welches Ihren Server auf die neuste Version aktualisiert.

Installieren Sie dann einige zusätzliche Pakete:

```
apt-get -y install nano wget ntp ntpdate
```

4.1 Installation von OpenVZ

Installieren Sie nun OpenVZ, die Basis für die virtuelle Multiserverumgebung.

Ein OpenVZ Kernel und die vzctl, vzquota und vzdump Pakete sind in den Debian Squeeze Repositories verfügbar, Sie können diese also folgendermaßen installieren:

```
apt-get install linux-image-openvz-amd64 vzctl vzquota vzdump
```

Erstellen Sie einen Symlink von */var/lib/vz* zu */vz* um Abwärtskompatibilität herzustellen:

```
ln -s /var/lib/vz /vz
```

Öffnen Sie die */etc/sysctl.conf* Datei und stellen Sie sicher, dass sie die folgenden Einstellungen enthält:

```
nano /etc/sysctl.conf
```

```
[...]

net.ipv4.conf.all.rp_filter=1
net.ipv4.icmp_echo_ignore_broadcasts=1
net.ipv4.conf.default.forwarding=1
net.ipv4.conf.default.proxy_arp = 0
net.ipv4.ip_forward=1
kernel.sysrq = 1
net.ipv4.conf.default.send_redirects = 1
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.eth0.proxy_arp=1
[...]
```

Mussten Sie die */etc/sysctl.conf* Datei editieren, benutzen Sie danach den

```
sysctl -p
```

Befehl.

Der folgende Schritt ist wichtig, falls die IP-Adressen Ihrer virtuellen Maschinen aus einem anderen Subnetz stammen als die IP-Adresse Ihres Hostsystems. Führen Sie ihn nicht aus, wird das Netzwerk bei den virtuellen Maschinen nicht funktionieren!

Öffnen Sie */etc/vz/vz.conf* und setzen Sie *NEIGHBOUR_DEVS* gleich *all*:

```
nano /etc/vz/vz.conf
```

```
[...]

# Controls which interfaces to send ARP requests and modify APR tables on.
NEIGHBOUR_DEVS=all
[...]
```

Starten Sie das System dann neu:

```
reboot
```

Startet Ihr System ohne Probleme neu, ist alles in Ordnung!

Benutzen Sie

```
uname -r
```

um den OpenVZ Kernel anzuzeigen:

```
root@root:~# uname -r

2.6.32-5-openvz-amd64
```

Da Hetzner */home* auf einer seperaten Festplatte mountet, können Sie diese als OpenVZ Backup Ort benutzen. Benutzen Sie dazu:

```
rm -rf /var/lib/vz/dump
```

```
ln -s /home/backup/vz /var/lib/vz/dump
```

Da wir fail2ban in unseren virtuellen Containern benutzen werden, müssen Sie IPTables Unterstützung für diese erlauben. Dies tun Sie, indem Sie die */etc/vz/vz.conf* Datei editieren:

```
nano /etc/vz/vz.conf
```

Suchen Sie die Zeile, die mit *IPTABLES* beginnt und kommentieren Sie diese aus (setzen Sie eine Raute (#) davor). Fügen Sie danach folgende Zeile ein:

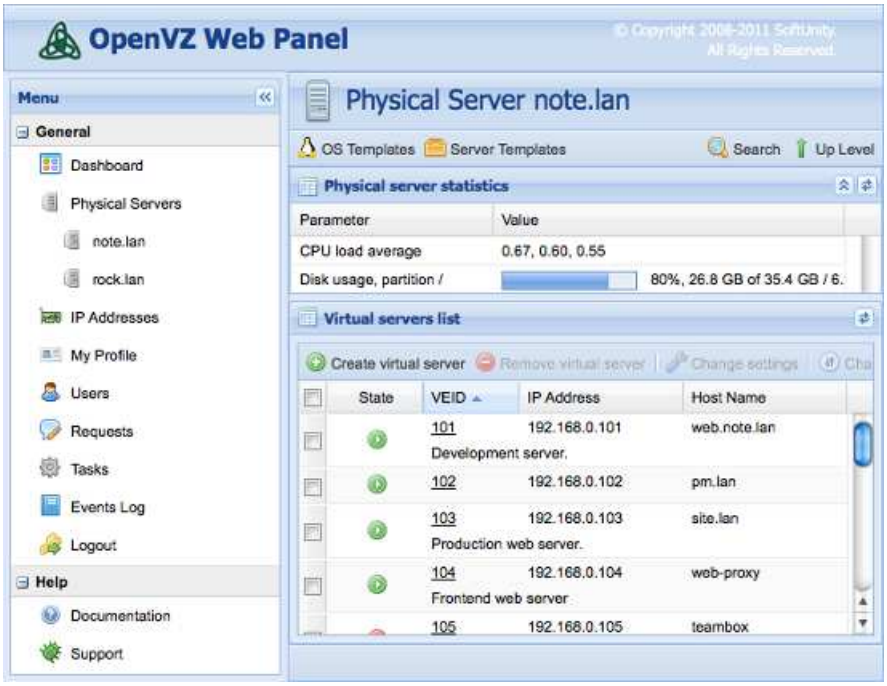
```
[...]

IPTABLES="ipt_REJECT ipt_tos ipt_limit ipt_multiport iptable_filter iptable__mangle ipt_TCPMSS ipt_tcpmss i
```

Aktivieren Sie dann das state Modul im Kernel:

```
modprobe xt_state
```

4.2 Installation des OVZ Web Panel

Das OpenVZ Web Panel ist ein Web-basiertes GUI Front-End zur Kontrolle von Hardware und virtuellen Servern mit der OpenVZ Virtualisationstechnologie.



Der einfachste Weg das OpenVZ Web Panel zu installieren ist der folgende Befehl:

```
wget -O - http://ovz-web-panel.googlecode.com/svn/installer/ai.sh | sh
```

Nach der Installation sollte das Panel unter folgender URL erreichbar sein:

```
http://<192.168.1.1>:3000
```

Die Login-Daten des Standardadministrators sind: admin/admin. Vergessen Sie nicht, das Standardpasswort zu ändern.

5 Erstellen der virtuellen Server

Nun können Sie das OVZ Web Panel benutzen um die virtuellen Server zu erstellen. Melden Sie sich am Panel an und fügen Sie Ihre IP-Adressen unter *IP Addresses* hinzu. Klicken Sie dann auf *localhost* und *OS Templates*.

Laden Sie nun eine Vorlage für Ihre virtuellen Server herunter. Tun Sie dies in dem Sie auf *Install New OS Template* -> *Contributed* klicken und *debian-6.0-amd64-minimal* auswählen.

Gehen Sie zurück zu *localhost* und klicken Sie auf *Create virtual server*. Füllen Sie die Felder wie folgt aus:
Server ID (VEID): eine Zahl (ich würde die letzte Ziffer Ihrer IP wählen, also 2 für die erste)
OS Template: die richtige Vorlage ist bereits ausgewählt
Server Template: unlimited (unbegrenzt)
IP Address: *192.168.1.2*
Host Name: *web.example.tld*
DNS Server: *8.8.4.4 8.8.8.8* (Googles DNS)
belassen Sie den Rest wie vorgegeben und wählen Sie Speicherplatz, RAM und CPU nach Ihren Wünschen...
Wiederholen Sie diesen Schritt für all Ihre virtuellen Server (insgesamt 4 Mal: Web, Mail, 2x DNS).

5.1 Vorbereiten der virtuellen Server

Melden Sie sich nun an jedem virtuellen Server an und benutzen folgende Befehle:

```
apt-get update && apt-get -y upgrade && apt-get -y dist-upgrade
```

```
apt-get -y install nano wget ntp ntpdate
```

Diese werden sie auf die aktuelle Version aktualisieren und einige zusätzliche Pakete installieren.

6 Installation der dedizierten Server

6.1 Installation des Web/DB Servers

Editieren Sie die hosts Datei und fügen Sie die IP-Adressen und Hostnamen aller Server hinzu. Vergessen Sie nicht diese an Ihr Setup anzupassen.

```
nano /etc/hosts
```

```
127.0.0.1 localhost

192.168.1.2 web.example.tld
192.168.1.3 mail.example.tld
192.168.1.4 ns1.example.tld
192.168.1.5 ns2.example.tld

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

Tragen Sie den Hostnamen des Servers ein:

```
echo web.example.tld > /etc/hostname
/etc/init.d/hostname.sh start
```

Installieren Sie den MySQL Server. Ein Exemplar eines MySQL Servers ist auf jedem Server notwendig, da ISPConfig diesen benutzt um die Konfiguration der Server zu synchronisieren.

```
apt-get -y install mysql-client mysql-server
```

Geben Sie, sobald Sie dazu aufgefordert werden, das neue MySQL ein.

MySQL soll alle Netzwerkschnittstellen benutzen, nicht nur localhost, deshalb müssen Sie die */etc/mysql/my.cnf* Datei editieren und die Zeile *bind-address = 127.0.0.1* auskommentieren:

```
nano /etc/mysql/my.cnf
```

```
[...]

# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
#bind-address = 127.0.0.1
[...]
```

Starten Sie MySQL dann neu:

```
/etc/init.d/mysql restart
```

Installieren Sie nun Apache2, PHP5, phpMyAdmin, FCGI, suExec, Pear und mcrypt wie folgt:

```
apt-get -y install apache2 apache2.2-common apache2-doc apache2-mpm-prefork apache2-utils libexpat1
ssl-cert libapache2-mod-php5 php5 php5-common php5-gd php5-mysql php5-imap phpmyadmin php5-cli php5-cgi
libapache2-mod-fcgid apache2-suexec php-pear php-auth php5-mcrypt mcrypt php5-imagick imagemagick
libapache2-mod-suphp libopenssl-ruby libapache2-mod-ruby sudo zip wget
```

Beantworten Sie folgende Frage:

Web server to reconfigure automatically: **<-- apache2**

Benutzen Sie folgenden Befehl um die Apache Module *suexec*, *rewrite*, *ssl*, *actions*, *headers*, *expires* und *include* zu aktivieren:

```
a2enmod suexec rewrite ssl actions include ruby dav_fs dav auth_digest headers expires
```

Installieren Sie PureFTPd:

```
apt-get -y install pure-ftpd-common pure-ftpd-mysql
```

Editieren Sie die */etc/default/pure-ftpd-common* Datei...

```
vi /etc/default/pure-ftpd-common
```

... und stellen Sie sicher, dass *VIRTUALCHROOT=true* gesetzt ist:

```
[...]

VIRTUALCHROOT=true
[...]
```

Konfigurieren Sie nun PureFTPd, sodass es FTP und TLS Sitzungen erlaubt. FTP ist ein sehr unsicheres Protokoll, da alle Passwörter und Daten in klarem Text übertragen werden. Durch Benutzung von TLS wird jegliche Kommunikation verschlüsselt, wodurch FTP sehr viel sicherer gemacht wird.

Wollen Sie FTP und TLS Sitzungen erlauben, benutzen Sie:

```
echo 1 > /etc/pure-ftpd/conf/TLS
```

Um TLS zu benutzen, müssen Sie ein SSL Zertifikat erstellen. Ich erstelle es in */etc/ssl/private/*, deshalb muss ich dieses Verzeichnis erst erstellen:

```
mkdir -p /etc/ssl/private/
```

Danach können Sie das SSL Zertifikat generieren:

```
openssl req -x509 -nodes -days 7300 -newkey rsa:2048 -keyout /etc/ssl/private/pure-ftpd.pem -out
/etc/ssl/private/pure-ftpd.pem
```

Country Name (2 letter code) [AU]: **<-- Geben Sie Ihr Land an (z.B., "DE").** *State or Province Name (full name) [Some-State]:* **<-- Geben Sie Ihr Bundesland an (z.B. Niedersachsen).** *Locality Name (eg, city) []:* **<-- Geben Sie Ihre Stadt an (z.B. Lueneburg).** *Organization Name (eg, company) [Internet Widgits Pty Ltd]:* **<-- Geben Sie den Namen Ihrer Firma an.** *Organizational Unit Name (eg, section) []:* **<-- Geben Sie den Namen Ihrer Abteilung an (z.B. "IT Department").** *Common Name (eg, YOUR name) []:* **<-- Geben Sie den qualifiezierten Domainnamen Ihres Systems an (z.B. "server1.example.com").** *Email Address []:* **<-- Geben Sie Ihre E-Mail Adresse an.**

Ändern Sie die Zugriffsrechte auf das SSL Zertifikat:

```
chmod 600 /etc/ssl/private/pure-ftpd.pem
```

Installieren Sie vlogger, webalizer und awstats:

```
apt-get -y install vlogger webalizer awstats
```

Öffnen Sie danach */etc/cron.d/awstats* ...

```
vi /etc/cron.d/awstats
```

... und kommentieren beide Cron Jobs in der Datei aus:

```
#*/10 * * * * www-data [ -x /usr/share/awstats/tools/update.sh ] && /usr/share/awstats/tools/update.sh


# Generate static reports:
#10 03 * * * www-data [ -x /usr/share/awstats/tools/buildstatic.sh ] && /usr/share/awstats/tools/buildstati
```

Installieren Sie Jailkit: Jailkit wird nur gebraucht, wenn Sie SSH Benutzer und Cron Jobs chrooten wollen. Es kann wie folgt installiert werden (Wichtig: Jailkit muss vor ISPConfig installiert werden - dies kann nicht nachträglich geschehen!):

```
apt-get -y install build-essential autoconf automake1.9 libtool flex bison debhelper
```

```
cd /tmp
```

```
wget http://olivier.sessink.nl/jailkit/jailkit-2.14.tar.gz
tar xvfz jailkit-2.14.tar.gz
cd jailkit-2.14
./debian/rules binary
cd ..
dpkg -i jailkit_2.14-1_*.deb
rm -rf jailkit-2.14*
```

Installieren Sie fail2ban: Dies ist zwar optional, wird aber empfohlen, da der ISPConfig Monitor versucht, dessen Log anzuzeigen:

```
apt-get install fail2ban
```

Um fail2ban PureFTPd überwachen zu lassen, erstellen Sie die Datei */etc/fail2ban/jail.local*:

```
vi /etc/fail2ban/jail.local
```

```
[pureftpd]


enabled = true
port = ftp
filter = pureftpd
logpath = /var/log/syslog
maxretry = 3
```

Danach erstellen Sie die folgende Filterdatei:

```
vi /etc/fail2ban/filter.d/pureftpd.conf
```

```
[Definition]

failregex = .*pure-ftpd: (.*@<HOST>) [WARNING] Authentication failed for user.*
ignoreregex =
```

Starten Sie fail2ban danach neu:

```
/etc/init.d/fail2ban restart
```

Als nächstes installieren Sie ISPConfig. Um zum Downloadlink der aktuellsten Version zu kommen, besuchen Sie bitte die ISPConfig Webseite: http://www.ispconfig.org/ispconfig-3/download/

Dies ist in unserem Setup der Master Server, auf dem die ISPConfig Kontrolloberfläche laufen wird. Um den anderen MySQL Exemplaren zu erlauben, sich während der Installation mit der MySQL Datenbank auf diesem Knoten zu verbinden, müssen Sie der Master Datenbank MySQL root Benutzereinträge für jeden Slave Server Hostnamen und deren IP-Adressen hinzufügen. Der einfachste Weg dies zu erledigen ist das webbasierte phpMyAdmin Administrationswerkzeug zu benutzen, welches Sie zuvor installiert haben. Öffnen Sie die URL *http://192.168.1.2/phpmyadmin* in einem Internetbrowser, melden Sie sich als MySQL root Benutzer an und führen Sie diese MySQL Befehle aus:

```
CREATE USER 'root'@'192.168.1.3' IDENTIFIED BY 'myrootpassword';
```

```
GRANT ALL PRIVILEGES ON * . * TO 'root'@'192.168.1.3' IDENTIFIED BY 'myrootpassword' WITH GRANT OPTION
MAX_QUERIES_PER_HOUR 0 MAX_CONNECTIONS_PER_HOUR 0 MAX_UPDATES_PER_HOUR 0 MAX_USER_CONNECTIONS 0 ;
```

```
CREATE USER 'root'@'192.168.1.4' IDENTIFIED BY 'myrootpassword';
```

```
GRANT ALL PRIVILEGES ON * . * TO 'root'@'192.168.1.4' IDENTIFIED BY 'myrootpassword' WITH GRANT OPTION
MAX_QUERIES_PER_HOUR 0 MAX_CONNECTIONS_PER_HOUR 0 MAX_UPDATES_PER_HOUR 0 MAX_USER_CONNECTIONS 0 ;
```

```
CREATE USER 'root'@'192.168.1.5' IDENTIFIED BY 'myrootpassword';
```

```
GRANT ALL PRIVILEGES ON * . * TO 'root'@'192.168.1.5' IDENTIFIED BY 'myrootpassword' WITH GRANT OPTION
MAX_QUERIES_PER_HOUR 0 MAX_CONNECTIONS_PER_HOUR 0 MAX_UPDATES_PER_HOUR 0 MAX_USER_CONNECTIONS 0 ;
```

```
CREATE USER 'root'@'mail.example.tld' IDENTIFIED BY
'myrootpassword';
```

```
GRANT ALL PRIVILEGES ON * . * TO 'root'@'mail.example.tld' IDENTIFIED BY 'myrootpassword' WITH GRANT
OPTION MAX_QUERIES_PER_HOUR 0 MAX_CONNECTIONS_PER_HOUR 0 MAX_UPDATES_PER_HOUR 0 MAX_USER_CONNECTIONS 0 ;
```

```
CREATE USER 'root'@'ns1.example.tld' IDENTIFIED BY 'myrootpassword';
```

```
GRANT ALL PRIVILEGES ON * . * TO 'root'@'ns1.example.tld' IDENTIFIED BY 'myrootpassword' WITH GRANT
OPTION MAX_QUERIES_PER_HOUR 0 MAX_CONNECTIONS_PER_HOUR 0 MAX_UPDATES_PER_HOUR 0 MAX_USER_CONNECTIONS 0 ;
```

```
CREATE USER 'root'@'ns2.example.tld' IDENTIFIED BY 'myrootpassword';
```

```
GRANT ALL PRIVILEGES ON * . * TO 'root'@'ns2.example.tld' IDENTIFIED BY 'myrootpassword' WITH GRANT
OPTION MAX_QUERIES_PER_HOUR 0 MAX_CONNECTIONS_PER_HOUR 0 MAX_UPDATES_PER_HOUR 0 MAX_USER_CONNECTIONS 0 ;
```

Ersetzen Sie in den obigen Befehlen die IP-Adressen (*192.168.1.3 - 192.168.1.5*) mit den IP-Adressen Ihrer Server, *mail.example.tld*, *ns1.example.tld* und *ns2.example.tld* mit den Hostnamen Ihrer Server und *myrootpassword* mit dem gewünschten root Passwort.

Klicken Sie auf den reload permissions Button oder starten Sie MySQL neu. Schließen Sie danach phpMyAdmin.

Kehren Sie zur Shell von *web.example.tld* zurück und laden Sie die aktuelle stabile Version von ISPConfig 3 herunter:

```
cd /tmp
wget http://www.ispconfig.org/downloads/ISPConfig-3-stable.tar.gz
tar xfz ISPConfig-3-stable.tar.gz
cd ispconfig3_install/install/
```

Starten Sie dann das Installationsskript:

```
php -q install.php
```

Select language (en,de) [en]: **<-- en**

Installation mode (standard,expert) [standard]: **<-- expert**

Full qualified hostname (FQDN) of the server, eg server2.domain.tld [web.example.tld]: **<-- web.example.tld**

MySQL server hostname [localhost]: **<-- localhost**

MySQL root username [root]: **<-- root**

MySQL root password []: **<-- Geben Sie hier Ihr SQL root Passwort ein**

MySQL database to create [dbispconfig]: **<-- dbispconfig**

MySQL charset [utf8]: **<-- utf8**

Shall this server join an existing ISPConfig multiserver setup (y,n) [n]: **<-- n**

Configure Mail (y,n) [y]: **<-- n**

Configure Jailkit (y,n) [y]: **<-- y**

Configure FTP Server (y,n) [y]: **<-- y**

Configure DNS Server (y,n) [y]: **<-- n**

Configure Apache Server (y,n) [y]: **<-- y**

Configure Firewall Server (y,n) [y]: **<--n**

Install ISPConfig Web-Interface (y,n) [y]: **<--y**

ISPConfig Port [8080]: **<-- 8080**

Enable SSL for the ISPConfig web interface (y,n) [y]: **<-- y**

Country Name (2 letter code) [AU]: **<-- *ENTER***

State or Province Name (full name) [Some-State]: **<-- ENTER**

Locality Name (eg, city) []: **<-- ENTER**

Organization Name (eg, company) [Internet Widgits Pty Ltd]: **<-- ENTER**

Organizational Unit Name (eg, section) []: **<-- ENTER**

Common Name (eg, YOUR name) []: **<-- ENTER**

Email Address []: **<-- ENTER**

A challenge password []: **<-- ENTER**

An optional company name []: **<-- ENTER**

Räumen Sie anschließend im Installationsverzeichnis auf:

```
cd /tmp
rm -rf /tmp/ispconfig3_install/install
```

```
rm -f /tmp/ISPConfig-3-stable.tar.gz
```

6.2 Installation des Mailservers

Editieren Sie die hosts Datei und fügen Sie die IP Adressen und Hostnamen aller Server hinzu. Achten Sie dabei darauf, dass Sie sie mit denen Ihres Setups ersetzen:

```
nano /etc/hosts
```

```
127.0.0.1 localhost

192.168.1.2 web.example.tld
192.168.1.3 mail.example.tld
192.168.1.4 ns1.example.tld
192.168.1.5 ns2.example.tld

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

Tragen Sie den Hostnamen des Servers ein:

```
echo mail.example.tld > /etc/hostname
echo mail.example.tld > /etc/mailname
/etc/init.d/hostname.sh start
```

Installieren Sie postfix, dovecot und MySQL mit einem einzigen Befehl:

```
apt-get -y install postfix postfix-mysql postfix-doc mysql-client mysql-server openssl getmail4 rkhunter
binutils dovecot-imapd dovecot-pop3d
```

Geben Sie, sobald Sie vom Installer dazu aufgefordert werden, das neue MySQL Passwort ein und beantworten Sie die anderen Fragen folgendermaßen:

General type of configuration? **<-- Internet site**

Mail name? **<-- mail.example.tld**

Um amavisd-new, SpamAssassin und ClamAV zu installieren benutzen Sie:

```
apt-get -y install amavisd-new spamassassin clamav clamav-daemon zoo unzip bzip2 arj nomarch lzop
cabextract apt-listchanges libnet-ldap-perl libauthen-sasl-perl clamav-docs daemon libio-string-perl
libio-socket-ssl-perl libnet-ident-perl zip libnet-dns-perl
```

Wollen Sie Mailinglisten auf Ihrem Server benutzen, so installieren Sie Mailman. Dieser Schritt ist optional. Mailman ist auf einen Apache Webserver angewiesen, wollen Sie also kein Apache auf Ihrem Mailserver laufen haben, sollten Sie Mailman nicht installieren.

```
apt-get -y install mailman
```

Der apt Installer von Mailman wird Sie auffordern, Sprachen für die Mailingliste auszuwählen. Erlauben Sie alle Sprachen, die in Mailman benutzen möchten. Erstellen Sie als nächstes die "mailman" Mailingliste

```
newlist mailman
```

und geben die E-Mail Adresse und das neue Passwort des Mailinglisten Administrators ein. Dies ist der letzte Schritt der Mailman Installation. Der nächste Befehl, welcher PHP installiert, muss auf jedem Server ausgeführt werden, ganz gleich ob Sie Mailman installiert haben oder nicht.

Installieren Sie dann die Kommandozeilenversion von PHP um PHP-basierte Skripts für ISPConfig ausführen zu können:

```
apt-get -y install php5-cli php5-mysql php5-mcrypt mcrypt
```

Installieren Sie fail2ban: Dies ist zwar optional, wird aber empfohlen, da der ISPConfig Monitor versucht, dessen Log anzuzeigen:

```
apt-get install fail2ban
```

Um fail2ban PureFTPd und Dovecot überwachen zu lassen, erstellen Sie die Datei */etc/fail2ban/jail.local*:

```
vi /etc/fail2ban/jail.local
```

```
[dovecot-pop3imap]


enabled = true
filter = dovecot-pop3imap
action = iptables-multiport[name=dovecot-pop3imap, port="pop3,pop3s,imap,imaps", protocol=tcp]
logpath = /var/log/mail.log
maxretry = 5
```

Erstellen Sie dann die folgende Filterdatei:

```
vi /etc/fail2ban/filter.d/dovecot-pop3imap.conf
```

```
[Definition]

failregex = (?: pop3-login|imap-login): .*(?:Authentication failure|Aborted login (auth failed|Aborted logi
ignoreregex =
```

Starten Sie fail2ban danach neu:

```
/etc/init.d/fail2ban restart
```

Installieren Sie nun ISPConfig 3 auf diesem Server. Für den Downloadlink der aktuellen stabilen ISPConfig 3 Version, besuchen Sie bitte die ISPConfig Webseite: http://www.ispconfig.org/ispconfig-3/download/

Laden Sie die aktuelle stabile ISPConfig 3 Version herunter:

```
cd /tmp
wget http://www.ispconfig.org/downloads/ISPConfig-3-stable.tar.gz
tar xfz ISPConfig-3-stable.tar.gz
cd ispconfig3_install/install/
```

Starten Sie dann das Installationsskript:

```
php -q install.php
```

Select language (en,de) [en]: **<-- en**

Installation mode (standard,expert) [standard]: **<-- expert**

Full qualified hostname (FQDN) of the server, eg server1.domain.tld [mail.example.tld]: **<-- mail.example.tld**

MySQL server hostname [localhost]: **<-- localhost**

MySQL root username [root]: **<-- root**

MySQL root password []: **<-- Geben Sie hier Ihr MySQL root Passwort an**

MySQL database to create [dbispconfig]: **<-- dbispconfig**

MySQL charset [utf8]: **<-- utf8**

Shall this server join an existing ISPConfig multiserver setup (y,n) [n]: **<-- y**

MySQL master server hostname []: **<-- web.example.tld**

MySQL master server root username [root]: **<-- root**

MySQL master server root password []: **<-- Geben Sie hier das root Passwort des Master Servers an**

MySQL master server database name [dbispconfig]: **<-- dbispconfig**

Configure Mail (y,n) [y]: **<-- y**

Country Name (2 letter code) [AU]: **<-- DE (Geben Sie hier den ISO Ländercode Ihres landes an)**

State or Province Name (full name) [Some-State]: **<-- Niedersachsen (Geben Sie Ihr Bundesland an)**

```
Locality Name (eg, city) []: <-- Lueneburg (Geben Sie Ihre Stadt an)
Organization Name (eg, company) [Internet Widgits Pty Ltd]: <- ENTER
Organizational Unit Name (eg, section) []: <- ENTER
Common Name (eg, YOUR name) []: <- ENTER
Email Address []: <-- ENTER
Configure Jailkit (y,n) [y]: <-- n
Configure FTP Server (y,n) [y]: <-- n
Configure DNS Server (y,n) [y]: <-- n
Configure Apache Server (y,n) [y]: <-- n
Configure Firewall Server (y,n) [y]: <--y
Install ISPConfig Web-Interface (y,n) [y]: <--n
```

Benutzen Sie...

```
rm -f /var/www/ispconfig
```

... um den ISPConfig Oberflächenlink im */var/www* Verzeichnis zu entfernen.

Räumen Sie anschließend im Installationsverzeichnis auf:

```
rm -rf /tmp/ispconfig3_install/install
rm -f /tmp/ISPConfig-3-stable.tar.gz
```

6.3 Installation des primären DNS Servers

Editieren Sie die hosts Datei und fügen die IP Adressen und Hostnamen aller Server hinzu. Denken Sie daran, diese an Ihr Setup anzupassen:

```
nano /etc/hosts
```

```
127.0.0.1 localhost

192.168.1.2 web.example.tld
192.168.1.3 mail.example.tld
192.168.1.4 ns1.example.tld
192.168.1.5 ns2.example.tld

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

Tragen Sie den Hostnamen des Servers ein:

```
echo ns1.example.tld > /etc/hostname
/etc/init.d/hostname.sh start
```

Installieren Sie den MySQL Client und Server:

```
apt-get -y install mysql-client mysql-server
```

Geben Sie das neue Passwort für MySQL ein, sobald Sie der Installer dazu auffordert.

Installieren Sie dann die Kommandozeilenversion von PHP um PHP-basierte Skripts für ISPConfig ausführen zu können:

```
apt-get -y install php5-cli php5-mysql php5-mcrypt mcrypt
```

Installation von fail2ban: diese ist optional, wird aber empfohlen, da der ISPConfig Monitor dessen Log anzuzeigen versucht:

```
apt-get install fail2ban
```

Installation des BIND DNS Servers:

```
apt-get -y install bind9 dnsutils
```

Nun installieren Sie ISPConfig 3 auf dem Server. Für den Downloadlink der aktuellen stabilen ISPConfig 3 Version, besuchen Sie bitte die ISPConfig Webseite: http://www.ispconfig.org/ispconfig-3/download/

Laden Sie die aktuelle stabile ISPConfig 3 Version herunter:

```
cd /tmp
wget http://www.ispconfig.org/downloads/ISPConfig-3-stable.tar.gz
tar xfz ISPConfig-3-stable.tar.gz
cd ispconfig3_install/install/
```

Starten Sie dann das Installationsskript:

```
php -q install.php
```

Select language (en,de) [en]: **<-- en**

Installation mode (standard,expert) [standard]: **<-- expert**

Full qualified hostname (FQDN) of the server, eg server1.domain.tld [db.example.tld]: **<-- ns1.example.tld**

MySQL server hostname [localhost]: **<-- localhost**

MySQL root username [root]: **<-- root**

MySQL root password []: **<-- Geben Sie hier Ihr MySQL root Passwort an**

MySQL database to create [dbispconfig]: **<-- dbispconfig**

MySQL charset [utf8]: **<-- utf8**

Shall this server join an existing ISPConfig multiserver setup (y,n) [n]: **<-- y**

MySQL master server hostname []: **<-- web.example.tld**

MySQL master server root username [root]: **<-- root**

MySQL master server root password []: **<-- Geben Sie hier das root Passwort des Master Servers an**

MySQL master server database name [dbispconfig]: **<-- dbispconfig**

Configure Mail (y,n) [y]: **<-- n**

Configure Jailkit (y,n) [y]: **<-- n**

Configure FTP Server (y,n) [y]: **<-- n**

Configure DNS Server (y,n) [y]: **<-- n**

Configure Apache Server (y,n) [y]: **<-- n**

Configure Firewall Server (y,n) [y]: **<--y**

Install ISPConfig Web-Interface (y,n) [y]: **<--n**

Benutzen Sie...

```
rm -f /var/www/ispconfig
```

... um den ISPConfig Oberflächenlink im */var/www* Verzeichnis zu entfernen.

Räumen Sie anschließend im Installationsverzeichnis auf:

```
rm -rf /tmp/ispconfig3_install/install
rm -f /tmp/ISPConfig-3-stable.tar.gz
```

6.4 Installation des sekundären DNS Servers

Editieren Sie die hosts Datei und fügen Sie die IP Adressen und Hostnamen aller Server hinzu. Achten Sie dabei darauf, dass Sie sie mit denen Ihres Setups ersetzen:

```
nano /etc/hosts
```

```
127.0.0.1 localhost

192.168.1.2 web.example.tld
192.168.1.3 mail.example.tld
192.168.1.4 ns1.example.tld
```

```
192.168.1.5 ns2.example.tld

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

Tragen Sie den Hostnamen des Servers ein:

```
echo ns2.example.tld > /etc/hostname
/etc/init.d/hostname.sh start
```

Installieren Sie den MySQL Client und Server:

```
apt-get -y install mysql-client mysql-server
```

Geben Sie, sobald Sie vom Installer dazu aufgefordert werden, das neue MySQL Passwort ein.

Installieren Sie dann die Kommandozeilenversion von PHP um PHP-basierte Skripts für ISPConfig ausführen zu können:

```
apt-get -y install php5-cli php5-mysql php5-mcrypt mcrypt
```

Installation von fail2ban: Diese ist optional aber empfohlen, da der ISPConfig Monitor versucht, dessen Log anzuzeigen:

```
apt-get install fail2ban
```

Installieren Sie den BIND DNS Server:

```
apt-get -y install bind9 dnsutils
```

Nun installieren Sie ISPConfig 3 auf dem DNS Server. Für den Downloadlink der aktuellen stabilen ISPConfig 3 Version, besuchen Sie bitte die ISPConfig Webseite: http://www.ispconfig.org/ispconfig-3/download/
Laden Sie die aktuelle stabile ISPConfig 3 Version herunter:

```
cd /tmp
wget http://www.ispconfig.org/downloads/ISPConfig-3-stable.tar.gz
tar xfz ISPConfig-3-stable.tar.gz
cd ispconfig3_install/install/
```

Starten Sie dann das Installationsskript:

```
php -q install.php
```

```
Select language (en,de) [en]: <-- en
Installation mode (standard,expert) [standard]: <-- expert
Full qualified hostname (FQDN) of the server, eg server2.domain.tld [ns2.example.tld]: <-- ns2.example.tld
MySQL server hostname [localhost]: <-- localhost
MySQL root username [root]: <-- root
MySQL root password []: <-- Geben Sie hier Ihr MySQL root Passwort an
MySQL database to create [dbispconfig]: <-- dbispconfig
MySQL charset [utf8]: <-- utf8
Shall this server join an existing ISPConfig multiserver setup (y,n) [n]: <-- y
MySQL master server hostname []: <-- web.example.tld
MySQL master server root username [root]: <-- root
MySQL master server root password []: <-- Geben Sie hier das root Passwort des Master Servers an
MySQL master server database name [dbispconfig]: <-- dbispconfig
Configure Mail (y,n) [y]: <-- n
Configure Jailkit (y,n) [y]: <-- n
Configure FTP Server (y,n) [y]: <-- n
```

```
Configure DNS Server (y,n) [y]: <-- y
Configure Apache Server (y,n) [y]: <-- n
Configure Firewall Server (y,n) [y]: <--y
Install ISPConfig Web-Interface (y,n) [y]: <--n
```

Benutzen Sie...

```
rm -f /var/www/ispconfig
```

... um den ISPConfig Oberflächenlink im */var/www* Verzeichnis zu entfernen.

Räumen Sie anschließend im Installationsverzeichnis auf:

```
rm -rf /tmp/ispconfig3_install/install
rm -f /tmp/ISPConfig-3-stable.tar.gz
```

6.5 Anpassen der Servereinstellungen in ISPConfig

Melden Sie sich auf dem Master Server mit einem Internetbrowser in ISPConfig an:

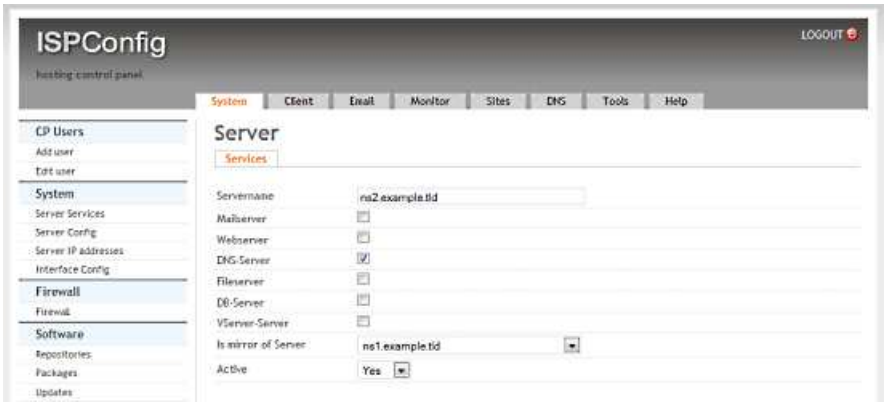
```
http://192.168.1.2:8080
```

Klicken Sie auf *System > Server Services > web.example.tld*, deaktivieren alle Kontrollkästchen außer den *Webserver*, *Fileserver* und *DB-Server* Kästchen und klicken auf *Speichern*.

Klicken Sie auf *System > Server Services > mail.example.tld*, deaktivieren alle Kontrollkästchen außer dem *Mailserver* Kästchen und klicken auf *Speichern*.

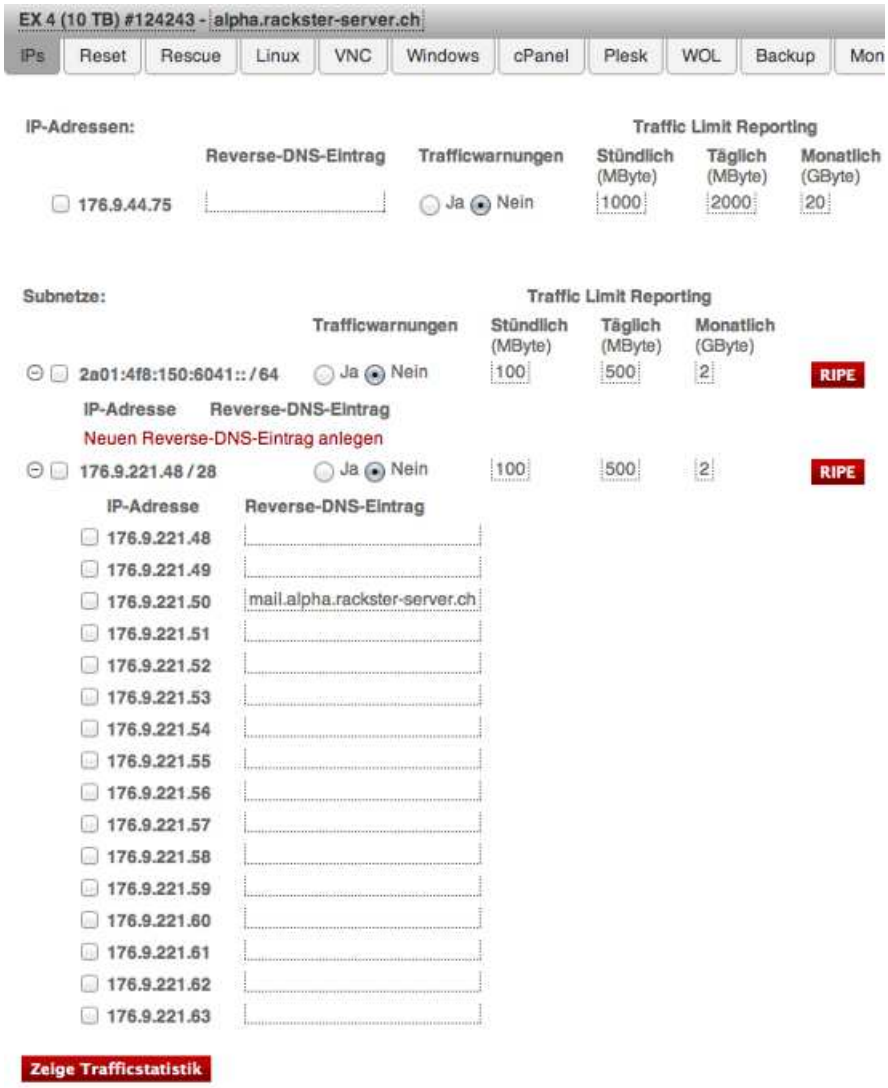
Klicken Sie auf *System > Server Services > ns1.example.tld* , deaktivieren alle Kontrollkästchen außer dem *DNS-Server* Kästchen und klicken auf *Speichern*.

Klicken Sie auf *System* > *Server Services* > *ns2.example.tld* , deaktivieren alle Kontrollkästchen außer dem *DNS-Server* Kästchen, wählen *ns1.example.com* in der *Ist Mirror von Server* Auswahlbox aus und klicken auf *Speichern*.



6.6 Reverse DNS einstellen

Da die meisten Mailserver auf einen gültigen Reverse DNS Eintrag überprüfen, müssen Sie einen für Ihren Mailserver erstellen. Hetzner erlaubt, dies in Ihrer Web-Oberfläche zu tun:



Beachten Sie den Eintrag für die IP 176.9.221.50. In unserem Fall müssen wir unter der IP *192.168.1.3* *mail.example.tld* eintragen.

7 Server erweitern

Sie sollten nun eine ohne Probleme laufende Umgebung aus einem dedizierten Server haben, auf welchem all Ihre virtuellen Server laufen. Es gibt jedoch noch eine Menge zusätzlicher Einstellungen, die Sie vornehmen können und sollten. Dies wird im folgenden getan werden - alle diese Einstellungen sind optional, es wird jedoch stark empfohlen, diese vorzunehmen.

Die ersten Schritte können auf allen Servern wiederholt werden.

7.0.1 SSH mit Authentifikationsschlüssel anstatt eines Passwortes

Das Benutzen von SSH Schlüsselauthentifikation ist sehr viel sicherer als ein Passwort, da Sie den privaten Schlüssel besitzen müssen um auf den Server zugreifen zu können. Haben Sie nicht schon einen, erstellen Sie ein RSA Schlüsselpaar (auf Ihrer lokalen Maschine):

```
ssh-keygen
```

```
Generating public/private rsa key pair.

Enter file in which to save the key (/home/username/.ssh/id_rsa): Enter passphrase (empty for no
passphrase):

Enter same passphrase again:

Your identification has been saved in /home/username/.ssh/id_rsa.

Your public key has been saved in /home/username/.ssh/id_rsa.pub.
```

Ist der öffentliche Schlüssel einmal auf dem Server installiert, wird der Zugriff ohne Passwortabfrage genehmigt. SSH bringt normalerweise ein Dienstprogramm namens ssh-copy-id mit, welches die Inhalte der *~/.ssh/id_rsa.pub* Datei des Clients zur *~/.ssh/authorized_keys* Datei des Servers hinzufügt:

```
ssh-copy-id -i .ssh/id_rsa.pub root@root.example.tld
```

Ab hier können Sie die Anmeldung des root Kontos per Passwort deaktivieren:

Probieren Sie bitte erst die Anmeldung mit Schlüssel aus, bevor Sie diesen Befehl ausführen!

```
passwd -l root
```

7.0.2 Installation von Logwatch

Logwatch ist ein kleines Paket, welches Ihnen detaillierte Breichte darüber sendet, was auf Ihrem Server passiert ist und zur Zeit passiert. Es ist sher nützlich zur Überwachung.

```
apt-get -y install logwatch
```

Konfigurieren Sie es nun

```
nano /usr/share/logwatch/default.conf/logwatch.conf
```

und setzen folgende Werte ein:

```
Output = mail

Format = text
MailTo = username@youremail.tld
Detail = High
Service = All
```

Sie werden nun jeden Tag eine E-Mail von Logwatch erhalten.

7.0.3 Zusätzliche fail2ban Regeln erlauben

Fail2ban ist großartig um den Zugriff ungewollter Benutzer auf Ihren Server zu blockieren. Da Sie es auf Ihrem Web/MySQL Server, wie auch auf Ihrem Mailserver bereits installiert haben, können Sie den ersten Schritt auf diesen überspringen. Führen Sie dies auf dem Node und beiden DNS Servern aus:

```
apt-get -y install fail2ban
```

Teilen Sie fail2ban nun mit, welche Dienste es überwachen soll und wie es falsche Anfragen behandeln soll:

Die folgenden Befehle müssen auf allen Servern ausgeführt werden (auch dem Web/MySQL Server und dem Mailserver):

```
nano /etc/fail2ban/jail.local
```

Fügen Sie der Datei folgendes hinzu (entfernen Sie keine der bestehenden Inhalte!):

```
[ssh]

enables = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 3

[ssh-ddos]

enabled = true
port = ssh
filter = sshd-ddos
logpath = /var/log/auth.log
maxretry = 5
```

Fail2ban wird nun SSH Einbruchsversuche aufspüren und versuchen, diese zu blocken. Starten Sie fail2ban danach neu:

```
/etc/init.d/fail2ban restart
```

7.1 Den Nodeserver erweitern

7.1.1 Installation von Ajenti

Ajenti ist ein nettes Server Kontrollpanel. Ich benutze es hauptsächlich zum verwalten der Firewall und wegen des eingebauten Filemanagers, der Konsole und dem Terminal.

Zuerst müssen Sie die Repository zur sources.list Datei hinzufügen. Öffnen Sie

```
nano /etc/apt/sources.list
```

und fügen Sie folgende Zeile hinzu:

```
deb http://repo.ajenti.org/debian main main
```

Danach müssen Sie den Schlüssel importieren:

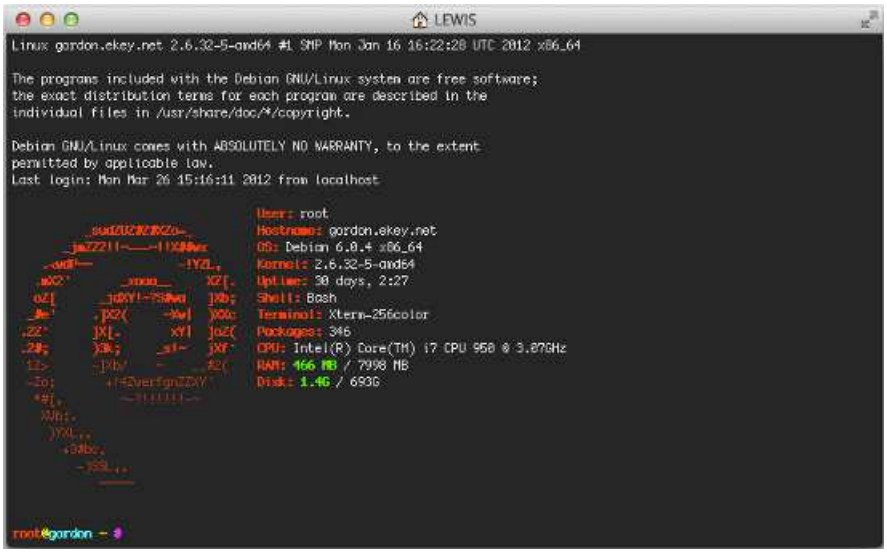
```
wget http://repo.ajenti.org/debian/key -O- | sudo apt-key add -
```

Sie sollten das Kontrollpanel nun unter *http://192.168.1.1:8000* erreichen können. Der Standardbenutzername und das Standardpasswort sind: *admin*
Haben Sie vor, das eingebaut Terminal zu verwenden, müssen Sie das Python PIL Modul installieren:

```
apt-get -y install python-imaging
```

7.1.2 Installation von Archey

Diese ist optional. Archey wird Ihnen bei der Anmeldung einige nette Informationen anzeigen.



Führen Sie zur Installation folgendes aus:

```
apt-get install lsb-release scrot
cd /tmp
wget https://github.com/downloads/djmelik/archey/archey-0.2.8.deb
dpkg -i archey-0.2.8.deb
rm archey-0.2.8.deb
nano /etc/bash.bashrc
```

Fügen Sie am Ende der Datei *archey* hinzu.

7.2 Den Web/DB Server erweitern

Die folgenden Schritte werden nur auf dem Web/DB Server ausgeführt.

7.2.1 Installation von cURL

```
apt-get -y install curl php5-curl libcurl3-dev
```

7.2.2 Installation des ionCube Loader

Dies sollten Sie nun alleine hinbekommen. Laden Sie einfach die korrekte Version unter http://www.ioncube.com/loaders.php herunter und folgen Sie den Anleitungen.

7.2.3 Installation von APC und anderen nützlichen Anwendungen

In dieser Sektion werden Sie APC installieren (PHP Beschleuniger), welcher von den selben Leuten entwickelt wird wie PHP und einige andere Anwendungen (htop, iptraf, logwatch, tiger).

```
apt-get -y install php-apc htop iptraf tiger
```

Editieren Sie */etc/php5/conf.d/apc.ini* um den Memory Cache zu erhöhen:

```
nano /etc/php5/conf.d/apc.ini
```

Fügen Sie folgende Zeile hinzu:

```
apc.shm_size=128
```

Starten Sie Apache neu:

```
/etc/init.d/apache2 restart
```

Mit htop werden Ihnen Systeminformationen besser angezeigt als mit top, mit iptraf können Sie real-time Statistiken Ihrer Verbindung einsehen und mit tiger können Sie sich periodisch Mails schicken lassen, welche Berichte über Sicherheitslücken in Ihrem System enthalten (falls es welche gibt).

Da eine Vielzahl von Skripten/Anwendungen Mails an den root Benutzer schickt, können Sie für roots E-Mail Adresse ein Alias auf eine 'echte' E-Mail Adresse erstellen. Nachdem Sie eine 'echte' Mail Adresse für Ihre example.tld Domain aufgesetzt haben können Sie die Aliasse bearbeiten eins zu root hinzufügen:

```
nano /etc/aliases
```

Ändern Sie die Zeile

```
root:root
```

in etwas wie

```
root:username@example.tld
```

Führen Sie danach folgendes aus:

```
newaliases
```

Wollen Sie Drupal (oder andere CMS) installieren, werden Sie wahrscheinlich uploadprogress und json benötigen. Um diese zu installieren, führen Sie folgendes aus:

```
apt-get -y install php5-dev php-services-json
pecl install uploadprogress
touch /etc/php5/apache2/conf.d/uploadprogress.ini
nano /etc/php5/apache2/conf.d/uploadprogress.ini
```

Fügen Sie hier folgende Zeile hinzu:

```
extension=uploadprogress.so
```

Starten Sie dann Apache neu:

```
/etc/init.d/apache2 restart
```

7.2.4 Installation von mod_security

Installieren Sie das Apache mod-security 2 Module mit apt aus den Debian Repositories:

```
apt-get -y install libapache-mod-security
```

Erstellen Sie das Verzeichnis für die mod-security Konfigurationsdateien:

```
mkdir /etc/apache2/mod-security
chmod 600 /etc/apache2/mod-security
```

Laden Sie die mod-security Regeln herunter und entpacken Sie:

```
cd /tmp
wget http://www.modsecurity.org/download/modsecurity core-rules_2.5-1.6.1.tar.gz
tar fvx modsecurity-core-rules_2.5-1.6.1.tar.gz
mv *.conf /etc/apache2/mod-security/
ln -s /var/log/apache2 /etc/apache2/logs
```

Konfigurieren Sie Apache dazu, die aktivierten mod-security Regeln zu laden:

```
nano /etc/apache2/conf.d/mod-security.conf
```

```
Include /etc/apache2/mod-security/*.conf
```

Um mod-security zu aktivieren, editieren Sie die Datei

```
nano /etc/apache2/mod-security/modsecurity_crs_10_config.conf
```

and entfernen Sie die Raute (#) vor der folgenden Zeile:

```
SecDefaultAction "phase:2,log,deny,status:403,t:lowercase,t:replaceNulls,t:compressWhitespace"
```

Laden Sie dann Apache neu.

```
/etc/init.d/apache2 force-reload
```

Mod security wird Hackversuche auf Ihre Webseite nun blocken und in der Datei */var/log/apache2/modsec_audit.log* protokollieren.

```
tail /var/log/apache2/modsec_audit.log
```

Sie werden sehr wahrscheinlich einige fälschlicherweise geblockte URLs vorfinden. Um diese zu whitelisten, tragen Sie die IDs der Regeln, die nicht benutzt werden sollen, in die Whitelist Datei ein.

Beispiel:

```
nano /etc/apache2/mod-security/modsecurity_crs_99_whitelist.conf
```

```
SecRuleRemoveById 960015

SecRuleRemoveById 960016
```

7.2.5 MySQL Tuning

Laden Sie *tuning-primer.sh* und *mysqltuner.pl* herunter. Diese werden Ihnen helfen MySQLs Konfigurationsdatei zu verbessern.

```
cd /root/scripts
wget http://www.day32.com/MySQL/tuning-primer.sh
wget http://mysqltuner.com/mysqltuner.pl
chmod 700 tuning-primer.sh mysqltuner.pl
```

Um sie auszuführen benutzen Sie:

```
perl /root/scripts/mysqltuner.pl
/root/scripts/tuning-primer.sh
```

Die Skripte werden einige einfache Fragen stellen (Benutzer/Passwort) und Ihre Vorschläge für kritische Einstellungen in rot darstellen. Sie können diese Vorschläge benutzen um die Performanz Ihres MySQL Servers zu verbessern.

7.2.6 Installation von RoundCube

Sie können Roundcube ganz normal über apt-get installieren. Sie können es jedoch auch manuell in seine eigene Subdomain installieren wenn sie möchten (falls Sie die Zeit und den Mut haben).

In den "Perfect Server ...." Tutorials wird normalerweise SquirrelMail installiert. Möchten Sie dieses nicht benutzen, können Sie es so deinstallieren:

```
apt-get remove squirrelmail
rm /etc/apache2/conf.d/squirrelmail.conf
```

Nun installieren Sie Roundcube. (Sie **MÜSSEN** das MySQL Administratorpasswort kennen bevor Sie fortfahren -- Lassen Sie dbconfig-common die Datenbank konfigurieren. Sie werden einige Fragen betreffend des Passwortes des Datenbankadministrators und des Passwortes des neuen Benutzers gefragt, der für Roundcube angelegt wird. Beantworten Sie diese Fragen und fahren Sie fort:

```
apt-get -y install roundcube roundcube-mysql
```

Beispielantworten:

"Configure database for roundcube with dbconfig-common?" .... Antwort **Yes**
"Database type to be used by roundcube:" ...Antwort **mysql**
"Password of the database's administrative user:" ... Antwort **Passwort des Datenbankadministrators**
"MySQL application password for roundcube:" ... Antwort **das Passwort des Roundcube-Benutzers**
"Password confirmation:"... Antwort **das Passwort des Roundcube-Benutzers (Bestätigung)**
Läuft etwas schief, können Sie immernoch folgenden Befehl benutzen:

```
dpkg-reconfigure roundcube-core
```

Sehen Sie sich für mehr Informationen diesen Post an.

Damit jeder auf sein Webmail zugreifen kann (unter seinem Domainnamen) müssen Sie die Datei */etc/apache2/conf.d/roundcube* editieren und ein Alias nach 'webmail' anlegen. Wollen Sie SSL benutzen, sollten Sie die letzen beiden Direktiven (IfModule mod_rewrite.c) einfügen, damit Apache IMMER zu Ihrer SSL Installation von ISPConfig umleitet.

```
nano /etc/apache2/conf.d/roundcube
```

```
# Those aliases do not work properly with several hosts on your apache server

# Uncomment them to use it or adapt them to your configuration
# Alias /roundcube/program/js/tiny_mce/ /usr/share/tinymce/www/
Alias /roundcube /var/lib/roundcube
Alias /webmail /var/lib/roundcube

# Access to tinymce files
<Directory "/usr/share/tinymce/www/">
Options Indexes MultiViews FollowSymLinks
AllowOverride None
Order allow,deny
allow from all
</Directory>

<Directory /var/lib/roundcube/>
Options +FollowSymLinks
# This is needed to parse /var/lib/roundcube/.htaccess. See its
# content before setting AllowOverride to None.
AllowOverride All
order allow,deny
allow from all
</Directory>

# Protecting basic directories:
```

```
<Directory /var/lib/roundcube/config>
Options -FollowSymLinks
AllowOverride None
</Directory>

<Directory /var/lib/roundcube/temp>
Options -FollowSymLinks
AllowOverride None
Order allow,deny
Deny from all
</Directory>

<Directory /var/lib/roundcube/logs>
Options -FollowSymLinks
AllowOverride None
Order allow,deny
Deny from all
</Directory>

<IfModule mod_rewrite.c>
<IfModule mod_ssl.c>
<Location /webmail>
RewriteEngine on
RewriteCond %{HTTPS} !^on$ [NC]
RewriteRule . https://%{HTTP_HOST}:50443%{REQUEST_URI} [L]
</Location>
</IfModule>
</IfModule>

<IfModule mod_rewrite.c>
<IfModule mod_ssl.c>
<Location /roundcube>
RewriteEngine on
RewriteCond %{HTTPS} !^on$ [NC]
RewriteRule . https://%{HTTP_HOST}:50443%{REQUEST_URI} [L]
</Location>
</IfModule>
</IfModule>
```

Editieren Sie */var/lib/roundcube/config/main.inc.php*:

```
nano /var/lib/roundcube/config/main.inc.php
```

and setzen Sie einige Variablen in der Datei (ist dies das erste Mal, dass Sie die Datei bearbeiten, sollten sie in den Zeilen 60 und 66 zu finden sein):

```
auto_create_user = TRUE;

$rcmail_config['default_host'] = 'mail.example.tld';
```

Werden Sie das folgende Plugin installieren (der Logger, der fail2ban hilft), müssen Sie die Liste der Plugins in der selben Datei erweitern. Ist das einzige Plugin jenes, das gleich installiert werden wird, müssen Sie Zeile 42 folgendermaßen editieren:

```
$rcmail_config['plugins'] = array('fail2ban');
```

Installieren Sie das Roundcube Logger Plugin von http://mattrude.com/projects/roundcube-fail2ban-plugin/.

Sie müssen die Datei nur herunterladen (fail2ban.php) und sie in den fail2ban Ordner im Plugins Ordner von Roundcube kopieren. Dies sollte der finale Pfad sein: */usr/share/roundcube/plugins/fail2ban/fail2ban.php*. Führen Sie nun folgendes aus:

```
cd /usr/share/roundcube/plugins/
wget --no-check-certificate http://cloud.github.com/downloads/mattrude/rc-plugin-fail2ban/roundcube-
fail2ban-plugin.1.1.tgz
tar -xvzf roundcube-fail2ban-plugin.1.1.tgz
touch /var/log/roundcube/userlogins
rm roundcube-fail2ban-plugin.1.1.tgz
chown www-data:www-data /var/log/roundcube/userlogins
```

Dieses Plugin wird die Logdatei nach jedem fehlgeschlagenen Login-Versuch aktualisieren: */var/log/roundcube/userlogins*
Vergessen Sie nicht, den Webmail Link in ISPConfig zu editieren (*System -> Interface Config -> (tab) Mail*) und ihn auf */webmail* zu setzen. Starten Sie dann Apache neu.

```
/etc/init.d/apache2 restart
```

Sie können Webmail nun unter *http://web.example.tld/webmail* erreichen.

7.2.7 Installation von fail2ban

Erweitern Sie die *jail.local* Datei, die Falko in The Perfect Server - Debian Squeeze (Debian 6.0) With BIND & Courier [ISPConfig 3] vorschlägt: */etc/fail2ban/jail.local*

```
nano /etc/fail2ban/jail.local
```

Folgendes müssen Sie anhängen oder editieren:

```
[roundcube]

enabled = true
port = http
filter = roundcube
logpath = /var/log/roundcube/userlogins
maxretry = 5
```

Vergessen Sie nicht zum Schluss die roundcube.conf Datei */etc/fail2ban/filter.d/roundcube.conf* anzulegen (sehr wichtig).

```
nano /etc/fail2ban/filter.d/roundcube.conf
```

Diese brauch den folgenden Inhalt:

```
[Definition]

failregex = FAILED login for .*. from <HOST>
ignoreregex =
```

Starten Sie fail2ban neu:

```
/etc/init.d/fail2ban restart
```

Werden viele Jails in fail2ban hinzugefügt, kann es passieren, dass einige von ihnen nicht starten (Fehler in */var/log/fail2ban.log*, nicht aber in der Ausgabe !!!). Sehen Sie es sich folgendermaßen selbst an:

```
iptables -L -n
```

Leider kommt die Lösung einem Hack nahe... aber es ist eine Lösung:

In der Datei */usr/bin/fail2ban-client* müssen Sie in Zeile 145 *time.sleep(0.1)* oder *time.sleep(0.05)* einfügen:

```
nano /usr/bin/fail2ban-client
```

Vor der Änderung sieht die Datei also so aus:

```
[...]

def __processCmd(self, cmd, showRet = True):
beautifier = Beautifier()
for c in cmd:
beautifier.setInputCmd(c)
try:
[...]
```

Und danach so:

```
[...]

def __processCmd(self, cmd, showRet = True):
beautifier = Beautifier()
```

```
for c in cmd:
time.sleep(0.05)
beautifier.setInputCmd(c)
try:
[...]
```

Starten Sie fail2ban neu:

```
/etc/init.d/fail2ban restart
```

Ob alle Jails aktiv sind können Sie mit folgendem Befehl überprüfen:

```
iptables -L -n
```

7.2.8 Installation von mod_evasive mit fail2ban Unterstützung

mod_evasive ist ein Apache Modul zur Handhabung von DDoS Angriffen. Installieren Sie dieses und konfigurieren Sie fail2ban dazu, automatisch gemeldete Angriffe zu bannen/entbannen.

```
apt-get install libapache2-mod-evasive
mkdir /var/lock/mod-evasive
chown www-data /var/lock/mod-evasive
ln -s /etc/alternatives/mail /bin/mail
nano /etc/apache2/mods-available/mod-evasive.conf
```

Fügen Sie folgendes ein:

```
<IfModule mod_evasive20.c>

DOSHashTableSize 3097
DOSPageCount 3
DOSSiteCount 60
DOSPageInterval 1
DOSSiteInterval 2
DOSBlockingPeriod 15
DOSEmailNotify username@example.tld
DOSLogDir "/var/lock/mod_evasive"
</IfModule>
```

Aktivieren Sie im Anschluss das Modul und starten Apache neu

```
a2enmod mod-evasive
/etc/init.d/apache2 restart
```

mod_evasive wird nun DDoS Angriffe erkennen. Um sie mit IPTables zu bannen, erstellen Sie diese Datei: */etc/fail2ban/filter.d/apache-dosevasive.conf*:

```
# Fail2Ban configuration file

#
# Author: Xela
#
# $Revision: 728 $
#

[Definition]

# Option: failregex
# Notes.: regex to match the Forbidden log entrys in apache error.log
# maybe (but not only) provided by mod_evasive
#
# Values: TEXT
#
failregex = ^[[^]]*]s+[error]s+[client ] client denied by server configuration:s

# Option: ignoreregex
# Notes.: regex to ignore. If this regex matches, the line is ignored.
# Values: TEXT
```

```
#
ignoreregex =
```

Fügen Sie danach folgendes zur */etc/fail2ban/jail.local* Datei hinzu:

```
[apache-dosevasive]


enabled = true
filter = apache-dosevasive
action = iptables-allports[name=dos]
logpath = /var/log/apache*/*error.log
bantime = 600
maxretry = 10
```

7.3 Erweitern des Mailservers

7.3.1 Verbesserter E-Mail Spamschutz

Der nachfolgende Befehl erlaubt bei Postfix strengere Maßnahmen gegen Spam auf ISPConfig 3 Servern.

```
postconf -e 'smtpd_recipient_restrictions = permit_mynetworks, permit_sasl_authenticated,
reject_invalid_hostname, reject_non_fqdn_hostname, reject_unknown_recipient_domain,
reject_non_fqdn_recipient, reject_unauth_destination, reject_non_fqdn_sender,
reject_unknown_sender_domain, reject_unknown_recipient_domain, reject_rbl_client
cbl.abuseat.org,reject_rbl_client dul.dnsbl.sorbs.net,reject_rbl_client ix.dnsbl.manitu.net,
check_recipient_access mysql:/etc/postfix/mysql-virtual_recipient.cf, reject_unauth_destination'
```

Starten Sie danach Postfix neu:

```
/etc/init.d/postfix restart
```

7.3.2 Installation von Postgrey

Postgrey eliminiert 99% aller Spammails, die Sie bekommen. Benutzen Sie zur Installation

```
apt-get install postgrey
/etc/init.d/postgrey start
```

Die Postfix Konfigurationsdateien finden Sie unter */etc/postfix*. Editieren Sie */etc/postfix/main.cf* and fügen Sie *check_policy_service inet:127.0.0.1:60000* zu smtpd_recipient_restrictions hinzu.

Laden Sie dann die Konfiguration neu:

```
postfix reload
```

7.4 Sicherung der Server durch SSL

Zu Ihrer Sicherheit sollten Sie folgendes Tutorial befolgen: http://www.howtoforge.com/securing-your-ispconfig-3-installation-with-a-free-class1-ssl-certificate-from-startssl. Führen Sie die Befehle auf dem richtigen Server aus!

8 Instand halten der Server

Führen Sie diese Befehle regelmäßig aus um sie auf aktuellem Stand zu halten:

```
apt-get update && apt-get -y upgrade && apt-get -y dist-upgrade
```

9 Links/Credits/Quellen

Da das meiste nicht von mir ist, hier die Quellen, die ich für das Tutorial verwendet habe:
http://www.faqforge.com/linux/enhanced-e-mail-spam-protection-in-ispconfig-3/
http://www.howtoforge.com/greylisting_postfix_postgrey
http://www.howtoforge.com/extending-perfect-server-debian-squeeze-ispconfig-3-p4

http://spielwiese.la-evento.com/xelasblog/archives/56-Apache-DOS-Attacken-erschweren-mit-mod_evasive.html
http://www.faqforge.com/linux/apache-mod-security-installation-on-debian-6-0-squeeze/
http://forum.whmcs.com/showpost.php?s=f876c3e3a7d56bd2f325685a80d746cf&p=16768&postcount=4
http://www.howtoforge.com/extending-perfect-server-debian-squeeze-ispconfig-3-p3
http://debian.nimmervoll.eu/tag/debian-logwatch-einrichten/
http://www.debian-administration.org/articles/530
http://www.howtoforge.com/securing-your-ispconfig-3-installation-with-a-free-class1-ssl-certificate-from-startssl
http://www.howtoforge.com/multiserver-setup-with-dedicated-web-email-dns-and-mysql-database-servers-on-debian-squeeze-with-ispconfig-3
http://debian.nimmervoll.eu/archey-debian-installation/
http://ajenti.org/
http://code.google.com/p/ovz-web-panel/wiki/Installation
http://www.howtoforge.com/installing-and-using-openvz-on-debian-squeeze-amd64

1 Kommentar(e)

Zum Posten von Kommentaren bitte anmelden oder registrieren.

Kommentare

Von: Arraken
Hallo!

Kleiner Hinweis, der auch beim englischen Tutorial gemacht wurde:

In /etc/vz/vz.conf ist ein Fehler :
IPTABLES=".....iptable__mangle.....

muss sein

IPTABLES="....iptable_mangle...

Tutorial Info

Autor: CSch
Tags: linux, apache, server management, debian, howtos & tutorials, virtual, multiserver, server, virtuelle, ispconfig 3, debian squeeze

Diese Seite empfehlen

Twittern