Dontpanic
Erfahrungsbericht

Björn Wiedersheim

27.10.2014

Oktober 2014

Überblick

- Hardware
- Netzwerk
  - Firewall-Konfiguration
- VM-Administration
- Statistiken
- Backup
- Jabber-Server
- TODO

Hardware

- Fujitsu CELSIUS M720 Workstation
- Intel Xeon E5-1650 @ 3.20 GHz, 6 Kerne, Hyperthreading
- 32GB RAM
- 4 SAS- und 2 SATA-Schnittstellen
- 6 Festplatten:
  - ST32000542AS (Seagate Barracuda)
  - WDC WD20EARS-00MVWB0 (WD green)
  - WDC WD30EFRX-68AX9N0 (WD red)
  - SEAGATE ST9600205SS
  - HGST HUS724020ALS640
  - HGST HUS724020ALS640
- **keinen seriellen Anschluss**

Netzwerk

- 217.10.0.18 – dontpanic
- 217.10.0.28 – bytebooster, Adresse des physikalischen Hosts
- 217.10.15.16/27 – eigenes Subnetz
  - 217.10.15.17 – Adresse von dontpanic-host im Subnetz (Gateway)
  - 217.10.15.32 – Broadcastadresse des Subnetzes
- 192.168.122.0/24 – privates Subnetz

Firewall

- dontpanic-host
  - SSH von überall
  - Mail von dontpanic, VMs
  - 8080, 8443 Weiterleitung zu munin 80, 443
  - alles vom VM-Subnetz
- dontpanic
  - alles von überall
- jabber(-test)
  - SSH von dontpanic, dontpanic-host
  - Mail von dontpanic
  - http/https von überall
  - xmpp-Ports (5222, 5269, 5280, 5281) von überall
- auf allen Kisten fail2ban für ssh und ggf. http(s)

---

siehe `/etc/network/if-up.d/iptables`

virtuelle Maschinen

VM	IP	CPUs	RAM	Beschreibung
dontpanic	217.10.0.18	4	4GB	fast alles
munin	192.168.122.32	1	512MB	Statistiken
ffmpeg	192.168.122.198	2	1GB	Chaosseminare (Björn)
jabber	217.10.15.19	2	4GB	XMPP-Server
pcv1	217.10.15.20	1	1GB	Test-VM (Raimund)
pcv2	217.10.15.21	1	1GB	Test-VM (Raimund)
jabber-test	217.10.15.30	1	512MB	XMPP-Server (Marcus)

Zugriffsberechtigungen

dontpanic-host Björn, Jens, Jürgen, Marcus

jabber jabber@dontpanic

jabber-test Marcus

munin (ssh) Björn

munin (https) siehe Wiki

ffmpeg Björn

pcv1 Raimund

pcv2 Raimund

VM-Verwaltung

- alle Kommandos auflisten: `help`
- Hilfe zu Kommando abrufen: `help` **Kommando**
- laufenden VMs anzeigen: `list`
- alle existierenden VMs anzeigen: `list --all`
- Konfiguration einer VM editieren: `edit` **vm-name**
- VM starten: `start` **vm-name**
- VM (kontrolliert) herunterfahren: `shutdown` **vm-name**
- Stecker ziehen: `destroy` **vm-name**
- serielle Konsole: `console` **vm-name**
- VNC-Port anzeigen: `vncport` **vm-name**
- Infos über VM anzeigen `dominfo` **vm-name**
- RAM anpassen (in KiB) `setmem` **vm-name mem-size**

VM-Verwaltung

- boot-Partition:

  ```
  lvcreate -L 100M -n testvm-boot lvm /dev/md1
  ```

- root-Partition:

  ```
  lvcreate -L 10G -n testvm-disk lvm /dev/md1
  ```

- Dateisystem (ext4) anlegen:

  ```
  mkfs.ext4 /dev/lvm/testvm-disk
  ```

- virtuelle Maschine erstellen und mit debian-installer aus dem Netz starten (siehe Wiki)
- alternativ virtuelle Maschine erstellen und mit iso-Image booten (siehe Wiki)

Network bridges für VMs

br0 bridge mit physikalischem Netzwerkinterface (sollte nicht für VMs benutzt werden)

br1 217.10.15.16/27, für VMs mit öffentlichen IPs

virbr0 192.168.122.0/24, dhcp+nat

feste IP-Adressen per DHCP:

br1 `virsh net-edit in-net`

virbr0 `virsh net-edit default`

VM-Verwaltung II

Partitionen vergrößern

- Parttion vergrößern:

  ```
  lvresize -L +10G /dev/lvm/testvm-disk
  ```

- Dateisystem vergrößern:

  ```
  resizef2 /dev/lvm/testvm-disk
  ```

VM löschen

- VM löschen: `virsh undefine testvm`
- boot-Partition löschen:

  ```
  lvremove /dev/lvm/testvm-disk
  ```

- root-Partition löschen:

  ```
  lvremove /dev/lvm/testvm-boot
  ```

Backup

- LVM-Snapshots
- wöchentlich komplettes Backup
- täglich inkrementelles Backup
- Backup-Dateien älter 30 Tage werden gelöscht
- logical volume *backup* (375GB von 1000GB genutzt)
- dort auch Reste alter Installationen
- home grown `/usr/local/sbin/vmbackup` (basierend auf *tar*)
- Konfiguration `/etc/vmbackup/vmbackup.cfg`

Backup II

Backup von:

- host-disk
- dontpanic-disk / dontpanic-home
- ffmpeg-disk
- jabber-disk
- munin-disk

kein Backup von:

- boot/swap-Partitionen
- dontpanic-data
- backup
- jabber-test-disk / pcv1-disk / pcv2-disk
- CCC-VIDEOs

Statistik

- https://bytebooster.ulm.ccc.de:8443/munin/
- Munin
- eher zuviel als zu wenig Informationen
- rrd-Datenbank
- ein Datensatz alle 5 Minuten
- Daten älter als ein Jahr werden überschrieben
- maximalwerte für Warnungen und Fehlernachrichten konfigurierbar
- kann Mails verschicken (aktuell nicht konfiguriert)
- neben Munin noch selbstgestrickte Lösung, die Temperaturen aufzeichnet und wöchentlich Zusammenfassung per E-Mail verschickt

Jabbermagie

- Prosody (0.9.6) mit *mu-conference* und *BOSH*
- verschlüsselte Passwörter
- Konfiguration /etc/prosody/prosody.cfg.lua
- Admingruppe (marcel@jabber.ulm.ccc.de, mrks@jabber.ulm.ccc.de, cips@jabber.ulm.ccc.de)
- In-Client-Administration Node: http://jabber.org/protocol/commands
- prosodyctl
- Logs größtenteils deaktiviert
- DNS-Konfiguration
- kleines Speicherleck
- SSL `https://xmpp.net/result.php?domain=jabber.ulm.ccc.de&type=client`

Prosody mod_admin_telnet

```
nc localhost 5582
```

- host:list()
- server:uptime()
- server:version()
- c2s:show()
- c2s:show_secure()
- c2s:show_insecure()
- s2s:show()
- bye

---

siehe https://prosody.im/doc/console

TODO

- Wiki-Update (moinmoin-Version hoffnungslos veraltet)
- Apache in eigene VM (kein Zugriff auf Home)?
- eigene VM /dev/radio?
- Dontpanic neu installieren
- RAIDs umstrukturieren?
- Debian testing?
- mehr VMs/Administratoren
- Jabber-TODO
- alte Daten löschen
- Raimunds Vision