Tipps und Tricks

In diesem Bereich des Wikis werden sporadisch Kurzanleitungen, Workarounds usw. zu verschiedenen Themenbereichen auftauchen.

Rettungsumgebung (Chroot)

Wie ich selbst leidvoll erkennen musste, taugt die openSUSE Rettungsumgebung nicht dazu eine vollständige „Chroot“ Umgebung aufzubauen um an einem nicht mehr startenden System zu arbeiten. Daher hier eine kurze Anleitung zur Realisation einer Chroot-Umgebung für openSUSE.

Schritt 1 ist statt des Rettungssystems ein openSUSE-Live-System zu starten.

Danach können Schritt für Schritt alle Teilverzeichnissysteme zu einer vollständigen Umgebungzusammen gesetzt werden. Im Folgenden wird dies basierend auf unserer Partitionierungsempfehlung mit Software-RAID und LVM vorgenommen:

```
linux:~ # mount /dev/system/root /mnt
linux:~ # mount /dev/system/var /mnt/var
linux:~ # mount /dev/mdXXX /mnt/boot
```

mdXXX steht für das Software-RAID Device auf dem das /boot-Verzeichnis liegt. Leider nummeriert die Live-Umgebung SW-RAID Devices anders durch, als das installierte System. Kann also sein, das aus /dev/md0 im realen System /dev/md127 in der Live-Umgebung wird. Einfach ausprobieren.

Dann müssen noch die speziellen Verzeichnisse hinzugefügt werden:

```
linux:~ # mount -t proc none /mnt/proc
linux:~ # mount -t sysfs non /mnt/sys
linux:~ # mount -o bind /dev /mnt/dev
```

(Genau der Teil funktioniert mit dem einfachen Rettungssystem nicht!)

Damit ist die Chroot-Umgebung fertig und kann betreten werden:

```
linux:~ # chroot /mnt
```

Jetzt kann im installierten System gearbeitet werden. Sie können hier beispielsweise Grub reparieren oder eine neue inird erzeugen.

Verlassen wird es einfach mit ***exit***

Nein Danke Zensursula

Hinweis: *Der folgende Text ist nicht ganz neutral geschrieben. Er enthält persönliche Meinungsäußerungen. Ich bitte dies zu entschuldigen.*

2010 trat das Web-Sperren-Gesetz gegen die Verbreitung von Kinderpornographie in Kraft. Dieses Gesetz ging, trotz des sicherlich aufrichtigen Ansatzes, am Thema vorbei und ermöglichte es allenfalls eine Zensurinfrastruktur nebst dazu passenden Überwachungsmöglichkeiten im Internet zu etablieren. Auch wenn das Gesetzt bereits ein Jahr später wieder aufgehoben wurde, zeigen wir hier eine Möglichkeit auf, es zu umgehen. Dass solch simple Wege die Umgehung DNS-basierter Web-Sperren ermöglichen, zeigt eigentlich auch die Sinnlosigkeit solcher Techniken.

Auch wenn es nicht um die Umgehung von Websperren geht, ist es eine kluge Entscheidung vertrauenswürdige DNS-Server zu nützen. Ein frei zugänglicher DNS-Server wie etwa der von Google angebotene „8.8.8.8“ ist sicherlich auch nicht der Weisheit letzter Schluss. Hier bietet ein Mega-Konzern, dessen Kerngeschäft die gewinnbringende Nutzung von Informationen ist, einen kostenfreien Dienst an. Dass dies nicht einfach dem Wohle der Menschheit dient liegt nahe. Schließlich lassen sich mit der Auswertung von DNS-Daten Unmengen spannende Daten der Nutzer gewinnen.

Wer einen invis-Server im eigenen Netz betreibt und sich (zumindest vorerst) sicher sein möchte, dass seine Nameserver-Abfragen nicht von „manipulierten“ oder „schnüffelnden“ Nameservern beantwortet werden, kann dies (wenn nicht bereits im Verlauf der Server-Installation geschehen) durch Ändern der „forwarders“ in der Konfiguration des lokalen Nameservers „bind“ umgehen.

Ändern Sie einfach in der Datei „/etc/named.conf“ die Einträge hinter „forwarders“:

```
        # The forwarders record contains a list of servers to which queries
        # should be forwarded.  Enable this line and modify the IP address
to
        # your provider's name server.  Up to three servers may be listed.
        # Die folgende Zeile ist um die IP-Adresse des fuer Sie zustaendigen
DNS
        # zu erweitern.

        forwarders { 194.25.2.129; 192.168.178.1; };

        # Enable the next entry to prefer usage of the name server declared
in
        # the forwarders section.

        forward first;
```

Tragen Sie statt des T-Online Nameservers und etwa dem einer Fritzbox (wie hier gezeigt) frei nutzbare **vertrauenswürdige** DNS-Server als Forwarder ein. Zu empfehlen sind hier die DNS-Server von Cloudflare (1.1.1.1) und Quad9 (9.9.9.9). Alternativ können Sie auch Nameserver aus der unter http://www.ungefiltert-surfen.de zu findenden Liste verwenden. Starten Sie anschließend ***bind*** mit:

```
invis:~ # systemctl restart named.service
```

neu.

Speicherüberlauf Cyrus Index-DB

Cyrus IMAP speichert die den Mailboxen zugehörigen Index-Datenbanken unter /var/lib/imap im Berkeley-DB (sleepycat) Format ab. Die für dieses Format übliche Konfigurationsdatei „DB_CONFIG“ fehlt im Verzeichnis /var/lib/imap/db. Das bedeutet, dass die Datenbank mit Standardwerten betrieben wird. Es kann vorkommen, das der per Default vorgegebene für die Datenbanken zur Verfügung stehende maximale Speicherplatz überschritten wird. Die Folge ist, dass Cyrus die weitere Annahme in die von ihm verwalteten Postfächer verweigert.

Dieser Fehler äußert sich in /var/log/messages mit folgenden Zeilen:

```
Feb 21 11:01:47 invis5bio lmtpunix[1802]: DBERROR db4: Logging region out of
memory; you may need to increase its size
Feb 21 11:01:47 invis5bio lmtpunix[1802]: DBERROR: opening
/var/lib/imap/deliver.db: Cannot allocate memory
Feb 21 11:01:47 invis5bio lmtpunix[1802]: DBERROR: opening
/var/lib/imap/deliver.db: cyrusdb error
Feb 21 11:01:47 invis5bio lmtpunix[1802]: FATAL: lmtpd: unable to init
duplicate delivery database
Feb 21 11:01:47 invis5bio master[17315]: service lmtpunix pid 1802 in READY
state: terminated abnormally
```

Behoben werden kann dieser Fehler durch erzeugen einer Konfigurationsdatei für die Berkeley-DB unter dem Namen „DB_CONFIG“ in /var/lib/imap/db:

```
set_cachesize 0 2097152 1

# Data Directory
#set_data_dir db

# Transaction Log settings
set_lg_regionmax 2097152
set_lg_bsize 2097152
set_lg_max 4194304
set_tx_max 200
set_tas_spins 1
#set_lg_dir logs
```

Daran anschließend ist Cyrus neuzustarten:

```
linux:~ #/etc/init.d/cyrus restart
```

Group-e -- Passwwort des Benutzers "config" zurück setzen

Das Passwort des Benutzers „config“ wird unabhängig von der generellen Benutzerverwaltung in Group-e immer in der MySQL-Datenbank verwaltet. Um es zurückzusetzen muss eine SQL-Anweisung über das MySQL-Komandozeilen Frontend abgesetzt werden:

```
linux:~ # mysql -u root -p

...
```

```
mysql> use groupe;
Database changed
mysql> UPDATE `ModulCfg` SET `CfgVal`=MD5( 'config' ) WHERE
`ModulCfg`.`FKModul`='global' AND `ModulCfg`.`FKCfgKey`='cfg/pwd' AND
`ModulCfg`.`FKObjID`=0;
Query OK, 1 row affected (0.01 sec)
Rows matched: 1  Changed: 1  Warnings: 0

mysql> quit
Bye
linux:~ #
```

Danach kann man sich wieder als Benutzer „config“ mit dem Passwort „config“ anmelden.

Faxgate-Client unter Linux nutzen

Um den Faxgate-Client unter Linux nutzen zu können sind ein paar Kleinigkeiten zu beachen:

1. Die Firewall des Linux-Clients muss Port 50000/TCP geöffnet haben.
2. Die „.jar“ Datei ist mittels der Befehlszeile „java -jar FaxgateClient.jar“ zu starten. Das lässt sich ja unter KDE oder Gnome als fertiges Icon auf den Desktop legen.
3. In der hosts-Datei von Client und Server sollten trotz funktionierendem DNS in Einträgen mit der IP „127.0.0.2“ stattdessen die realen IP-Adressen verwendet werden.
4. Da unter Linux nicht unter fremder Benutzerkennung gedruckt werden kann, muss für jeden Fax-Benutzer Serverseitig eine Fax-Konfiguration via YaST erzeugt werden. Wird dort die MSN für eingehende Faxe nicht eingetragen, kann dieser Eintrag nur für den Faxversand genutzt werden. Der Faxempfang kann so weiterhin über die Benutzerkennung „fax“ erfolgen. D.h. alle Faxe landen im speziellen Faxpostfach und sind für alle Nutzer lesbar.