

Betrieb von shared Servern - am Beispiel von Hostsharing.

ein kurzer Vortrag von Purodha Blissenbach,

beim

Hitforum - 26.November 2003

gefolgt von

einer regen Stunde mit Fragen und Antworten.

Betrieb von shared Servern - am Beispiel von Hostsharing.

Die Hostsharing eG betreibt viele Dienste.

Einige Beispiele:

Webserver (apache, apache-ssl, eigene Konfigurationen),
e-mail Server (postfix, procmail, courier, Webmail),
Datenbank-Server (mySQL, mySQL-ext, PostgreSQL,
Webinterfaces), ssh-Server, ftp-Server(Proftpd), cvs-Server,
Nameserver (Bind9), News/Mailinglisten (MailMan, Encartis),
Domainbestellsystem, Abrechnung, Backup und Restore,
Server-Überwachung (mon), eigene Websites, ...

Rahmenbedingungen:

Betrieb in Mitarbeiter- und Kundenhand => "jeder" kann
mitmachen, "jeder" soll durchblicken können,
Anspruch des *Lernens* ist in der Satzung verankert.

Betrieb von shared Servern - am Beispiel von Hostsharing.

Die Website sagt:

Grundsätzlich können alle Serverdienste angeboten werden, wenn

- a) sich jemand aus dem Kreis der Hostmaster findet, der die Betreuung übernimmt,
- b) Hostsharing genügend Serverplatz und Serverleistung für diese Anwendung zur Verfügung steht,
- c) eine gerechte Abrechnung der Leistungsnutzung für den jeweiligen Dienst gewährleistet ist und
- d) die Sicherheit des Serverbetriebs dadurch nicht gefährdet wird.

Ausserdem:

- e.2) Es findet sich wenigstens ein verlässlicher Betreuer oder Einrichter, bzw.
- e.1) das Gewünschte liegt als fertiges Debian Paket vor.

Betrieb von shared Servern - am Beispiel von Hostsharing.

Hierarchie der User:

“oben” Hostmaster	vn, ...
(Hostmaster-Anwarter)	vn, ...
(Hostsharing-Mitglied)	hsh00- xyz, hsh00- vn, ...
PaketAdmin	xyz00, xyz01, ...
(DomainAdmin)	xyz00- otto, xyz00- theo. k, ...
Paket-User	xyz02- i hk. muel ler. ei ns, ...
“unten” (Kunde eines Hostsharing-Mitglieds)	

Namen reflektieren Paketzugehorigkeit:

z.B. Datenbank: `xyz00_hoffmans` oder

popmail Account: `xyz03- schul ze. kg. user. 4711`

Betrieb von shared Servern - am Beispiel von Hostsharing.

Sicherheit:

- typisch für Multiuserbetrieb
- “root” user darf und kann alles (hostmaster)
- jeder User ist für sich selbst verantwortlich
- jeder User verantwortet mit, was er delegiert
- User haben lesenden Zugriff, wo nichts zu verbergen ist
- kein User hat Zugriff auf Dinge, die ihn nichts angehen
- User hat Schreibzugriff nur im “eigenen Bereich”
- außerdem kann jeder User versehentlich oder absichtlich
Andern Rechte einräumen
(in Grenzen, die die Implementation setzt)
- Rechte-Erwerb nach “oben” (eG-Verantwortungsbereich)
erfordert datenschutzrechtlich relevante Unterschrift

Betrieb von shared Servern - am Beispiel von Hostsharing.

Gliederungskonzept "Pakete":

- eine unix-Gruppe pro Paket (Rechteschleuse)
- ein home-Verzeichnis pro Paket
- Hostsharing besitzt selber Pakete
- User sind "unterhalb" eines Paketes angesiedelt
- Domains sind "unterhalb" eines Paketes angesiedelt
- Zentrale Konfigurations-Daten werden verteilt auf Pakete (oder User oder Domains)
- bestimmte Paket-Eigenschaften:
 - eigene oder gemeinsame IP-Adresse,
 - Dynamic-Web / Static-Web / NS -Paket
 - Anon-ftp
 - cvs-Server
 - Zope-Server
 - SSL-Kommunikation per eigenem Zertifikat
- usw.
- ein Paket liegt auf einem bestimmten Host.

Betrieb von shared Servern - am Beispiel von Hostsharing.

Gliederungskonzept "Domains":

- ein Verzeichnis pro Domain
- zentrales Verzeichnis aller (delegierten) Domains
- Hostsharing besitzt selber Domains
- Domains sind "unterhalb" von Paketen angesiedelt
- DomainAdmin (User im Paket) ist für Domain verantwortlich (das kann auch der PaketAdmin selber sein)
- Mehrere:
 - Domains pro Paket
 - DomainAdmins pro Paket
 - Domains pro DomainAdmin
- Konfigurations-Daten liegen in Domain-Verzeichnissen
- Subdomains (für Webserver) vom DomainAdmin einrichtbar per ``mkdi r``
- (Webserver) Subdomain-Rechte an andern User delegierbar
- eine Domain liegt auf einem bestimmten Host.

Betrieb von shared Servern - am Beispiel von Hostsharing.

Rechte im Dateisystem:

Problematik:

- Daemon-Prozesse sollen nicht als "root" laufen.
- Server brauchen Zugriff auf User-Verzeichnisse.
- User einer Gruppe (Paket) sind strikt zu trennen.

Lösung: (Rechteschleuse)

User a ohne, b mit Domains:

SW-Paket:

```
drwx- -x- -0 xyz02 httpd /home/pacs/xyz00/
```

DW-Paket:

```
drwx- -x- -x xyz00 xyz00 /home/pacs/xyz00/
```

```
drwxr- x- -x xyz00 xyz00 /home/pacs/xyz00/users/
```

```
drwxr- x- -x xyz00- a xyz00 /home/pacs/xyz00/users/a
```

```
drwxr- x- -x xyz00- b httpd /home/pacs/xyz00/users/b
```

```
dr xr- xr- T httpd xyz00 /home/pacs/xyz00/users/b/doms
```

Serverprozesse laufen als user `httpd` .

DomainAdmin kann User-Rechte annehmen - spezielles ``su`` .

Betrieb von shared Servern - am Beispiel von Hostsharing.

Zentrale Dienste, zum Beispiel:

Config-Robot:

z.B.:

- /etc/passwd
- /etc/aliases
- /etc/postfix/virtusertable
- /etc/bind/pri.*domain*

Domain-Robot (mehrere Prozesse, e-mail-Robot)

- ~/etc/dom-order.*domain*

Zentraler Backup (mehrere Prozesse auf zwei Servern)

- täglich mehrere rsync-Läufe, Datenbanken extra,
- "sinnvoll" inkrementell Packen und Linken,
- Lösch- und Bestandslisten führen

Zentrales Monitoring (Prozesse mehreren Servern)

- Alarme per SMS
- Alarme per e-mail
- Infos per e-mail
- Statistik-Daten

Betrieb von shared Servern - am Beispiel von Hostsharing.

Abrechnungen:

Paket-Verwaltung, Optionen

Domain-Verwaltung, TLD, Abrechnungsarten und Laufzeiten

“Verbrauchszählungen” zu Stichtagen (Speicher, User, usw.)

Laufende Überwachung mit Warn-e-mails (Quota, Traffic)

Trafficmessungen per **iptables** und Auswertung per **ipacct**

Traffic-Hochrechnungen aufgrund von Logfile-Auswertungen
(für bestimmte Dienste)

Monatliche Rechnungserstellung aufgrund der gesammelten
Abrechnungsdaten

Zahlungen und Buchen mit **Lexware**, Bank-Daten per **hbci**,
eigene Abrechnungs- und Controlling Software.

Betrieb von shared Servern - am Beispiel von Hostsharing.
Beispiele für Probleme beim shared / virtuellen Zugriff:

Anonymous ftp : Welches Verzeichnis ?

cvs (pserver) : Zuordnung der Repositories zum Paket ?

http-ssl : Virtueller Server erst nach ssl-Entschlüsselung bekannt.

Apache, mod_php : phpsavemode=yes notwendig, infolgedessen
Datei-Zugriffe mit Rechten des httpd
bzw. weitgehend blockiert - File-Uploads ?

Apache, php via cgi : phpsavemode wahlfrei, jedoch
Datei-Zugriffe mit Rechten des PaketAdmin
freier konfigurierbar, File-Uploads inkompatibel
mit mod_php .

IMAP4 : shared folders exportieren "zu viele" Rechte.

... und weitere ...

Betrieb von shared Servern - am Beispiel von Hostsharing.

Vertiefende Fragen und ihre Antworten:

... und weiteres ...

Noch offen.

Betrieb von shared Servern - am Beispiel von Hostsharing.

Vielen Dank !

Wer noch nicht hat:

Flyer mitnehmen !