heinlein

Robert Sander <r.sander@heinlein-support.de>

Netzwerk-Zugangskontrolle mit FreeRADIUS und OpenLDAP

Robert Sander <r.sander@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 17 Mitarbeitern
- Eigener Betrieb eines ISPs seit 1992
- Täglich tiefe Einblicke in die Herzen der IT aller Unternehmensgrößen

Robert Sander <r.sander@heinlein-support.de>

Teil 1:
Motivation

Robert Sander <r.sander@heinlein-support.de>

Sicherheit

- Zugang nur für bekannte Teilnehmer
  - Offene Netzwerk-Dosen in jedem Büro schwer zu überwachen
  - WLAN ist per se offen
- Verschiedene Netzteilnehmer voneinander trennen
  - Mitarbeiter (Software-Entwickler, HR, „Der Rest“)
  - Drucker, VoIP, Switches
  - Partner
  - Gäste
- Netzbereiche durch Firewall getrennt

Robert Sander <r.sander@heinlein-support.de>

Bequemlichkeit

- Offener Zugang in jedem Büro
  - Mitarbeiter können flexibel wechseln
  - Gäste kommen „mal eben“ ins Internet
- Kein Aufwand für Kontrolle + Management der Switchports
  - Einheitliche Konfiguration der Access-Ports
  - Kein Umpatchen, weil der Teilnehmer wechselt
  - Weniger Admin-Aufwand

Robert Sander <r.sander@heinlein-support.de>

Teil 2:

Grundlagen

Robert Sander <r.sander@heinlein-support.de>

Virtual Local Area Network (VLAN)

- Tagged VLAN (802.1q): Ethernetpakete tragen VLAN-ID
- Tagged Port: Der Teilnehmer übergibt Pakete mit Tag
- Untagged Port: Der Switch weist Tag zu, nicht der Teilnehmer

- Mehrere Netzsegmente können so über einen Switch laufen
  - Tagged Ports zwischen Switches = Trunk mit mehren VLANs
- Zuordnung auf Port-Ebene (statisch oder dynamisch)
- Verkehr zwischen VLANs benötigt Router
  - So wie zwischen LANs

Robert Sander <r.sander@heinlein-support.de>

Remote Authentication Dial-In User Service (RADIUS)

- Authentifiziert Einwahlverbindungen
  - Modem, ISDN, DSL
  - Aber auch WLAN und LAN (z.B. per 802.1X)
- Erhält vom Remote Access Server (Authentikator) Logindaten
  - Benutzername + Passwort
  - Zertifikat
- Überprüft Anmeldedaten mittels PAP, CHAP oder EAP
  - Interne Datenbank (Textdatei)
  - Externe Datenbank (SQL, LDAP)
- Kurze Nachrichten, schnelles Antwortverhalten
  - Daten zum Authentikator in Access-Accept-Antwort

Robert Sander <r.sander@heinlein-support.de>

Extensible Authentication Protocol (EAP)

- RFC3748
- WPA2 Enterprise mit Zertifikaten (802.11i, EAP-TLS)
- Supplicant (Netzwerk-Teilnehmer, z.B. `wpa_supplicant`) fragt
- Authentikator (Switch / WLAN-Controller), der ist Vermittler zu
- Authentisierungs-Server (z.B. FreeRADIUS)

- Eine Certificate Authority signiert Server- und TN-Zertifikate
- Teilnehmer kann Server, Server muß Teilnehmer überprüfen

Robert Sander <r.sander@heinlein-support.de>

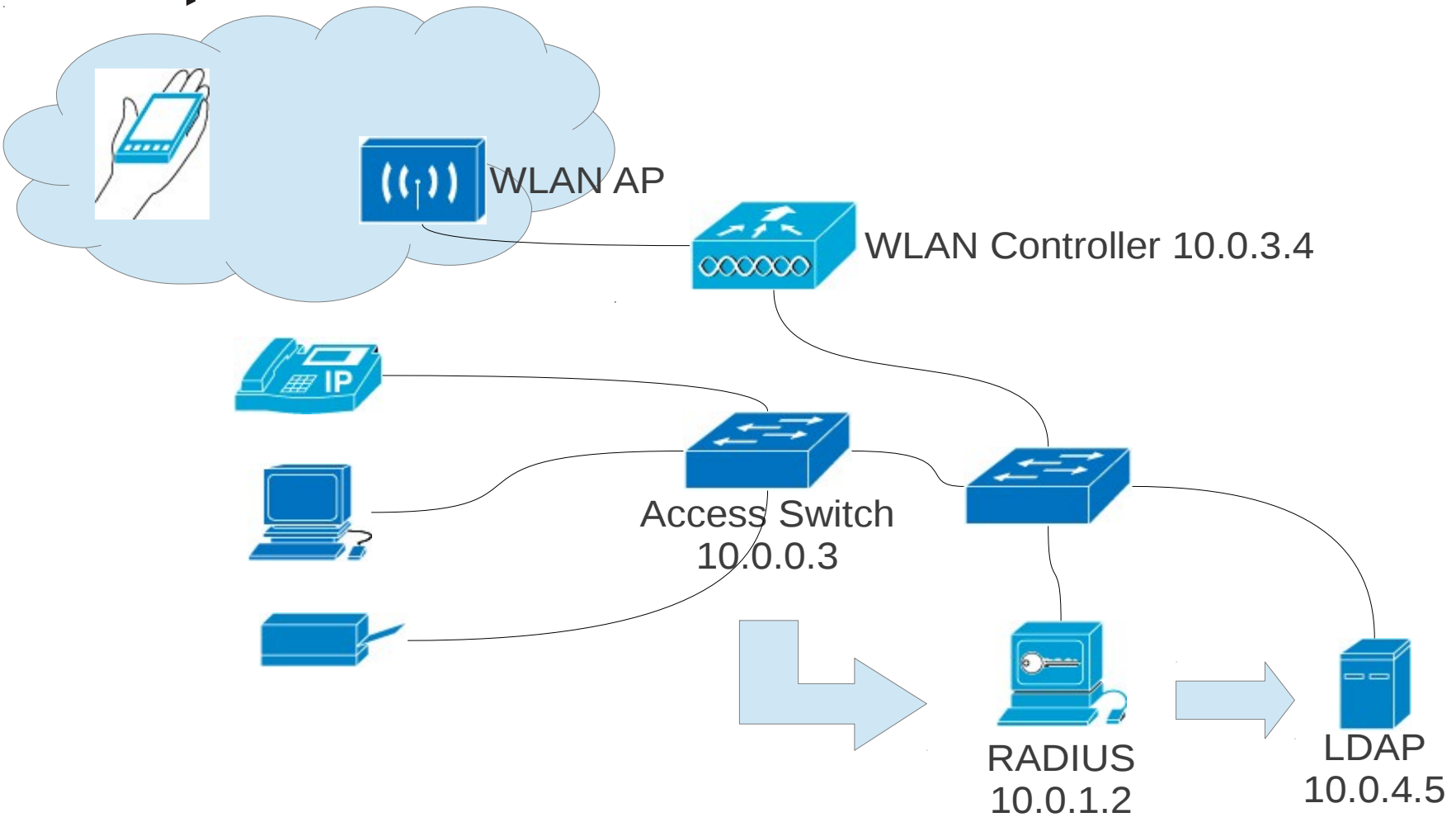
Lightweight Directory Access Protocol (LDAP)

- Verzeichnisdienst mit Baumstruktur
- Flexible Schemata
  - Alle benötigten Informationen an einer Stelle
- Schnelles Lookup (mit entsprechenden Indices)
- Replikation (Ausfallsicherheit)

- Meist schon für Accounts und Hosts vorhanden

Robert Sander <r.sander@heinlein-support.de>

Konzept - Übersicht



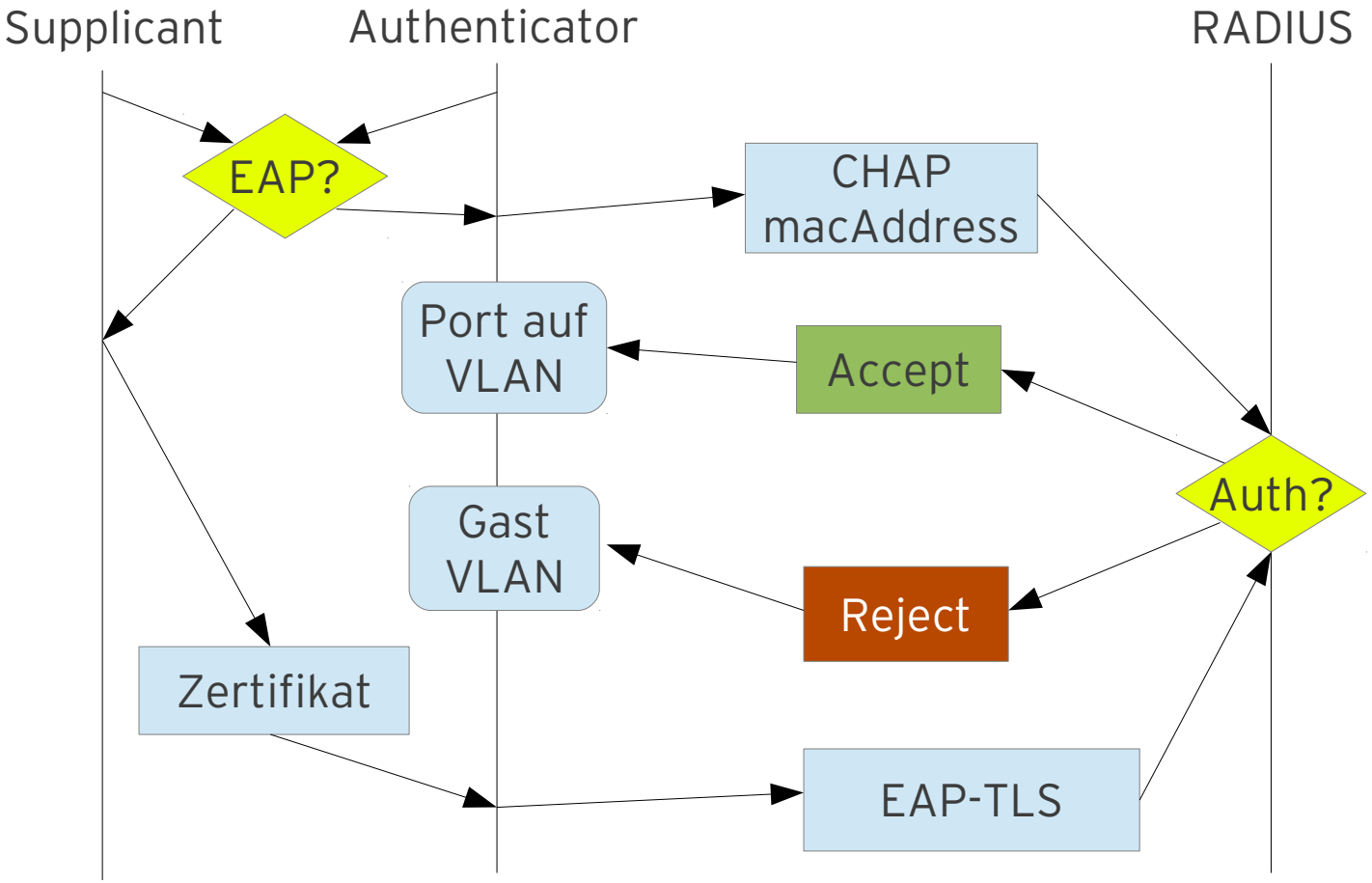
Robert Sander <r.sander@heinlein-support.de>

Teil 3:

Umsetzung

Robert Sander <r.sander@heinlein-support.de>

Ablauf



Robert Sander <r.sander@heinlein-support.de>

Access Switches & WLAN Controller

- Stichworte:
  - 802.1X bzw. RADIUS
  - Port Access Security (evtl. MAC based)
  - VLANs (802.1q)
- RADIUS Server eintragen
  - IP-Adresse + Kennwort (Switch meldet sich bei RADIUS-Server an)
- Port Access
  - MAC-based
    - Benutzername & Kennwort = MAC-Adresse (Schreibweise!)
    - CHAP (d.h. Challenge-Response-Verfahren)
  - 802.1X
    - Zertifikat vom Teilnehmer (Identifikation im commonName-Attribut)

Robert Sander <r.sander@heinlein-support.de>

Beispiel: HP ProCurve Switches

- Port-Access:

```
radius host 10.0.1.2 key S3cr3tPW

aaa port-access mac-based <port range>
aaa port-access mac-based <port range> addr-limit 1
aaa port-access mac-based <port range> unauth-vid <Gast-VLAN-ID>
aaa port-access mac-based addr-format multi-colon

aaa port-access authenticator <port range>
aaa port-access authenticator client-limit <port range> 1
aaa port-access authenticator <port range> unauth-vid <Gast-VLAN-ID>
aaa port-access authenticator active
```

- http://wiki.freeradius.org/vendor/HP

Robert Sander <r.sander@heinlein-support.de>

freeRADIUS Authenticators

- /etc/freeradius/clients.conf
  - RADIUS-Clients, also Switches & WLAN-Controller

```
client 10.0.0.3 {
     secret            = S3cr3tPW
     shortname         = access-switch
     virtual_server    = default
}

client 10.0.3.4 {
     secret            = 5up3rPW
     shortname         = wlan-controller
     virtual_server    = default
}
```

Robert Sander <r.sander@heinlein-support.de>

freeRADIUS Auth-Methoden

- /etc/freeradius/sites-enabled/default

```
authorize {
     preprocess
     chap
     eap {
          ok = return
     }
     suffix
     redundant-load-balance {
          ldap1
          ldap2
     }
     files
}
```

```
authenticate {
     Auth-Type CHAP {
          chap
     }
     eap
}
```

Robert Sander <r.sander@heinlein-support.de>

freeRADIUS LDAP Anbindung

- /etc/freeradius/modules/ldap
  - Verbindung zum LDAP (ldap2 dann analog zu ldap1 mit anderer IP)

```
ldap ldap1 {
     server = "10.0.4.5"
     basedn = "dc=example,dc=com"
     filter = "(|(cn=%{%{Stripped-User-Name}:-%{User-Name}})
                 (macAddress=%{%{Stripped-User-Name}:-%{User-Name}}))"
     ldap_connections_number = 5
     timeout = 4
     timelimit = 3
     net_timeout = 1
     set_auth_type = no
     dictionary_mapping = ${confdir}/ldap.attrmap
}
```

```
checkitem     Cleartext-Password     macAddress
```

Robert Sander <r.sander@heinlein-support.de>

freeRADIUS EAP

- /etc/freeradius/eap.conf
  - Konfiguriert die verschiedenen EAP-Methoden
- `private_key_password` von `server.key` muß gesetzt werden
- Ebenso in /etc/freeradius/modules/inner-eap
  - Für EAP-TTLS und PEAP (MS CHAPv2)
  - /etc/freeradius/sites-enabled/inner-tunnel

- http://wiki.freeradius.org/protocol/EAP

Robert Sander <r.sander@heinlein-support.de>

freeRADIUS Zertfikate & CA

- /etc/freeradius/certs/
  - CA, Teilnehmer-Zertifikate (kann aber auch extern sein)
- `*.cnf` Konfiguration inkl. Passwörter für private Keys
- `Makefile` zum Generieren der Zertifikate
  - Ändern von `client.cnf` für ein neues Teilnehmer-Zertifikat
  - commonName = cn des Hosts im LDAP
  - `make client.pem` erzeugt Zertifikatsdatei

Robert Sander <r.sander@heinlein-support.de>

freeRADIUS statische Defaults

- /etc/freeradius/users

```
DEFAULT Auth-Type == Accept
              Tunnel-Type = 13,           # VLAN
              Tunnel-Medium-Type = 6,     # IEEE-802
```

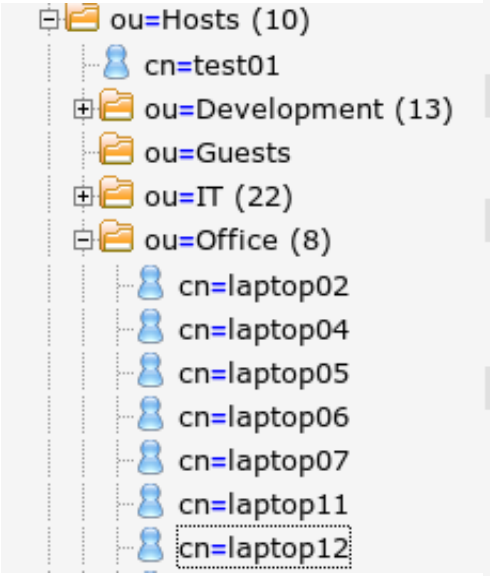
Robert Sander <r.sander@heinlein-support.de>

OpenLDAP

- radiusprofile objectClass hinzufügen
- radiusTunnelPrivateGroupId = VLAN-ID
- macAddress
  - Schreibweise: Kleinbuchstaben und mit Doppelpunkt getrennt (12:34:56:78:9a:bc)
- cn = commonName aus Zertifikat
- userPassword wird in diesem Szenario nicht benötigt
  - keine Benutzer-Auth, sondern Maschinen
  - außerdem liegt es nicht im Klartext vor, kein CHAP möglich
  - anonymous Bind sollte also meistens ausreichen

OpenLDAP - Organisation

- organizationalUnit als VLAN-Container
  - RadiusTunnelPrivateGroupId gesetzt
- Host-Einträge unterhalb von organizationalUnits
- Skript automatisiert per Cronjob
  - Host-Einträge „erben“ radiusTunnelPrivateGroupId von ou
- Verschieben von Host-Eintrag ändert VLAN



Robert Sander <r.sander@heinlein-support.de>

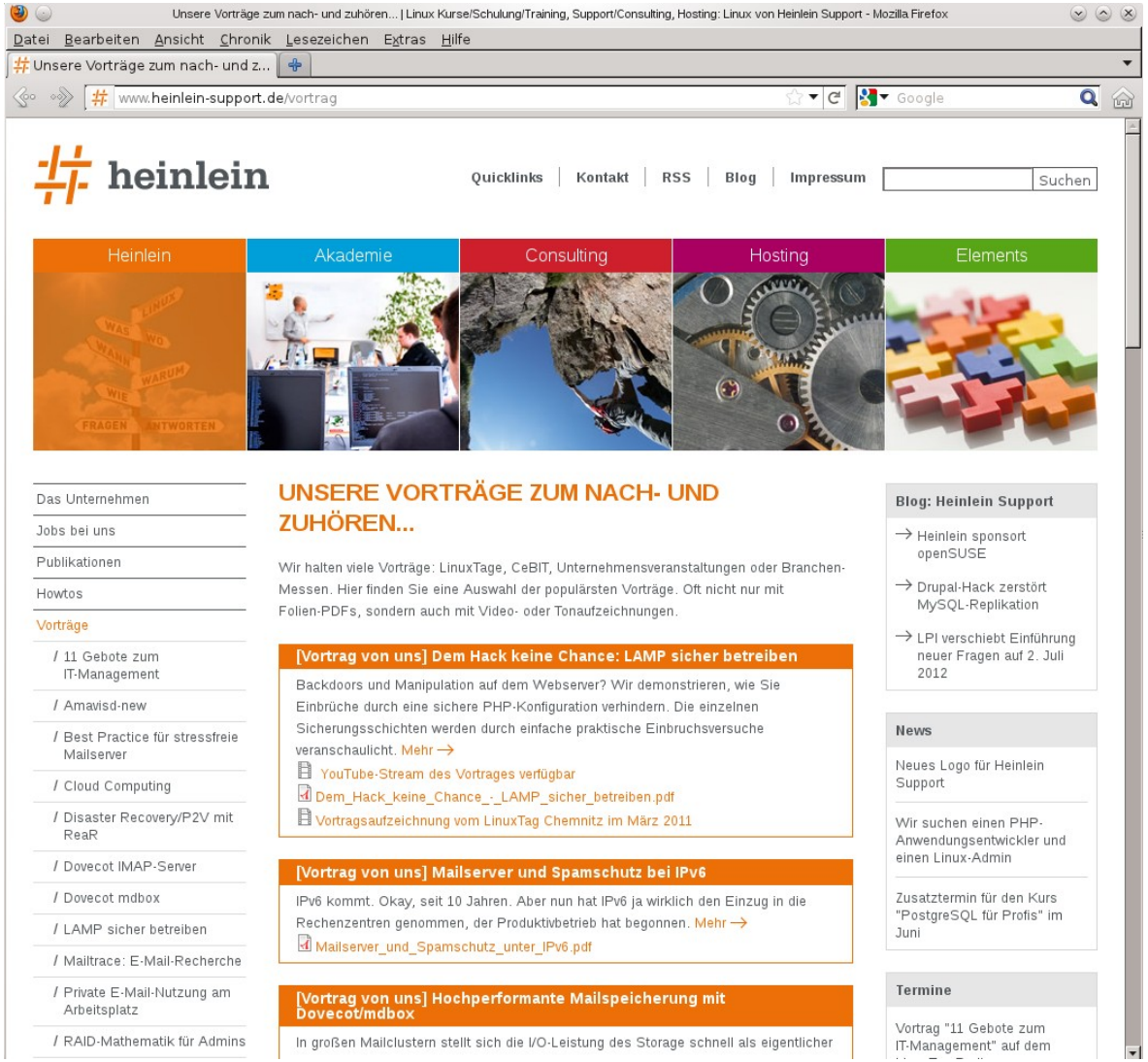
Zusammenfassung

- FreeRADIUS und openLDAP sind ein prima Team
- Netzwerkzugangskontrolle ist nicht schwierig
- Ermöglicht „plug'n'play“ Netzwerke
- Sichere Authentifizierung mittels Zertifikaten
  - ggfs. auch per MAC-Adresse möglich

- Natürlich und gerne stehe ich Ihnen jederzeit mit Rat und Tat zur Verfügung und freue mich auf neue Kontakte.
  - Robert Sander
  - Mail: r.sander@heinlein-support.de
  - Telefon: 030/40 50 51 – 43
- Wenn's brennt:
  - Heinlein Support 24/7 Notfall-Hotline: 030/40 505 - 110

heinlein

Netzwerk-Zugangskontrolle
[CLT 2013]
Robert Sander <r.sander@heinlein-support.de>



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

Robert Sander <r.sander@heinlein-support.de>

Soweit, so gut.

Gleich sind Sie am Zug:
Fragen und Diskussionen!

Robert Sander <r.sander@heinlein-support.de>

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

Robert Sander <r.sander@heinlein-support.de>

Und nun...

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

Bis bald.

heinlein

Netzwerk-Zugangskontrolle
[CLT 2013]
Robert Sander <r.sander@heinlein-support.de>

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.