Stephan Seitz <s.seitz@heinlein-support.de>

Serverdokumentation mit RackTables und Net-SNMP

Stephan Seitz <s.seitz@heinlein-support.de>

Wer sind wir?

- wir bieten seit 20 Jahren Wissen und Erfahrung rund um Linux-Server und E-Mails
- IT-Consulting und 24/7 Linux-Support mit 21 Mitarbeitern
- Eigener Betrieb eines ISPs seit 1992
- Täglich tiefe Einblicke in die Herzen der IT aller Unternehmensgrößen

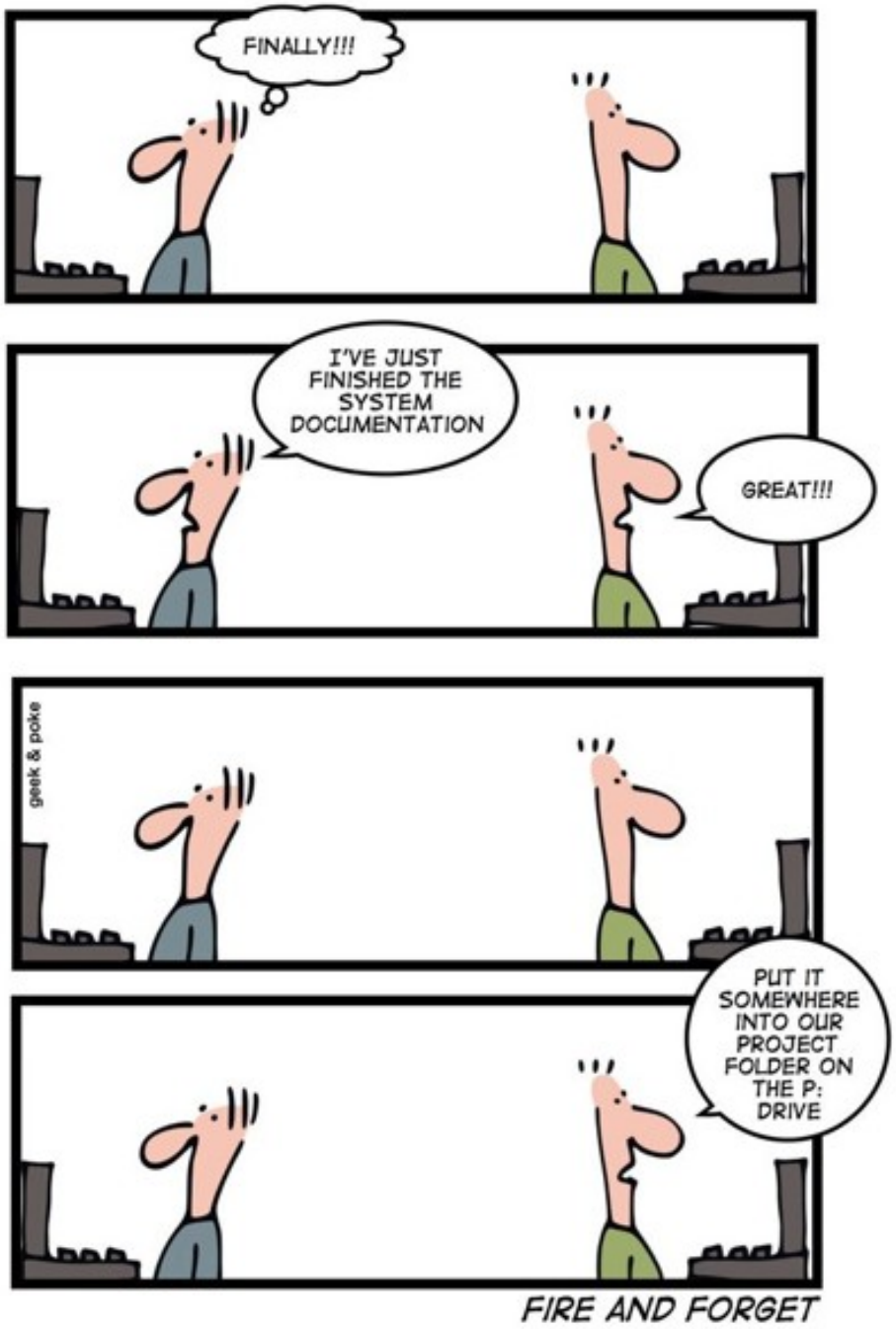
Stephan Seitz <s.seitz@heinlein-support.de>

Teil 1:
Dokumentation

heinlein

Dokumentation ...

- → ist (häufig)
  - → schwer wiederzufinden
  - → selten aktuell
  - → ziemlich umständlich zu erstellen
  - → zeitraubend (bzw. wird oft so empfunden)
  - → verteilt über diverse Doku-Systeme
    - → inklusive PostIt :)
  - → meist nicht verlässlich
  - → folglich äußerst unbeliebt
  - → notwendig



Stephan Seitz <s.seitz@heinlein-support.de>

Dokumentation ...

- geht auch einfacher
  - an einer zentralen Stelle geführt
    - Hardware (Asset Management)
    - Layer 2 und Verkabelung im allgemeinen
    - Layer 3
    - Betriebssystem und Softwarestände
  - automatisiert aktuell zu halten
  - einfach zu ergänzen
  - durch Verknüpfung von Teilbereichen übersichtlicher und schneller
    - L2/L3 → Cluster → Services, etc..
  - in einem Doku-System
    - triviales Backup / Recovery
  - dadurch insgesamt verlässlicher

Stephan Seitz <s.seitz@heinlein-support.de>

Teil 2:
Die Werkzeuge

Der Unterbau

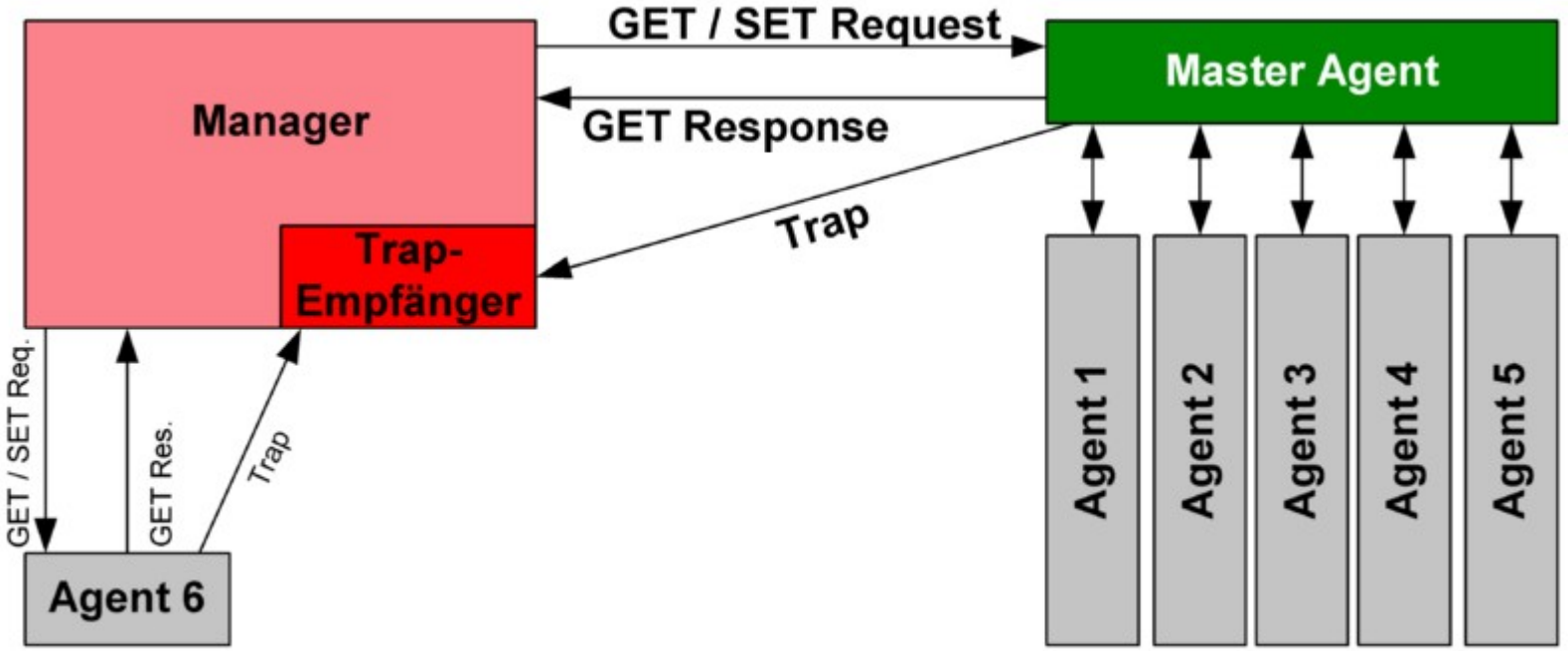
RackTables

- 2005 aus der Not heraus von Admins für Admins entstanden
- unter GNU GPLv2 lizensiert
- PHP 5 + MySQL
  - benötigt php-snmp und idealerweise php-pcntl
- wird aktiv weiterentwickelt
- ist eher ein Framework und keine „Business-Solution“
  - muss an die eigenen Bedürfnisse angepasst werden
  - bietet eine recht gut dokumentierte Framework-API an
  - unterstützt von Haus aus rechenzentrumsübliche Hardware (Switches, Router, Server)
    - SNMP MIBs/OID-Bäume und Dialoge für aktuell 880 Switch-Modelle
  - kann Benutzer gegen LDAP authentisieren
- diverse contrib-/Plugin-Sammlungen auf github

Der Unterbau

Net-SNMP

- Arbeitsweise von SNMP (v1 / v2)



- Quelle: Wikipedia

Der Unterbau

Net-SNMP

- Simple Network Management Protocol
  - de-facto Standard zur Überwachung und (teilweise auch Konfiguration) von Netwerk-Komponenten (Router, Switches, Server, auch: Drucker, IP-Telefone, etc...)
  - Agentenbasiert. Auf jedem Device läuft ein SNMP Agent
- OID
  - Informationen sind in OID-Bäumen (Objekt Identifikatoren) nach ASN.1 organisiert
    - Vorteil: Die Objektklassen und Typen sind klar definiert
    - Nachteil: Die OID und die enthaltenen Werte sind natürlich Geräte- /Hersteller-/Modell-spezifisch
- MIB
  - Zur Identifizierung von OID und Werten werden Message Information Base Dateien verwendet.
    - IETF, IANA, RFC-Editor definieren Standards, Hersteller nutzen häufig definierte „enterprise“ Unterbäume

Versionen und Implementierungen

Net-SNMP

- 1988 → SNMPv1
  - Passwörter werden im Klartext übertragen
- 1992 → Secure SNMP
  - RFC 1351, 1352, 1353 wurde nie implementiert sondern direkt ersetzt durch:
- 1993 → SNMPv2p/u/c
  - p / Party-Based
    - Versucht Sicherheit durch eine Art Session zu erhöhen
  - u / User-Based
    - führt Benutzernamen ein, mit dem Versuch mehr Sicherheit zu bieten
  - c / Community-Based
    - führt Communities ein, (ebenfalls mit der Idee von Sicherheit)
    - Communities sind praktisch zur Eingrenzung von Geräte-Pools
- SNMPv1/v2X → Security is Not My Problem :)

Versionen und Implementierungen

Net-SNMP

- 2002 → SNMPv3
  - Erste wirkliche Ansätze zur Sicherung von SNMP-Paketen
  - Definiert durch RFC 3410 – 3418 (**neun** RFC's ...)
  - Unterschiedliche Möglichkeiten zur Implemetierung von TLS
  - Sicherung durch x.509 Zertifikate
- SNMP im Alltag
  - Sicherheit? Hmmm....
  - v3 ist deutlich aufwendiger auszurollen als v1/v2X
  - Bestehende Strukturen auf v1/v2X wurden häufig in eigenen Netzsegmenten geführt
    - meist immer noch.... Portbased-VLAN geht schneller als x.509 Vertrauensverhältnisse :)

Stephan Seitz <s.seitz@heinlein-support.de>

Teil 3:
Setup und Konfiguration

Voraussetzungen

RackTables

- Aktueller LAMP-Stack
  - Idealerweise eine eigene VM
  - Platz benötigt im Wesentlichen nur die MySQL Datenbank
    - auch für grosse Landschaften sehr übersichtlicher Platzbedarf im Wesentlichen bestimmt durch beigestellte Dokumente (PDFs, Bilder, etc...)
  - an MySQL werden keine besonderen Anforderungen gestellt, Version >5.x reicht aus
  - PHP 5 (aktuell ist je nach Distro 5.4 oder bereits 5.5)
    - aus Performanzgründen gerne auch als FPM
    - Installer klärt über wichtige und empfohlene PHP-Module auf
    - einziger Haken kann pcntl (Process-Control) sein. pcntl ist zu Recht auf vielen Distributionen nicht einkompiliert / nicht aktiv / via function_disable eingeschränkt
  - Webserver
    - **kann** Apache sein, lighttpd oder nginx funktionieren ebenfalls
    - rewrite, redirect wird nicht benötigt
- Zugriff auf DNS und natürlich die SNMP Agenten :)

Voraussetzungen

RackTables

- Wahl der Authentisierung
  - Standardmässig (und damit kann man ohne Probleme bereits starten)
    - Benutzer mit (gehashten) Passwörtern in MySQL
  - Vom Installer wird ein „Admin“ Benutzer angelegt
- das erste – und wichtigste – Plugin: „snmpgeneric“

```
git clone https://github.com/github138/myRT-contribs.git
cp myRT-contribs/snmpgeneric.php ../racktables/wwwroot/inc/
cp MyRT-contribs/snmpgeneric.jpg ../racktables/wwwroot/pix/
cat > ../racktables/wwwroot/inc/local.php << EOF
<?php
     include 'inc/snmpgeneric.php';
EOF
# less myRT-contribs/snmpgeneric.php # SQL Kopieren & Ausführen
```

Voraussetzungen

RackTables

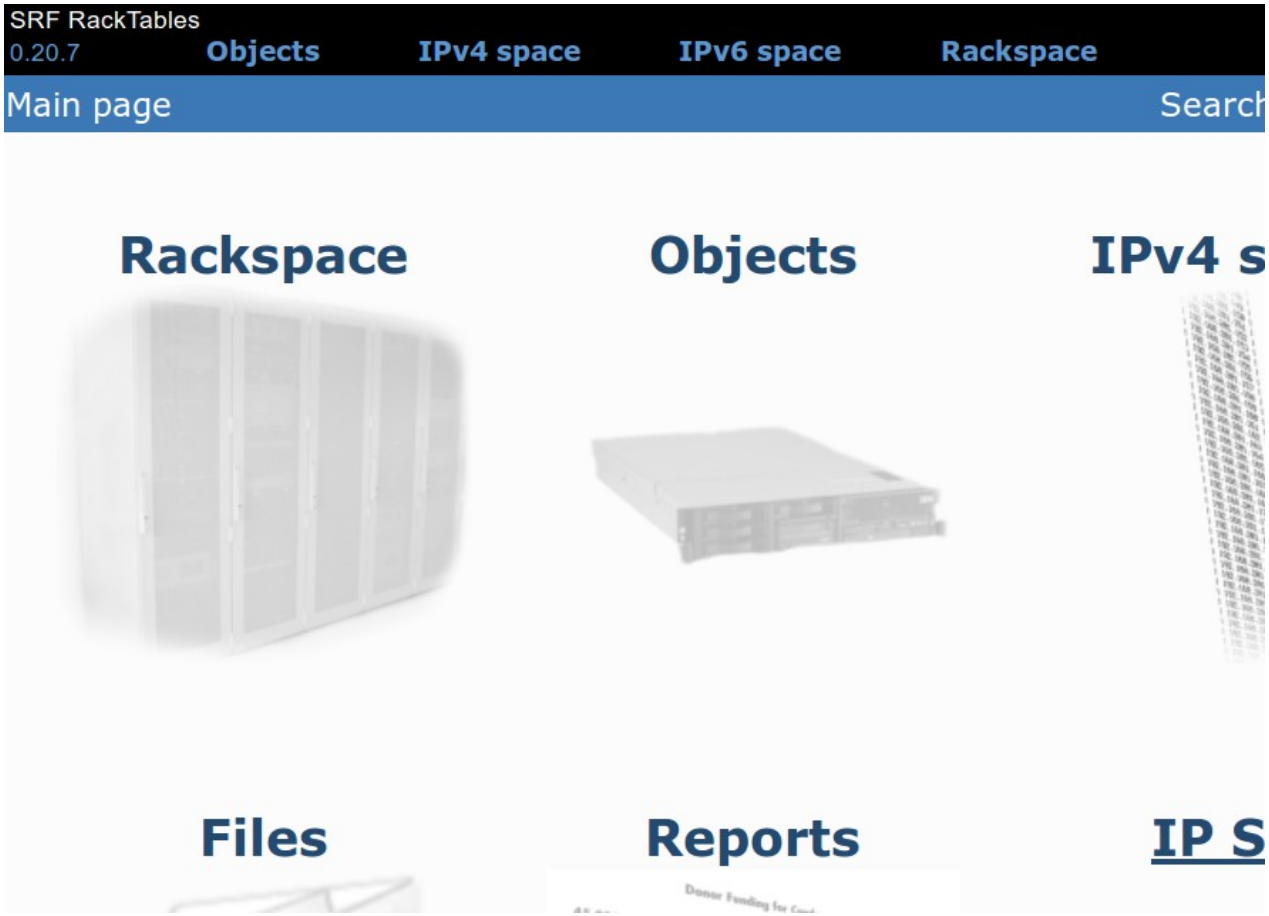
- Abschliessend:
  Alle verfügbaren Dokumente, Bilder, PostIts, Steintafeln, etc...
  - Die Dokumentation muss natürlich aufgebaut werden

Stephan Seitz <s.seitz@heinlein-support.de>

Teil 4:
Der erste Blick auf das neue System

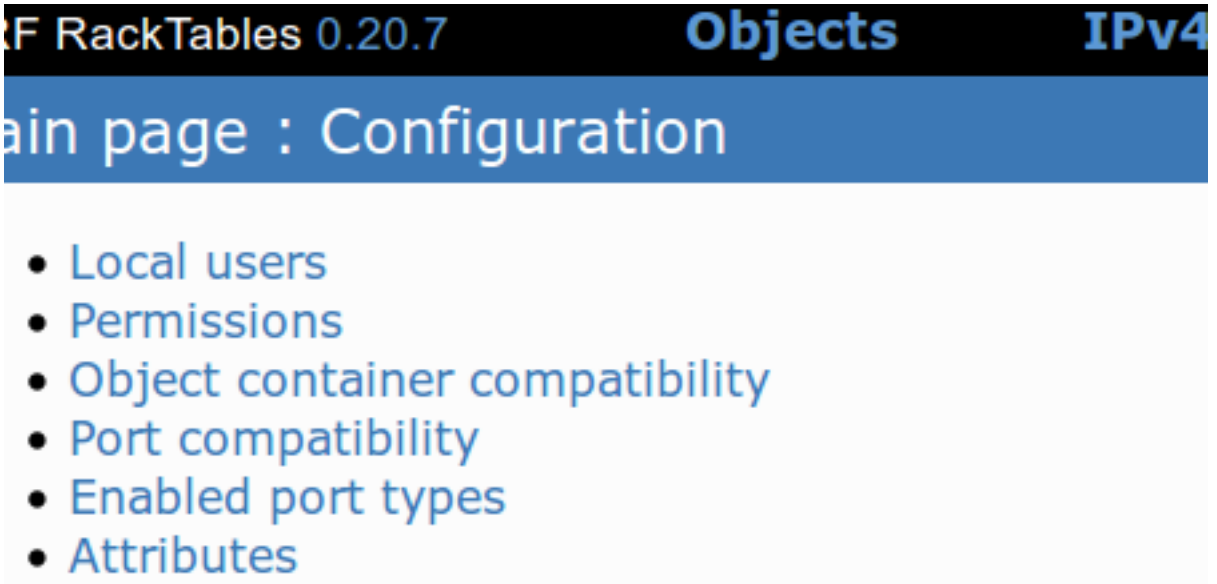
RackTables

- … und los



RackTables

- zuerst Konfigurieren :)



- ... zum interaktiven Teil

Stephan Seitz <s.seitz@heinlein-support.de>

Teil 5:

Dokumentieren mit RackTables (Interaktiv)

Links

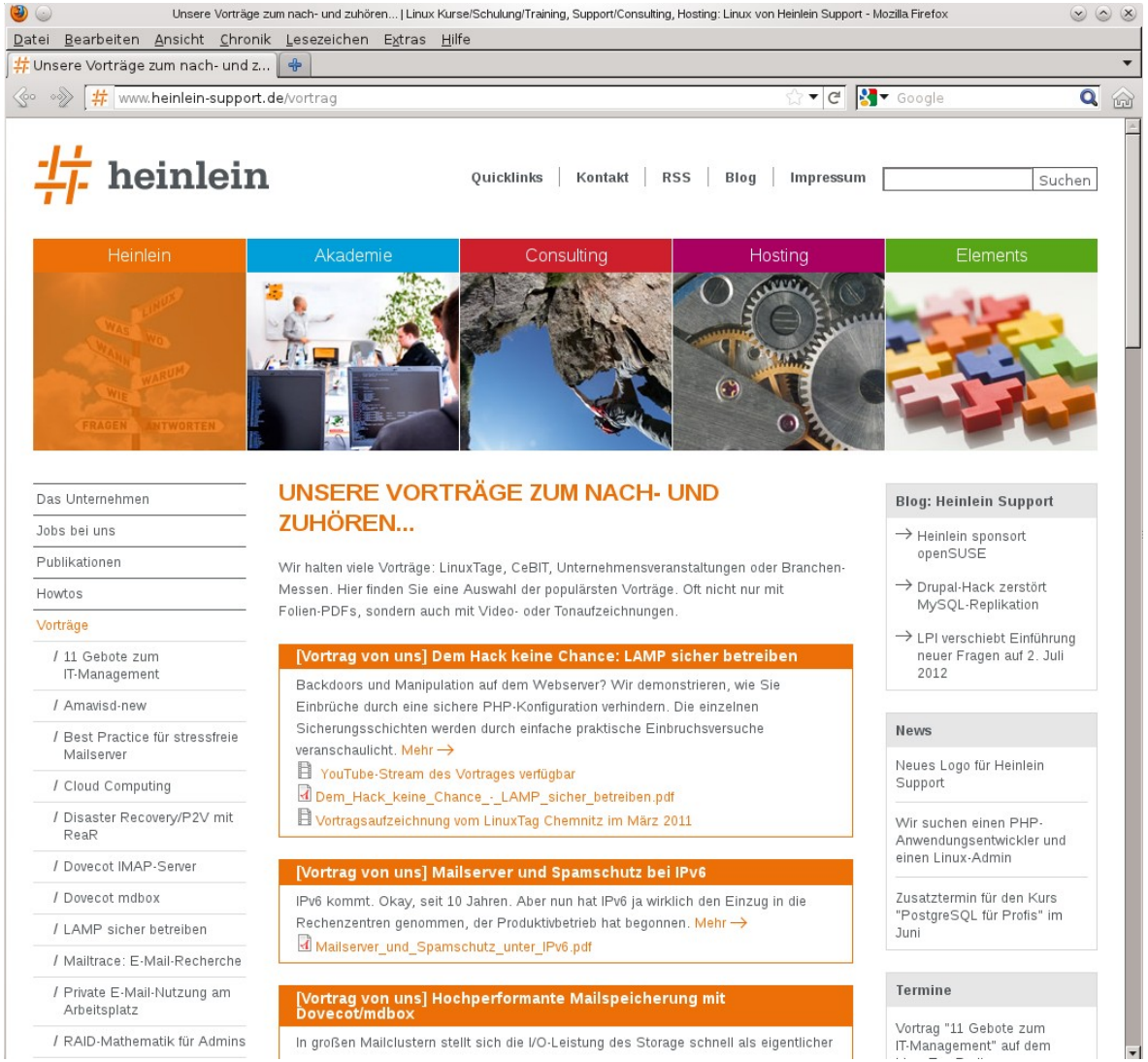
- RackTables
  - http://www.racktables.org/
  - https://github.com/github138/myRT-contribs
    - Repository von <m.ehinger@ltur.de>
  - https://github.com/RackTables/racktables-contribs
    - von den RackTables-Entwicklern gepflegte Sammlung
- SNMP MIBs
  - Am Einfachsten
    - `aptitude install snmp-mibs-downloader`
      zumindest unter Debian / Ubuntu
  - http://www.simpleweb.org/ietf/mibs/
  - http://www.iana.org/
  - http://www.rfc-editor.org/

- Natürlich und gerne stehe ich Ihnen jederzeit mit Rat und Tat zur Verfügung und freue mich auf neue Kontakte.
  - Stephan Seitz
  - Mail: s.seitz@heinlein-support.de
  - Telefon: 030/40 50 51 – 44

- Wenn's brennt:
  - Heinlein Support 24/7 Notfall-Hotline: 030/40 505 - 110

heinlein

Stephan Seitz <s.seitz@heinlein-support.de>



Ja, diese Folien stehen auch als PDF im Netz...
http://www.heinlein-support.de/vortrag

Soweit, so gut.

Gleich sind Sie am Zug:
Fragen und Diskussionen!

Wir suchen:
Admins, Consultants, Trainer!

Wir bieten:
Spannende Projekte, Kundenlob, eigenständige Arbeit, keine Überstunden, Teamarbeit

...und natürlich: Linux, Linux, Linux...

http://www.heinlein-support.de/jobs

Und nun...

- Vielen Dank für's Zuhören...
- Schönen Tag noch...
- Und viel Erfolg an der Tastatur...

Bis bald.

Stephan Seitz <s.seitz@heinlein-support.de>

heinlein

Heinlein Support hilft bei allen Fragen rund um Linux-Server

HEINLEIN AKADEMIE
Von Profis für Profis: Wir vermitteln die oberen 10% Wissen: geballtes Wissen und umfangreiche Praxiserfahrung.

HEINLEIN HOSTING
Individuelles Business-Hosting mit perfekter Maintenance durch unsere Profis. Sicherheit und Verfügbarkeit stehen an erster Stelle.

HEINLEIN CONSULTING
Das Backup für Ihre Linux-Administration: LPIC-2-Profis lösen im CompetenceCall Notfälle, auch in SLAs mit 24/7-Verfügbarkeit.

HEINLEIN ELEMENTS
Hard- und Software-Appliances und speziell für den Serverbetrieb konzipierte Software rund ums Thema eMail.