Geräte im Netz, die Spectrum *nicht* kennt.

Dr. Michael Schwartzkopff, sys4 AG

sys4 AG

Enterprise Experts

Was wir machen ...

- Wir lösen komplexe Probleme.
- Wir entwickeln maßgeschneiderte Lösungen basierend auf etablierten Standards.
- Wir wissen, welche Open Source Werkzeuge passen und verlässlich sind.
- Unsere Teams bestehen aus bekannten Experten.

Motivation

- Spectrum ist ein nettes Monitoring Tool.
- Aber Spectrum hat keine Informationen, über Geräte im Netzwerk, die es *nicht* verwaltet.
- Es gibt deshalb keinen Bericht:
  „Alle Geräte im Netz, die nicht modelliert sind“.
- Manchmal will der Admin aber genau das wissen.

3 Schritte zum Durchblick

- In diesem Vortrag präsentiere ich ein `perl` Script, das genau diese Informationen liefert.
  - 1. Schritt: Welche Geräte kennt Spectrum?
  - 2. Schritt: Die Umgebung von Geräten.
  - 3. Schritt: Das Programm

Abfrage von Geräten

- Spectrum bietet eine API, über die man Informationen abfragen kann.
- Die URL ist: *http://$specserver/spectrum/restful/devices*
- Es gibt eine gute Doku für die API.
- Die API liefert die Informationen in XML.
- Für uns: Abfrage der Attribute Name (0x1006e) und IP Adresse (0x12d7f).

Abfrage der API über `perl`

- Ich mache `wget`, weil mein RHEL die passende Bibliothek nicht hat:

```
@args = ("wget", "--http-user=$user", \
  "--http-password=$pass", "-O devices.xml", \
  "http://$specserver/spectrum/restful/devices?\
  attr=0x1006e&attr=0x12d7f");

system(@args) == 0 or die "system @args failed: $?";
```

Parsen der Ausgabe der API

- RHEL hat sehr wohl eine Bibliothek zum Parsen von XML (`XML::Simple`).
- Das Ergebnis liegt als Array of Hashes vor:

```
my $xml = new XML::Simple;

my $device = $xml->XMLin("devices.xml");

foreach (@{$device->{'model-responses'}->{'model'}}) {
 $devhash {$_->{'attribute'}->{'0x1006e'}->{'content'}}
  = $_->{'attribute'}->{'0x12d7f'}->{'content'};
}
```

Die Umgebung von Geräten

- Wie erfahre ich von bekannten Geräten, welche anderen Geräte es gibt?
  -> Cisco Discovery Protocol!

- LLDP, FDP, ARP Table, ARP Cache, Routing Table gehen auch.

Abfrage aller Geräte

- Alle CDP Informationen kann man per SNMP abfragen:

```
# CDP MIB ist ciscoMgmt.23

$CDPOID = "1.3.6.1.4.1.9.9.23.1.2.1.1.6";

snmpwalk $device $CDPOID
```

- Für die anderen Informationen gibt es auch MIBs.

`snmpwalk` liefert eine Liste

- `snmpwalk` liefert eine Liste aller Nachbarn, die ein bekanntes Gerät kennt.
- Diese Liste wird nach unbekannten Geräten durchsucht:

```
foreach $neighbour ( @resultlist ) {
  $neighbour =~ s/["\x0D\x0A]//g;
  print "$key: $neighbour\n"
    if !exists $devhash {$neighbour};
}
```

Programm: Pseudo Code

Read all known devices via API: `$devicelist`

Loop each `$device` in `$devicelist`

 `snmpwalk $device $CDPOID: $neighborlist`

 Loop each `$neighbor` in `$neighborlist`

  Print `$neighbor` if not in `$devicelist`

 End loop `$neighborlist`

End loop `$devicelist`

Programm

- Vollständige Beschreibung unter http://sys4.de/de/blog/2013/11/05/detect-devices-spectrum-doesnt-know

Verbesserungen

- `wget` ersetzen durch `perl` Funktion.
- `snmpwalk` ersetzen durch `perl` Funktion.
- Liste der Nachbarn normalisieren.
- Einlesen der anderen Umgebungsinformationen: LLDP, ...
- Verbesserung des Parsings:
  - z.B. liefern Cisco Nexus ihre Seriennummer anstelle des Systemnamens.

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Michael Schwartzkopff
ms@sys4.de