Linux (allgemein): Der Rescue-/Recovery-Modus

Der Recovery-Modus (oder auch Rescue-Modus) den inzwischen fast jeder Server-Hoster anbieten, ist eine schöne Sache.
Wenn man sich damit auskennt... :)

Begriffserklärung

Da es manch einem nicht klar ist, hier kurz der Unterschied zwischen "Recovery-Modus", "serielle Konsole" und "VNC":

- Der Recovery-Mode ist ein von extern (Netzwerk, virtuelle Platte, USB-Stick) gebootetes Linux.
- Die Serielle-Konsole greift nur auf den Server über eine andere Schnittstelle zu. Ist ansonsten wie eine normale SSH-Verbindung.

  Das große Missverständnis: Hier befindet man im selben Linux-System. Es ist kein Recovery-Modus! Wenn das System an sich nicht mehr läuft, kann man auch auf der Seriellen-Konsole nichts mehr machen.
  Vorteil: Fehlermeldungen z.B. über defekte Hardware wird ggf. noch auf dieser Konsole sichtbar.
- Bei VNC wird der Monitor-Ausgang und der Tastatur/Maus-Eingang des Servers über unterschiedliche Techniken mit dem heimischen PC verbunden.

  Sehr verbreitet ist das System "LARA" als Hardware-Lösung. Per Software gibt es die Möglichkeit ein externes Linux mit VNC-Server zu booten. Dies ist insbesondere für eine Windows-Installation per Remote brauchbar.

  Auch dies ist *kein* Recovery-System!

Wofür ein Recovery?

Es gibt viele Vorteile eines extern gebootetem Betriebsystems. Je nach Server-Ausfall/-Crash kommen unterschiedliche Faktoren zusammen:

- Es bootet.
- Hardware-Tests: den Speicher (z.B. mit memtest86), Festplatten oder gar Stress-Test (z.B. mit `stress`).
- Die Festplatten sind i.d.R. nicht gemountet. (Ein `fsck` ist möglich.)

- Die Boot-Optionen können geändert werden. (Wenn er gerade mal nicht mehr bootet.)
- Oder sogar ein ganz anderes (vom Hoster nicht angebotenes) OS installieren.
- Ursachenforschung für den Absturz. (Die Logfiles werden nicht rotiert/fortgesetzt.)
- Datensicherung/Forensic nach einem Einbruch.

Häufig nutzt man das Recovery-System um einen `fsck` (Dateisystem-Check) über die ungemounteten Festplatten zu machen. Dies empfiehlt sich nach jedem Server-Absturz.

Arbeiten im Recovery-Mode

Bei den meisten Hostern kann der Recovery-Modus im Kunden-Login-Bereich gesetzt werden. Solange der Rechner noch läuft und erreichbar ist, sollte man den Reboot dann selber per SSH abschicken.
Wenn man diese Möglichkeit nicht mehr hat (z.B. totaler Absturz), gibt es den Button für den Hardware-Reset.

Je nach Hoster wird einem nun ein "einmal Passwort" oder ein ständiges Passwort für den Recovery-Modus angezeigt.
Der SSH-Login ist über die IP mit dem Benutzer `root` möglich.

Übliche Schritte im Recovery:

Die Festplatten-Partitionen ermitteln:

```
fdisk -l
```

(Achtung: Fehler in dieser Ausgabe brauchen nicht beachtet werden.)

Wir erhalten hier eine Liste mit allen erkannten Festplatten.
Bei Software-RAID werden sowohl die einzelnen Platten (`/dev/sda` und `/dev/sdb`) als auch das RAID-Device `/dev/md` aufgelistet.

Dateisystem-Check der Festplatte

Der `fsck` sollte immer nur über eine nicht gemountete Partition laufen!

```
fsck /dev/hda1
```

(Achtung: Wer ein Software-RAID hat sollte auf jedenfall immer das RAID-Device mounten!)

Bei Fehlern muss das Dateisystem repariert werden. Den Parameter `-r`fsck dann selber vor.

Mounten der Festplatte

```
mount /dev/md1 /mnt
```

(Achtung: Wer ein Software-RAID hat sollte auf jedenfall immer das RAID-Device mounten!)

Bei einigen Hostern ist von vornherein eine Partitionierung vorhanden. Dann könnte es so aussehen:

```
mkdir /mnt/root ; mkdir /mnt/var
mount /dev/sda1 /mnt/root
mount /dev/sda2 /mnt/var
```

Oder man bindet die var-Partition an der richtigen Stelle in der Root-Partition ein:

```
mount /dev/sda1 /mnt
mount /dev/sda2 /mnt/var
```

Bei Nutzung von LVM muss man natürlich die LVM-Partitionen mounten:

```
mount /dev/vg00/usr /mnt/usr
mount /dev/vg00/var /mnt/var
mount /dev/vg00/home /mnt/home
```

Danach kann auf die Festplatten über das gewählte Verzeichnis zugriffen werden.

Aber Vorsicht mit den üblichen, schnell getippten Befehlen:

`vim /etc/apache2/...` muss nun heißen `vim /mnt/etc/apache2/...`.

Oder `less /var/log/...` nun `less /mnt/var/log/...`.

Probleme mit Software-RAID

Wenn ein RAID-System vorhanden ist aber mit `fdisk -l` nicht angezeigt wird, muss erstmal das RAID-Modul in den Kernel geladen werden:

```
modprobe md
modprobe raid1
```

Falls `fdisk` immer noch keine RAID-Platte findet, kann man diese per Hand erstellen:

```
mdadm --assemble /dev/md0 /dev/sda1 /dev/sdb1
```

Achtung: Vorher sollte man sich wirklich klar darüber sein, ob man ein RAID hat oder nicht!!!

Auch die Art des RAIDs kann variieren: raid0 oder raid1

Ein Umgebungswechsel (`chroot`)

Eine Recovery-Funktionen muss man so ausführen, als wäre man im eigentlichen System.

Auch arbeitet sich für viele Admins etwas leichter mit den gewohnten Pfad angaben.

Dafür gibt es den `chroot`-Befehl. Vorher muss mind. die Root-Partition gemountet sein.
Bei verteilten Partitionen macht es Sinn die anderen in das root-System zu mounten.

Wer mehr braucht sollte vorher die System-Verzeichnisse ins neue root-System binden.

```
#Systemverzeichnisse binden:
mount -o bind /proc /mnt/proc
mount -o bind /dev /mnt/dev
mount -o bind /sys /mnt/sys

#nun der chroot
chroot /mnt
```

Damit teilt man Linux nun mit, dass es die gemountete Partition unter `/mnt` als Wurzelverzeichnis `/` nehmen soll.

Ab nun kann man wieder mit `less /var/log/...` arbeiten. Oder `lilo` sein Boot-Menü schreiben lassen, MySQL starten lassen um ein Backup zu ziehen, `rkhunter` laufen lassen, oder oder oder...

Den `chroot` beendet man mit dem Befehl: `exit`

Beenden des Recovery:

Dieser Punkt wird immer wieder auf die leichte Schulter genommen. Leider kann hierbei aber die gerade reparierte Partition zerstört werden.

- Falls ein `chroot` stattgefunden hat:

  Mit `exit` beenden.
- Alle gemounteten Partitionen unmounten.
- Im Kunden-Bereich das zu bootende System einstellen (ohne Reset).
- Den `reboot` möglichst noch im Recovery-System ausführen.

Eindeutige ID: #1379
huschi
2012-10-16 20:11