

NetDot und RANCID

Jens Link

jl@jenslink.net

NetDot und RANCID

1 Dokumentation

2 netdot

3 Rancid

- Freiberuflicher Consultant
- komplexe Netzwerke
- Netzwerksecurity
- Netzwerkmonitoring
- Troubleshooting

Übersicht

- 1 Dokumentation
- 2 netdot
- 3 Rancid

Dokumentation?! (I)

- Wichtig!
- Aber wird sie auch gemacht?
- Wann?
- Wird sie auch gepflegt?
- Wirklich? ;-)

Wie wird dokumentiert?

- Doku existiert im Kopf des Admins
- Office-Dateien, per eMail verschickt, ohne Datum und Versionsnummern
- Wiki / Ticketsysteme / ...
- T-Shirt ;-)

Probleme:

- Pflege von Doku - Keiner macht es gerne, es gibt immer “wichtigeres” zu tun
- Änderungen “mal eben schnell” werden auch schnell wieder vergessen
- Daten werden mehr als einmal gepflegt

Mögliche Lösungen:

- Praktikant / Azubi
- Tools!

Übersicht

- 1 Dokumentation
- 2 netdot
- 3 Rancid

- Vieles geht automatisch
- Device Discovery via SNMP
- Layer2 Topologie (CDP / LLDP), Spanning-Tree, Forwarding-Tables,
- IPv4 / IPv6 Adressverwaltung
- Verkabelung
- Kontakte

Voraussetzungen:

- Perl
- diverse Sachen aus CPAN
- Apache /Mod-Perl
- MySQL / Postgres

Vorteile gegenüber anderen Tools:

- Freie Software
- Sehr aktive Entwicklung und Mailingliste
- Klare Roadmap
- Vorschläge und Patches werden angenommen

- **CDP** - Cisco Discovery Protocol
- **LLDP** - Link Layer Discovery Protocol

Erkennen von Layer-2 Verbindungen **ohne** funktionierende Layer-3 Kommunikation.

```
r3#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID      Local Intrfce   Holdtme    Capability   Platform   Port ID
r2             Fas 1/0        139        R S I       3640       Fas 1/0
r1             Fas 0/0        145        R S I       3640       Fas 2/0
```

- Kein fertiges Paket bekannt
- Installation aber recht einfach
- **Nett:** `make installdeps-apt-get`

Übersicht

- 1 Dokumentation
- 2 netdot
- 3 Rancid**

- Really Awesome New Cisco config Differ
- Kann mehr als nur Cisco
- Mischung aus Expect, Shell, Perl, awk,
- Liest Konfiguration eines Gerätes per ssh / telnet aus
- Speichert als Textdatei und im CVS / SVN (/ GIT)
- Verschickt bei Änderungen Mails
- Erkennt auch Änderungen an der Hardware (z.B. Austausch eines SFPs)
- Probleme: Passwörter werden u.U. nicht mit gespeichert, ebenso evtl. Crypto-Keys, ...

Rancid (II)

Konfiguration:

rancid.conf

```
TERM=network; export TERM
umask 027
TMPDIR=/tmp; export TMPDIR
BASEDIR=/var/lib/rancid; export BASEDIR
PATH=/usr/lib/rancid/bin:/usr/bin:/usr/sbin:/bin:/usr/local
export PATH
CVSROOT=$BASEDIR/SVN; export CVSROOT
LOGDIR=$BASEDIR/logs; export LOGDIR
RCSSYS=SVN; export RCSSYS
ACLSORT=YES; export ACLSORT
OLDTIME=4; export OLDTIME
LIST_OF_GROUPS="lan"
```

Konfiguration:

```
/etc/aliases
```

```
....
```

```
rancid-lan: jens  
rancid-admin-lan: jens
```

Initialisierung:

```
netdot:/var/lib/rancid# bin/rancid-cvs
```

Konfiguration:

lan/router.db

```
192.0.2.1:cisco:up
192.0.2.10:cisco:up
192.0.2.15:cisco:up
192.0.2.17:cisco:down
192.0.2.99:cisco:up
192.0.2.100:juniper:up
```

.cloginrc

```
add user 192.0.2.0/24          admin
add password 192.0.2.0/4      {geheim}          {secret}
add method 192.0.2.0/24      ssh telnet
```

clogin (I)

```
jens@netdot:~$clogin -c '"sh cdp neigh" 192.0.2.10
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
```

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
r2	Fas 1/0	139	R S I	3640	Fas 1/0
r1	Fas 0/0	145	R S I	3640	Fas 2/0

clogin (II)

Neuer NTP-Server:

```
jens@netdot:/var/lib/ranci#bin/clogin -c \  
"conf t; no ntp server 10.10.20.10;  
 ntp server 10.10.10.9; end; wr; " \  
192.0.2.1 192.0.2.15 192.0.2.17
```

*..I have noticed a behaviour change since implementing RANCID. The entire NOC team gets an email when a config change is made. The result is everyone is cautious about making changes on the fly, and any changes that are made are quickly explained by the changer. Before, changes would be made and if it broke something.....silence. So, at the very least we have fewer ****problems**** that magically appear. – Jason Lewis*