

22:28 Dirk Deimeke: ramon: Ich sehe gar nichts

22:28 Hans-Peter Bruegger: Ich auch nicht...

22:29 Ramon Kukla: Ihr macht nicht nervoes ;D

22:29 Dirk Deimeke: Sind wir bald da?

22:29 Hans-Peter Bruegger: ctrl+a, 0 ;o)

22:30 Ramon Kukla: Pft.

22:30 Hans-Peter Bruegger: Ich könnt's auch nicht mit Publikum. :oD

Bare Metal Restore

oder wie ich lernte das Backup zu lieben

Dirk Deimeke und Ramon Kukla

Ubucon 2010

16.10.2010



Inhalt

- 1 Vorstellung
- 2 Einführung
- 3 Vorüberlegung
- 4 Umsetzung
- 5 Die Katastrophe
- 6 Der Neuaufbau
- 7 Lessons learned

Dirk Deimeke

- Senior Unix Systems Administrator
bei der Credit Suisse in der Schweiz
(Best Global Bank laut Euromoney)
- Verheiratet, zwei Hunde
- Geboren in Wanne-Eickel
(Ruhrgebiet / Nordrhein-Westfalen / Deutschland)
- Wohnhaft im Grüt
(Zürcher Oberland / Kanton Zürich / Schweiz)
- 2008 in die Schweiz ausgewandert
- Bekennender »Alter Sack«
- Fühle mich als Weltbürger und Ruhrie
(Ja, auch als Netzbürger)
- Mehr unter <http://dirk.deimeke.net/>
Podcast <http://deimhart.net/>

Dirk Deimeke (Ubuntu)

- Vereinsvorsitzender ubuntu Deutschland e. V.
- Ansprechpartner für das deutsche LoCo-Team
- Ubuntu Member
- Organisationsteam der Ubucon
- ... mehr unter <http://d5e.org/ubuntu>

Ramon Kukla

- Intermediate/Senior Network/Security/System Administrator
bei der ROLAND Rechtsschutz-Versicherungs AG in Köln
- Verheiratet, 1.8 Kinder
- Geboren in Bonn / Nordrhein-Westfalen / Deutschland
- Wohnhaft in Niederkassel / Nordrhein-Westfalen
/ Deutschland
- <http://blog.portsonline.net>

Ramon Kukla (Ubuntu)

- Mitglied des ubuntu Deutschland e. V.
- Mitglied des deutschen LoCo-Team
- Organisationsteam der Ubucon
- Administrator für ubucon.de, ubuntu-de.org

ywc.ptlx.de - Hardware

- AMD Athlon(tm) 64 X2 Dual Core Processor 5600+
- 4 GB Ram
- 2 x 400 GB (Software-RAID 1)
- 7 offizielle IPv4-Adressen

ywc.ptlx.de - Infrastruktur

- Rettungssystem
 - Beheben von Dateisystemfehlern mit Rettungssystem möglich
 - Via installimage Neuinstallation aus dem Rettungssystem
- Backup
 - Im selben Rechenzentrum ein FTP-Server für Ablage von Backups
 - 100 GB Platz auf FTP-Server

ywc.ptlx.de - Hosting

- Drei Administratoren
- 20 DNS-Domains
- 44 Webseiten (grep ServerName sites-available/*)
- Reichlich Mailaccounts
- Jabber
- Trafficvolumen (in, out) 2009: 416 GB, 587 GB
- Trafficvolumen (in, out) 2010: 430 GB, 1127 GB

Einführung

Bin ich hier richtig?

- Das wird sich gleich zeigen ... :-)

Worum geht es?

- Wie bereite ich mich auf ein mögliches Disaster vor?
- Was tue ich wenn der schlimmste Fall eintritt (PANIK!)?
- Was tue ich um die Ausfallzeit kurz zu halten?

Worum geht es hier nicht?

- Schritt-für-Schritt Anleitung für ein Bare Metal Restore
- Konfiguration von Rechnern, Programmen oder Diensten

Fahrplan

- Vorüberlegungen
- Umsetzung
- Die Katastrophe
- Der Neuaufbau

Hinweis

- Die Session soll kein sturer Vortrag, sondern vielmehr ein Miteinander sein
- Bei Fragen bitte immer fragen!

Was gehört (nicht) in das Backup?

Das gehört rein

- Betriebssystem
- Programme
- Konfigurationsdateien (z.B. /etc/*)
- Server- und Anwendungsdaten (z.B. /var/www/, /srv/www/, /var/mail/, Datenbanken)
- ggf. Homelaufwerke

Das gehört nicht rein

- Temporäre Dateien und Ordner (/tmp/)
- *.bak-Dateien

Wie hilft Debian/Ubuntu

- Paket-Repositories
- System und Programme aus der gleichen Quelle

Ausfallzeit

Die mögliche (erträgliche) Ausfallzeit kann von verschiedenen Faktoren beeinflusst werden.

- Welche Ausfallzeit kann verkraftet werden?
- Wie bereite ich mich auf einen Ausfall vor?
- Entstehen mir Kosten beim Ausfall meiner Dienste?
- Entstehen Mitbenutzern Kosten beim Ausfall der Dienste?
- Kann ich ausgefallene Dienste vorübergehend mit Alternativen ersetzen?

Vorbereitung

Die Vorbereitung auf den Ernstfall ist in der Regel nie vollständig. Wichtige Punkte für den Notfall sind:

- Nutzt das angebotene und/oder ein eigenes Monitoring.
- Kontaktdaten des Hosters.
- Liste mit Kontaktdaten der Mitadministratoren.
- Liste mit alternativen Mailadressen der Benutzer.
- Notfalldokument, in dem alle wichtigen Informationen beschrieben sind.

Hinweis:

Das Notfalldokument bitte **nicht** auf dem selben Server ablegen, auf den die Beschreibung sich bezieht!

Was ist bei dem Backup zu beachten?

- Vollbackup oder nicht?
- Ein RAID oder Cluster ist kein Backup!
- Hab Zugriff auf das Kennwort/den Key wenn das Backup verschlüsselt ist!
- Das Backup nicht auf die selbe Maschine legen!
- Das Backup nicht im selben Raum vorhalten! (Feuer ...)

Backup des Systems

- `dpkg --get-selections`
- Weltweite Mirrors halten die Pakete vor

Backup beispielsweise von...

- Homeverzeichnissen
- Webseiten
- Mails
- Logs, ec.

hotcopy.bash

```
...
for i in $directories_to_copy
do
# vim backups entfernen
find $i -iname '*~' | xargs -r rm
filename=$target_directory/$(echo $i-$timestamp.tar.bz2 | \
sed "s/^\\\\\\\\g~;\\\\\\\\-\\\\\\\\g")
tar -cjf ${filename} ${i} -X /root/scripts/exclude.lst
done
...
```

Backup beispielsweise von...

■ subversion

hotcopy.bash

```
...
subversion_repositories="ywc_docsil_adminbuch_deimeke_deimhart_bruegger"
...
for i in $subversion_repositories
do
    filename=$target_directory/var-svn-$i-$timestamp.svn.bz2
    svnadmin dump /srv/svn/$i | bzip2 -9 > $filename
done
...
```

Backup beispielsweise von...

■ Datenbanken

hotcopy.bash

```
...
db_prefix="db_"
database_username="username"
database_password="password"
databases_to_copy=$(mysqlshow -u $database_username -p$database_password |\
awk '!/Databases|--/ {print $2}')
...
for i in $databases_to_copy
do
    filename=$target_directory/$db_prefix$i-$timestamp.sql.bz2
    mysqldump -c --databases --add-drop-database -u $database_username \
    -p $database_password $i | bzip2 -9 > $filename
done
...
```

Backup beispielsweise von...

■ Trac

hotcopy.bash

```
...
trac_wikis="ywc_edocsil_adminbuch_deimhart"
...
for i in $trac_wikis
do
    trac-admin /srv/trc/${i} hotcopy /bak/backup-md1/${i}-${timestamp}
    tar cjf /bak/backup-md1/${i}-${timestamp}.tar.gz /bak/backup-md1/${i}-${timestamp}
    rm -r /bak/backup-md1/${i}-${timestamp}
done
...
```

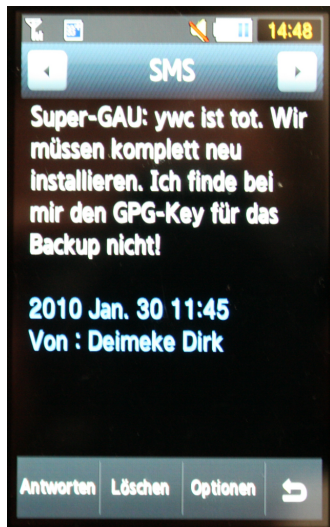
Abschliessend...

- Alte Backups löschen
- Backup PGP-verschlüsselt auf den FTP-Server kopieren

hotcopy.bash

```
...  
find $target_directory -mtime +6 | xargs rm  
/root/scripts/ftpbackup.bash >> /root/scripts/ftpbackup.log 2>&1  
...
```


Die Katastrophe



Wie ist es aufgefallen?

- Server war schon länger instabil
- Nach Absturz via Rettungssystem angemeldet
- Ewig viele Einträge in `/var/log/message` zu inode

Was ist zu beachten

- Erst einmal, ganz klar, **PANIK!**
- Zurück lehnen und durchatmen
- Mitadministratoren informieren
- Mitbenutzer informieren
- Weitere Vorgehensweise planen, bzw. Notfallpläne rausholen
- Via Chat-Tool Details koordinieren (wir nutzen <http://etherpad.org/etherpadsites.html>)
- screen für das "Vier-Augen-Prinzip", auch um die Verbindung mal unterbrechen zu können (Kopieraktion)
- Aufhören wenn es zu viel wird. Lieber ausruhen und später weiter machen

Erste Schritte nach dem GAU

- System im Rettungssystem gebootet
- RAID 1 mittels `mdadm --assemble /dev/md1` wieder hergestellt
- `fsck.ext3 -y /dev/md1`
- `mount /dev/md1 /mnt`
- Alle Daten finden sich im `/mnt/lost+found`, damit ist die Platte nicht mehr nutzbar
- Alle Daten von `lost+found` weggesichert für den Fall, dass wir im Backup etwas vergessen haben.
- Image von Provider aufspielen
- Hier zahlt es sich aus, Bekannte mit einem root-Server zu haben, um alles sichern zu können.

Der Neuaufbau

- Anwendungen nachinstallieren (`dpkg --set-selections`)
- `apt-get dselect-upgrade`
- Backup zurück kopieren

Die Rücksicherung

22:07 Dirk Deimeke: Alles in Screen

22:08 Dirk Deimeke: in Window 0 sehen wir aktuell eine Shell auf YWC

22:08 Ramon Kukla: Haha :D

22:08 Dirk Deimeke: in Window 1 läuft der Rsync des kompletten Backups

22:08 Ramon Kukla: Auf der linken Seite sehen Sie nun den Big Ben. Auf der rechten Seite den Versuch ywc. wieder zu beleben :D

22:08 Dirk Deimeke: Und hinter Tor 2 findet sich die Rücksicherung der nötigen Backups

Die Rücksicherung

- Backup Schritt für Schritt wieder einspielen
- Einen Dienst nach dem anderen wieder in Gang bringen
- Nicht verzetteln!

Probleme

23:13 Dirk Deimeke: Schei**e, jetzt habe ich Mist gebaut

23:14 Ramon Kukla: Ich schei**e mir jetzt nicht in die Hose o lange ich nicht weiss was es ist.

23:14 Ramon Kukla: :)

23:14 Hans-Peter Bruegger: Auch ich bleibe ganz ruhig

23:14 Dirk Deimeke: Ich habe das root-Passwort kaputt gemacht, aber ich komme ohne Passwort rein

Probleme

- UIDs stimmten nach der Installation nicht mehr
 - Neu setzen mit chown
- Postfix: warning mail queue enter: create file maildrop
Permission denied

```
ports@ywc:~$ /etc/init.d/postfix stop
ports@ywc:~$ killall -9 postdrop
ports@ywc:~$ chgrp -R postdrop /var/spool/postfix/public
ports@ywc:~$ chgrp -R postdrop /var/spool/postfix/maildrop/
ports@ywc:~$ postfix check
ports@ywc:~$ postfix reload
```

Nachbearbeitung - Lessons learned

13:54 Ramon Kukla: Ich fahre dann mal die IPs wieder hoch, ja?

13:54 Dirk Deimeke: stop

13:54 Ramon Kukla: Immer wenn es geil wird sagt Dirk 'Stop'.

Nachbearbeitung - Lessons learned

- Backup auch auf Partnerserver legen
- Backup aufräumen (srv/svn/bruegger fehlte z.B.)
- Kenne dein/das System!

Auslöser

14:19 Dirk Deimeke: Maschinenraum, die ip-adressen bitte

14:19 Ramon Kukla: Bin so angespannt, kann nicht tipppennn

Auslöser

- Arbeitsspeicher?
- Festplatte?
- Mainboard?

Abschliessend

Fragen?

Abschliessend

Danke!