

Impressum:

Heinlein Professional Linux Support GmbH

Schwedter Straße 8/9 B, 10119 Berlin

Telefon: 030/40 50 51-0, Telefax: 030/40 50 51-19

<http://www.heinlein-support.de>, mail@heinlein-support.de

V.i.S.d.P.: Peer Heinlein, Schwedter Str. 8/9 B, 10119 Berlin

Postfix: qmgr darf nicht chrooted sein

In SuSE-Installationen wird bei Postfix der qmgr in einer chroot-Umgebung gestartet. Das kann zum Verlust von Logzeilen führen, da der qmgr den Syslog-Dämon nicht mehr erreicht. Für den qmgr sollte in der master.cf also chroot deaktiviert werden.

Tool Tipp: Cluster-SSH

„Der gute Admin hat nichts zu tun.“ Auf dem Weg zu diesem Ziel begleiten uns zahlreiche Scripte und hilfreiche Tools. Hier möchten wir Ihnen ein Werkzeug vorstellen, das für die identische Administration mehrerer Server hilfreich ist: ClusterSSH.

Das Tool loggt sich auf mehreren Servern gleichzeitig per SSH ein, so dass der Admin Kommandos an alle Server simultan absetzen kann. Begrenzt wird das muntere Treiben lediglich von der Größe des eigenen Bildschirms. Zwingende Voraussetzung ist allerdings ein X-Server, der Fenster darstellen kann.

ClusterSSH ist in Perl programmiert, die Quellen sind über <http://sourceforge.net/projects/clusterssh/> zu bekommen und schnell installiert. Administratoren von SUSE-Systemen finden fertige RPM-Pakete im RPM-Repository von Peer Heinlein (<http://download.opensuse.org/repositories/home:/pheinlein/>), das auch in YaST eingebunden werden kann.

Die Syntax ist einfach:

```
cssh [user@]server1[:port] [user@]
server2[:port] [user@]server3[:Port]
```

Es öffnet sich sowohl ein Fenster als Steuerkonsole als auch jeweils ein Fenster pro Zielsystem, auf dem die Ausführung der Kommandos kontrolliert werden kann. Eine zusätzliche Verbindung baut man mit [STRG] [+] auf. Sollte eine Verbindung zu einem Server nicht auf Anhieb funktionieren, kann man mit dem Schalter „-e“ diese eine Verbindung von cssh überprüfen lassen.

Peer Hartleben

Heinlein Mail-Archiv zum Test bereit



Nach mehreren Mannjahren Entwicklungsarbeit bietet das Heinlein Mail-Archiv nun eine flexible revisionssichere Mail-Archivierung, wie sie vom Gesetzgeber für Unternehmen gefordert wird. Das Besondere: Das Mailarchiv arbeitet als SMTP-Relay mit jeder beliebigen Groupwarelösung zusammen – und weil's aus dem Hause Heinlein kommt

ist auch gleich ein wirkungsvoller Spam-Schutz als Zusatzmodul verfügbar. Für den Betrieb kann zwischen einer VMware-Installation oder einer in drei Größen verfügbaren Appliance gewählt werden. Per Download oder Demo-Zugang kann man das Mail-Archiv nun auf Herz und Nieren prüfen.

<http://www.heinlein-support.de/mailarchiv>

4. Secure Linux Administration Conference

Am 10. und 11. Dezember 2009 findet in Berlin wieder die Secure Linux Administration Conference (SLAC) statt. An zwei Tagen bietet die Konferenz insgesamt 18 hochkarätige Vorträge. Die Highlights dieses Jahres: Einblicke in Virenlabors, Verwundbarkeitsanalysen, MySQL-Performancetuning, LDAP-Replikationen und viele andere Themen, die im Admin-Alltag weiterhelfen.

<http://www.heinlein-support.de/slac>

Der Film zur Mailserver-Konferenz

Spannende Vorträge liefen auf der 4. Mailserver-Konferenz im vergangenen Juli. Grund genug, diesmal die Videokamera mitlaufen zu lassen. Neben Aufzeichnungen ganzer Vorträge ist auch eine fünfminütige Dokumentation entstanden:

<http://www.heinlein-support.de/mk09>

Der Newsletter von Heinlein Support.

logfile-200910

- ReaR: Disaster-Recovery
- Greylisting: Der Virenschutz
- Tooltipp: Cluster SSH

ReaR: Disaster-Recovery und P2V-Migration

„Viele verwechseln Backup und Disaster Recovery“ urteilte kürzlich Schlomo Schapiro, der das Softwareprojekt ReaR einst aus der Taufe gehoben hat. Denn im Disaster Fall ist es mit einem reinen Datenbackup nicht getan. Selbst wenn sich die Nutzdaten eines Servers mehr oder weniger systematisch archiviert irgendwo befinden, was zählt ist die sichere und schnelle Wiederherstellung des gesamten Systems – die voll-automatische Wiederherstellung im Krisenfall.

Vierorts ist nach einem Crash echte Handarbeit angesagt: Das Hardware-RAID eines Ersatzsystem muss eingerichtet und die Installation des Betriebssystems vorgenommen werden, um letztendlich die eigentlichen Nutzdaten zurückspielen zu können, die sich hoffentlich vollständig und halbwegs aktuell in irgendeinem Backup befinden. Am Ende bleibt die Hoffnung, dass alle Pakete installiert, die Partitionsaufteilung richtig vorgenommen, alle Userrechte wieder repariert und alle Netzwerk-Besonderheiten bedacht worden sind.

Doch in der Praxis scheitert es oft schon an der sicheren Verfügbarkeit des Installationsmediums: Die alten Betriebssystem-DVDs von anno dazumal sind längst verloren gegangen, gerade verlegt, ausgeborgt oder am Ende unlesbar zerkratzt. Nicht selten wird aus der Not heraus eine aktuellere Version installiert, so dass mitten im größten Crash auch noch ein Versionsprung in Kernel oder Anwendungsprogrammen dazukommt.

Wohl dem, der seine alte Konfiguration unter den neuen Versionen ohne größere Anpassungen wieder zum Laufen kriegt. Wehe dem, der feststellt, dass einige Programme wohl manuell compiliert waren und mit dem Server auch der zugrundeliegende Quellcode untergegangen ist.

► „Relax and Recover“: Der Name ist Programm

Doch es geht auch anders: Das unter der GPL frei verfügbare Projekt „Relax and Recover“ (kurz: ReaR) macht seinem Namen alle Ehre. Ist

der Ursprungsserver einmal sauber mit ReaR erfasst worden, kann ReaR dieses Setup jederzeit bei Null beginnend wiederherstellen.

Während sich der Admin noch vom Schreck erholt, bootet eine von ReaR passend zum Server angelegte Rescue-Installation, die per CD, USB-Stick oder PXE-Bootimage bereitgestellt werden kann. Diese Installation ist nur wenige MByte groß und wurde von ReaR individuell aus dem Linux des Originalservers heraus angefertigt. Damit ist sichergestellt, dass Kernel und alle Kernel-Module genau dem Ursprungssystem entsprechen. Auch manuell nachinstallierte Kernelmodule für exotische Server-Hardware werden eingebunden, so dass das Rettungs-System sicher auf der fraglichen Hardware booten kann.

Bevor die Daten zurückgespielt werden können, muss die neue Hardware eingerichtet werden. Auch das erledigt ReaR vollautomatisch und kann selbst die Hardware-RAID-Controller der bekannten Hersteller ohne weitere Zuarbeit initialisieren. Komplizierte Linux-Setups mit Software-RAID, LVM, Crypto-Partitionen (oder beliebige Kombinationen davon!) bringen ReaR nicht aus der Ruhe. Sind auch die jeweiligen Dateisysteme formatiert worden, kann

(h|b)log

Vor wenigen Wochen war es endlich soweit: Nach vielen Mannjahren Programmierarbeit konnten wir die erste Beta-Version unserer Software zur Mailarchivierung an Kunden zum freien Test herausgeben. Die Rückmeldungen unserer Testkandidaten haben unsere kühnsten Erwartungen übertroffen: Es gab entweder begeisterte Antworten („genau das, was ich brauche“) oder gar keine, was uns zunächst etwas nervös werden lies. Doch auch hier konnten wir uns über die Begründung, warum die Tester nichts haben von sich hören lassen, nur freuen: „Es gab halt nix zu meckern, es hat alles funktioniert.“ Nun, das hören wir gerne.

Und nicht nur das Mailarchiv wurde released, auch die Mitarbeiter unseres Teams forken fröhlich Nachwuchs in die Welt: Eine Maja erblickte am 27. Oktober das Licht der Welt und wie man munkelt sind weitere familiäre Neuzugänge in den nächsten Monaten angesetzt. „Fruchtbare Firma“ – anders kann man unseren Baby-Boom wohl kaum erklären...

Schöne Grüße aus Berlin,
Peer Heinlein

ReaR die Daten des Backups zurückspielen. Die dafür notwendige Backup-Software für den Zugriff auf die Tape-Library hat ReaR ebenfalls aus dem Ursprungssystem extrahiert und in die Rettungs-Umgebung mit aufgenommen. Denn ReaR trennt klar die Funktionen „Recovery“ und „Backup“ – für letzteres sollte spezialisierte Backup-Software zuständig sein, mit der ReaR gerne zusammenarbeitet. Für anspruchslöse Setups auf die Schnelle bieten sich hilfsweise auch tgz-Archive auf NFS-Laufwerken an.

Am Ende werden LILO oder GRUB wiederhergestellt. Nach einem Reboot startet das System als ob nie etwas vorgefallen wäre. Je nach Datenmenge geht der gesamte Recovery-Prozess binnen weniger Minuten ohne Programmrückfragen über die Bühne.

► **Neue Hardware kann auch virtuell sein**

Doch damit bei Weitem nicht genug. Denn wer sagt denn, dass ReaR das Recovery nur auf einer baugleichen Hardware durchführen kann? Im Auftrag eines Kunden und zusammen mit ReaR-Maintainer Schlomo Schapiro entwickelte Heinlein Support die Version „ReaR P2V“. Jetzt erkennt ReaR geänderte Festplatten-Controller oder Netzwerkkarten automatisch und passt die Linux-Installation im Idealfall vollautomatisch an: Konfigurationen werden übertragen, Hardware-IDs oder MAC-Adressen angepasst, IP-Adressen werden umkonfiguriert – falls notwendig wird auch der Inhalt der initrd angepasst. Werden vorab schon entsprechende Mapping-Dateien vorbereitet, kann ReaR die gesamte Migration ohne Rückfragen ausführen.

Egal, ob der Wechsel von IDE zu SATA, ein Schwenk auf SAS oder gar die Verlagerung des Plattenspeichers in ein SAN: ReaR P2V ändert alle notwendigen Platten-IDs und Partitionsnamen, damit das neue System startet, als ob es nie anders installiert worden wäre.

Auf die Besonderheiten der virtuellen Maschinen wird intelligent Rücksicht genommen: Netzwerkbondings und Software-RAIDs werden nicht mehr benötigt, die Anbindung eines SAN wird unterstützt. Zukünftig soll ReaR auch die Möglichkeit bieten, die Größe von Festplattenpartitionen automatisch anpassen zu können, denn beim Gang in eine virtualisierte Umgebung sollen in den seltensten Fällen die ursprünglichen Partitionsgrößen beibehalten werden. ReaR ist damit ein universelles herstellerunabhängiges Migrations-tool geworden: Von Hardware zu Hardware oder rein in virtuelle

Umgebungen: ReaR rollt das System im Idealfall ohne Anpassungsaufwand durch den Administrator in rasanter Zeit neu aus. Selbst der Wechsel von einer virtuellen Umgebung zurück auf eine physikalische Hardware klappte schon beim ersten Test unserer Entwicklungsversion sofort fehlerfrei.

ReaR ist damit mehr als „nur“ ein Disaster-Recovery-Tool. Ab sofort bietet es Unternehmen die Grundlage jederzeit flexibel und frei eine Hardware- oder Virtualisierungsplattform zu wechseln. Denn anders als die von einigen Virtualisierungsherstellern angebotenen Import-Tools verfolgt ReaR keine herstellereigenen Interessen – und arbeitet darum prinzipiell mit allen Plattformen zusammen. So steht auch einem Wechsel von einer Virtualisierungslösung zu einer anderen Technik nichts mehr im Wege – und kann vor allem bei minimaler Planung, kürzester Ausfallzeit und geringem Arbeitsaufwand für den Admin vorgenommen werden.

ReaR unterliegt der GPL und ist damit kostenfrei verfügbar – manche Distributionen bringen von Haus aus eigene ReaR-Pakete mit, die Aufnahme in Enterprise-Varianten sollte in Kürze erfolgen. Als GPL-Software ist ReaR frei nutzbar – und das Team von Heinlein Support steht mit seinem Know-how für Teststellungen oder zur Konzeptentwicklung zur Verfügung, bietet 24/7 Support oder führt den schlüsselfertigen Rollout einer ReaR-basierten Disaster Recovery oder P2V-Lösung durch.

► **Werden auch Sie ReaR-Pate**

Die folgenden Features warten darauf, in entsprechenden Projekten umgesetzt zu werden:

- Migrationen nach XEN oder KVM inkl. Einrichtung der virtuellen Maschine in der Virtualisierungslösung
- Vergrößerung/Verkleinerung von Dateisystemen beim Recovery
- Management-GUI zur Verwaltung und Kontrolle aller Server und ihrer Zustände
- Task-Manager zum zeitgesteuerten Recovery mehrerer Installationen

Weitere Informationen zum Projekt und eine Filmdokumentation zur P2V-Migration auf: <http://www.heinlein-support.de/rear>

Peer Heinlein

Das Projekt KIVBF Mailbackbone 2008

Die Kommunale Informationsverarbeitung Baden-Franken (KIVBF), mit 550 Städten, Gemeinden und Landkreisen eines der führenden kommunalen IT-Systemhäuser, betreibt für seine Kunden eine Mailbackbone-Infrastruktur mit einem Mailaufkommen von mehreren Millionen E-Mail-Nachrichten pro Tag. Im Jahr 2008 wurde diese komplett auf eine OpenSource-Plattform umgestellt. Unterstützung bezog KIVBF dabei in Rat und Tat durch die Heinlein Professional Linux Support GmbH, mit dessen Akademie man bereits im Vorfeld, u. a. bei Postfix-Schulungen zusammengearbeitet hatte. Trotz umfangreicher Dimensionierung der Systeme an zwei Standorten konnte innerhalb weniger Tage eine erstaunliche Optimierung hinsichtlich Performance, Redundanz und SPAM-Erkennungsqualität erzielt werden. Dies führte u. a. auch zur Einsparung aller kommerziellen Lösungen für Anti-Spam/Anti-Virus.

Martin Nelius, IT-Security, Kommunale Informationsverarbeitung Baden-Franken

Unsere Veranstaltungstermine: Januar bis Juni 2010

KW	Datum	Kurs	Dozent
10	10.03. - 12.03.	Aufbau einer Unternehmens-PKI	Jan Rösner
10	15.03. - 19.03.	Linux Admin Grundlagen	Peer Hartleben
11	15.03. - 19.03.	Sichere Mailserver mit Postfix	Peer Heinlein
12	22.03. - 26.03.	Nagios Networkmonitoring	Sven Velt
12	22.03. - 26.03.	Xen - Virtualisierte Server	Thomas Wurfbaum
15	12.04. - 14.04.	NEU bash-Scripting für Admins	S. Semmelroggen
15	12.04. - 16.04.	Hochverfügbarkeit mit Heartbeat2 und LVS	Dr. M. Schwartzkopff
16	19.04. - 23.04.	Samba als Alternative zu Windows	Stefan Kania
16	19.04. - 23.04.	Linux Admin Fortgeschrittene	Peer Hartleben
17	26.04. - 30.04.	LPI-Zertifizierung (LPIC-2)	A. Niederländer
17	26.04. - 30.04.	Netzwerkrouting für Profis	Richard Müller
17	26.04. - 30.04.	NEU HA-Virtualisierungscluster mit KVM	Thomas Wurfbaum
18	03.05. - 05.05.	SpamAssassin und AMaViS	Peer Heinlein
18	03.05. - 05.05.	VMware für Profis	Holger Uhlig

KW	Datum	Kurs	Dozent
20	17.05. - 19.05.	Cyrus IMAP-Server	Peer Hartleben
20	17.05. - 19.05.	Windows-Software-Verteilung mit opsi	Detlef Oertel
20	17.05. - 21.05.	NEU Hochperformante Webcluster	n. n.
22	31.05. - 04.06.	PostgreSQL für Profis	Hans Schöning
22	31.05. - 04.06.	Linux Admin Grundlagen	Peer Hartleben
23	07.06. - 11.06.	LPI-Zertifizierung (LPIC-1)	A. Niederländer
23	07.06. - 11.06.	Apache Webserver	Sven Velt
24	14.06. - 18.06.	LDAP zur zentralen Benutzerauthentifizierung	Stefan Kania
24	14.06. - 18.06.	Sichere Mailserver mit Postfix	Peer Heinlein
25	21.06. - 25.06.	Nagios für Fortgeschrittene	Sven Velt
25	21.06. - 25.06.	PHP-/Webserversicherheit	Peter Prochaska
26	28.06. - 30.06.	Systematische Fehler- u. Netzwerkdiagnose	S. Semmelroggen
26	28.06. - 30.06.	High-End-Mailserver Postfix am Limit	Peer Heinlein

Irrtümer und Änderungen vorbehalten. Stand: 11/2009. Beachten Sie <http://www.heinlein-support.de/akademie> für den letzten Stand.

Greylisting: Unverzichtbarer Virenschutz

Rund 80 bis 90 Prozent des heutigen Spams wird über Botnetze verschickt, also über virenfizierte Windows-PCs, die von Hackern ferngesteuert werden können. Greylisting hat sich schon seit vielen Jahren als höchst effektiver Spam-Schutz bewährt. Verkannt wird jedoch: Greylisting schützt auch gegen Viren.

Leider existieren gerade in Unternehmen oft Vorbehalte über die Auswirkungen, Vor- und Nachteile von Greylisting. Oft basieren diese auf Irrtümern, falschen Annahmen – oder Erfahrungen mit schlechter Software. Denn nicht selten werden einfach nur mangelhafte Greylisting-Implementierungen eingesetzt. Aus den daraus entstehenden Problemen wird dann abgeleitet, Greylisting sei per se problematisch und untauglich. –Weit gefehlt! Anders als oft behauptet hat es – richtig eingesetzt und konfiguriert – so gut wie keine Auswirkungen auf den Empfang erwünschter E-Mails und ist damit der derzeit beste und vor allem nebenwirkungsfreieste Spam-Schutz. Unsere Programm-Empfehlung: „postgrey“ von David Schweikert (<http://postgrey.schweikert.ch>).

► Fast alle Viren-Mails stammen aus Botnetzen

Und doch gibt es neben dem Spam-Schutz noch einen weiteren wichtigen Grund, als Unternehmen nicht auf den Einsatz dieser Technik zu verzichten: der Virenschutz! Denn genauso, wie der Empfang von Spam verhindert wird, kann Greylisting auch den Empfang von Viren verhindern. Das ist ganz besonders deshalb interessant, weil „nur“ rund 80 bis 90 Prozent des heutigen Spams über Viren-Botnetze versandt werden – aber nahezu 100 Prozent der Mail-Viren stammen aus diesen Quellen.

Der Wirkungsgrad von Greylisting gegen Viren liegt also noch weit über den bereits beachtlichen Wirkungen gegen Spam. Dabei hilft Greylisting bereits „ab Sekunde Null“, also genau der Zeit, in der herkömmliche Virenkiller noch blind sind und den Virus mangels geeigneter Signaturen oft nicht erkennen können. In der heiklen Zeit zwischen Ausbruch eines neuen Virus und der Verfügbarkeit aktuallisierter Signaturpattern kann Greylisting ein Unternehmen effektiv und sicher schützen.

Im Idealfall kann der Empfang der Virenmails komplett verhindert werden, doch selbst wenn „nur“ eine Verzögerung erreicht wird, ist das genau der entscheidende Zeitvorsprung, den die Virenkiller-Hersteller zur Verbreitung neuer Signaturupdates benötigen. Greylisting hilft also sicher über die gefährliche „Stunde Null“ hinweg.

► Greylisting greift, wo Virenkiller schwach sind

Gerade weil Greylisting die etablierten Virenkiller genau in dem Bereich ergänzt, wo diese eine Schwachstellen haben, sollte jeder IT-Sicherheitsverantwortliche auf den Einsatz von Greylisting im Unternehmen geradezu drängen. Wenn Unternehmen einerseits immense Summen für einen effektiven Virenschutz ausgeben und ein immenses Schadensrisiko bei einem erfolgreichen Virenbefall existiert, ist es geradezu unverantwortlich auf einen kostenlosen und sehr effektiven Virenschutz komplett außen vor zu lassen. Die positiven Auswirkungen auf den Spamschutz sind angesichts der Bedrohung durch Viren schon fast als lediglich angenehmer Nebeneffekt zu bezeichnen.

Peer Heinlein