Der Chaosdorf-Adminreport

Daniel Friesel Maximilian Gaß

Chaosdorf

1. Oktober 2010

Am Anfang war das FreeBSD

- FreeBSD-System mit Jails auf chaosdorf.de
- Von ? bis Sommer 2009

Anforderungen

- Zentrale Nutzerverwaltung
- Shellserver
- Mailserver
- Website
- Internes Wiki + Interner Bugtracker

The Next Generation

- To Boldly Serve How Noone Has Served Before
- vm.chaosdorf.de
  - backend.chaosdorf.de
  - frontend.chaosdorf.de
  - shells.chaosdorf.de
- Debian Stable

Hardware und Hosting

- Hosting by OpenIT
- 217.69.82.240/29 in eigenem VLAN
- Keinerlei Remote-Zugriff außer SSH

vm.chaosdorf.de

- Drei VMs mit qemu-kvm + libvirt
- Zwei Festplatten, RAID 1 + LVM
- Verschlüsselte Volumes für die einzelnen VMs
- Paketfilter mit ferm, auch zwischen VMs etc.

backend.chaosdorf.de

- LDAP
- (Noch:) Webserver mit phpldapadmin
- approx (Debian-Paketcache)
- reprepro für das Admin-Toolkit

frontend.chaosdorf.de

- Mail
  - Postfix mit postgrey und SpamPD
  - Mailinglisten (miniml)
  - Roundcube mit MySQL
  - Dovecot
  - Alle mit LDAP-Anbindung

frontend.chaosdorf.de

- Webserver: Apache2
  - ikiwiki: Website und Wiki
  - Ticketsystem: Roundup mit SQLite
- Userzugriff: SSH für git + SFTP für Userwebsites
- Userquotas

shells.chaosdorf.de

- Shell-Zugriff. Sonst Nichts.
- Userlimits und Quotas

Clubraum-Infrastruktur

- Raumserver: figurehead
- Routing mit dn42-Anschluss
- MPD
- FTP
- In Zukunft: WLAN-AP
- Keine Useraccounts, daher keine LDAP-Anbindung

Clubraum-Terminal

- In Planung
- Mit LDAP-Anbindung
- Option, eigene Livesysteme vom USB-Stick zu booten
- Problem: Booten externer Sticks vs. LDAP-Passwort auf Festplatte

Dokumentation und Transparenz

- Doku schreiben, während man das System aufsetzt. Nicht später
- Änderungen: im öffentlichen Log + in #chaosdorf
- Idee: Auditing mit sudo und Logcheck
- User haben Lesezugriff auf's Monitoring
- Alle Änderungen werden angekündigt

Versionskontrolle

- etckeeper (Git für /etc)
- Ebenfalls: Git für /usr/local

Monitoring

- Will man haben
- Auf vom System komplett unabhängigen Host
- Zusätzliche Checks schaden nie
- Für SSH-CHecks: Separater key mit forcecommand
- Goodie: Ankündigungen im IRC per Bot

Besondere Checks

- Git-Status (/etc + /usr/local)
- Kein offener Mailrelay
- Kein SSH-Passwortlogin
- RBL (frontend nicht blacklisted)
- Laufende Kernelversion
- SSL-Zertifikate

Automatisierung

- Puppet (Rubyrant von mxey)
- $\rightarrow$ Admin-Toolkit als .deb mit reprepro

Siehe auch

- https://intern.chaosdorf.de/admin/
- http://github.com/chaosdorf/chaosdorf-admin-toolkit