SNMP Applied

SNMP-Monitoring planen, konfigurieren und integrieren

Gerrit Beine

mail@gerritbeine.com

Motivation:
Warum dieser Vortrag?

Ich habe mir seit Jahren gewünscht,
dass mir jemand SNMP erklärt...

Ziele des Vortrags

- Überblick zu SNMP liefern
- Grundlegende Anwendung von Net-SNMP erklären
- Erstellen eigener SNMP Traps mit Perl
- Zusammenspiel von SNMP und Nagios beleuchten

Grundlegendes zu SNMP

SNMP

- Simple Network Management Protocol
  - Verwendet UDP, Ports 161 und 162
- Historie
  - Version 1 (1988) Ursprüngliche Spezifikatin in RFC 1155-1157
  - Secure SNMP (1992) RFC1351-1353, nie offiziell eingeführt
  - Party-based SNMP (1993, SNMPv2p) RFC 1441, 1445-1447, führte getbulk ein, erhöhte Sicherheit, heute nicht mehr im Einsatz
  - User-based SNMP (1996, SNMPv2u) RFC 1909-1910, heute nicht mehr im Einsatz
  - Community-based SNMP (1996, SNMPv2c) RFC 1901, 1905-1906, Erweiterung von Version 1 um Features aus SNMPv2p
  - Version 3 (2002), RFC 3410-3418, Fokus auf Sicherheit

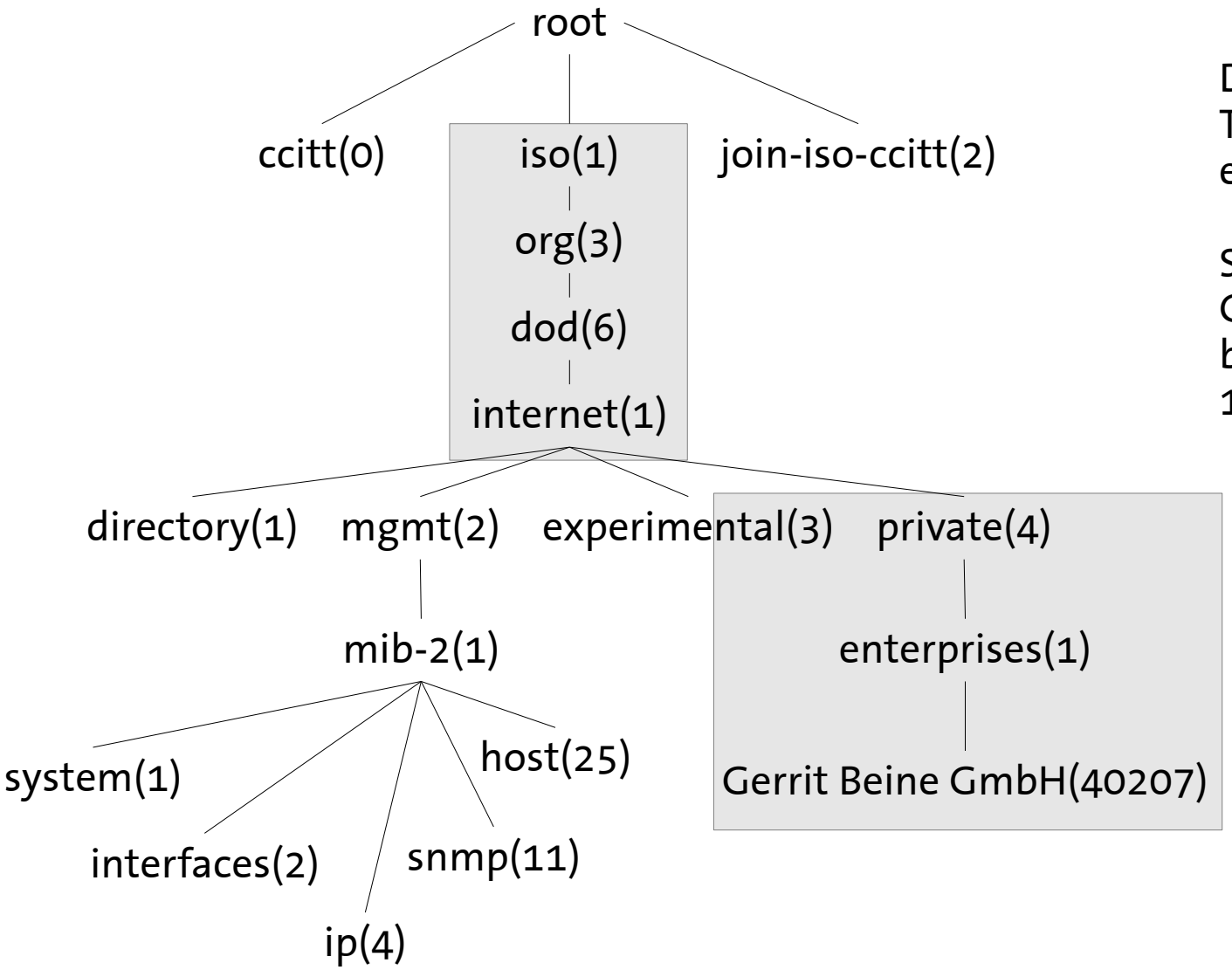
Anwendungen von SNMP

- Kontinuierliches Monitoring (Polling)
  - Uptime, Load
  - Netzwerkverkehr
  - Speicherverbrauch (RAM, Festplatten)
  - Hardware-Zustand (S.M.A.R.T., Lüfterdrehzahl)
- Information über Ereignisse (SNMP-Traps)
  - Fehlersituationen
  - Zustandswechsel

SNMP Begriffswelt

- Agent – SNMP-Daemon, der Informationen via UDP 161 bereitstellt oder Traps via UDP 162 versendet
- Manager – SNMP-Client, der Informationen via UDP 161 einsammelt
- Trap – SNMP-Nachricht, über UDP 162 versendet
- MIB – Management Information Base
  - Dateien mit strukturiertem Text nach ASN.1
  - Beschreiben Monitoring-Objekte
  - Übersetzen OIDs in Namen und interpretieren der entsprechenden Werte
- OID – Object Identifier
  - Identifikatoren in durch ASN.1 definiertem Namensraum
- community – in SNMP Version 1 und SNMPv2c zur Anmeldung am Agent verwendet

Der MIB-Baum



Die Position im MIB-Tree liefert den OID eines Objektes.

SNMP-Objekte der Gerrit Beine GmbH beginnen immer mit 1.3.6.1.4.1.40207.

OID: Object Identifier

- OID's sind eindeutige Identifikatoren innerhalb eines Agenten bzw. eines Gerätes
- OID's navigieren durch SNMPs MIB-Baum
- Hersteller-spezifische OID's immer unterhalb von 1.3.6.1.4.1
- Mapping auf Domains
  - 1.3.6.1.4.1.40207 – gerritbeinegmbh.enterprises.private.internet.dod.iso.org.
- Unterhalb der OID ist jeder Hersteller frei in seinen Definitionen
- Zuweisung der Enterprise-Identifkation erfolgt durch die IANA: http://www.iana.org/assignments/enterprise-numbers

MIB internet (1.3.6.1)

- directory(1) – OSI Verzeichnis
- mgmt(2) – RFC Standard Objekte
- experimental(3) – Experimente
- private(4) – MIB's von Herstellern bzw. Unternehmen
- security(5) – Sicherheitsrelevante MIB's
- snmpV2(6) – SNMP Version 2 interne MIB's

Net-SNMP

Net-SNMP

- OpenSource SNMP Implementierung (CMU, BSD-Like)
- Läuft auf fast allen Unix- und Linux-Systemen
- Unterstützt SNMP Version 1, SNMPv2c, SNMPv3 via IPv4 und IPv6
- Kommandozeilenapplikationen zu
  - Abfrage von SNMP-Agents (snmpget, snmpwalk, ...)
  - Ändern von Konfigurationen via SNMP (snmpset)
  - Übersetzen von OID's (snmptranslate)
- Daemon zum Empfangen von SNMP Traps (snmptrapd)
- Daemon als SNMP Agent (snmpd)
- C- und Perl-API's
- Zu finden hier: http://www.net-snmp.org/

Net-SNMP snmpd konfigurieren

- Minimale Konfiguration definiert Standort, Kontakt und erlaubt Auslesen

```
# /etc/snmp/snmpd.conf
syslocation Server Room
syscontact Sysadmin (root@localhost)

# allow localhost read-only access via community public
rocommunity public 127.0.0.1
# allow whole network read-only access via community public
rocommunity public 172.16.166.0/24
# allow localhost read-write access via community mysecret
# rwcommunity mysecret 127.0.0.1
```

- Abfrage des snmpd erfolgt via snmpwalk

```
~ gbeine$ snmpwalk -c public -v1 172.16.166.129
SNMPv2-MIB::sysDescr.0 = STRING: Linux linux-dwoa 3.1.10-1.16-default #1 SMP
Wed Jun 27 05:21:40 UTC 2012 (d016078) x86_64
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (635449) 1:45:54.49
SNMPv2-MIB::sysContact.0 = STRING: Sysadmin (root@localhost)
SNMPv2-MIB::sysName.0 = STRING: linux-dwoa
SNMPv2-MIB::sysLocation.0 = STRING: Server Room
...
```

Net-SNMP snmptrapd konfigurieren

- Minimale Konfiguration nimmt alle Traps entgegen

```
# /etc/snmp/snmptrapd.conf

# allow community public
authCommunity log,execute,net public
```

- snmptrapd im Vordergrund starten

```
linux-dwoa:~ # snmptrapd -f -Le
NET-SNMP version 5.7.1
```

Traps in SNMP Version 1

- Allgemeine Aufrufsyntax

```
snmptrap -v 1 -c public
[-Ci] # Antwort des Trap Daemon anfordern
host # Host oder IP des Trap Daemon
Enterprise-oid # OID des MIB, numerisch oder als Text
agent # Informationen zum Sender, zumeist ""
generic trap # Wert von 0-6, 6 bedeutet "enterpise", 0-5 sind fest definiert
specific trap # Wenn generic trap = 6, wird spezifischer Trap Type erwartet
uptime # Uptime-Informationen, zumeist ""
[oid type value] # Inhalte der Trap
```

- Versand einer Beispiel SNMP Trap über SNMPv2c

```
~ gbeine$ snmptrap -v 1 -c public 172.16.166.129 \
NET-SNMP-EXAMPLES-MIB::netSnmpExampleHeartbeatNotification "" 6 17 "" \
netSnmpExampleHeartbeatRate i 123456
~ gbeine$
```

- Empfang einer Beispiel SNMP Trap über SNMP Version 1

```
2012-08-22 20:47:38 192.168.99.18(via UDP: [172.16.166.1]:53901-
>[172.16.166.129]:162) TRAP, SNMP v1, community public
        NET-SNMP-EXAMPLES-MIB::netSnmpExampleHeartbeatNotification Enterprise
Specific Trap (17) Uptime: 3 days, 8:42:36.98
        NET-SNMP-EXAMPLES-MIB::netSnmpExampleHeartbeatRate = INTEGER: 123456
```

Traps in SNMPv2c

- Allgemeine Aufrufsyntax

```
snmptrap -v 2c -c public
[-Ci] # Antwort des Trap Daemon anfordern
host # Host oder IP des Trap Daemon
uptime # Uptime-Informationen, zumeist ""
trap-oid # OID des MIB, numerisch oder als Text
[oid type value] # Inhalte der Trap
```

- Versand einer Beispiel SNMP Trap über SNMPv2c

```
~ gbeine$ snmptrap -v 2c -c public 172.16.166.129 "" \
NET-SNMP-EXAMPLES-MIB::netSnmpExampleHeartbeatNotification  \
netSnmpExampleHeartbeatRate i 123456
~ gbeine$
```

- Empfang einer Beispiel SNMP Trap über SNMPv2c

```
2012-08-22 20:47:17 <UNKNOWN> [UDP: [172.16.166.1]:63927-
>[172.16.166.129]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (29053542) 3 days,
8:42:15.42  SNMPv2-MIB::snmpTrapOID.0 = OID: NET-SNMP-EXAMPLES-
MIB::netSnmpExampleHeartbeatNotification     NET-SNMP-EXAMPLES-
MIB::netSnmpExampleHeartbeatRate = INTEGER: 123456
```

SNMP-Traps mit Perl

SNMP Traps mit Perl (via Net::SNMP) - I

```
 1 #!/usr/bin/perl
 2
 3 use strict;
 4 use warnings;
 5
 6 use Net::SNMP qw(:snmp :asn1);
 7
 8 my $host = '172.16.166.129';
 9 my $port = 162;
10 my $version = 'snmpv1';
11 my $community = 'public';
12
13 my ($session, $error) = Net::SNMP->session(
14          -hostname    => $host,
15          -port        => $port,
16          -version     => $version,
17          -community   => $community
18 );
19
20 if (!defined($session)) {
21     printf("ERROR: %s.\n", $error);
22     exit 1;
23 }
24
```

SNMP Traps mit Perl (via Net::SNMP) - II

```
25 # translated via
26 # 'snmptranslate -On NET-SNMP-EXAMPLES-
MIB::netSnmpExampleHeartbeatNotification'
27 my $svSvcName = '.1.3.6.1.4.1.8072.2.3.0.1';
28 my $message = '123456';
29 my @oids = ($svSvcName, INTEGER, $message);
30
31 my $result = $session->trap(
32          -agentaddr    => '172.16.166.2',
33          -varbindlist  => \@oids
34 );
35
36 if (!defined($result)) {
37     printf("ERROR: %s.\n", $session->error);
38     $session->close;
39     exit 1;
40 }
41
```

SNMP Traps mit Perl (via Net::SNMP) - III

- Empfang einer Beispiel SNMP Trap via Perl

```
2012-08-22 20:52:35 172.16.166.2(via UDP: [172.16.166.1]:58027-
>[172.16.166.129]:162) TRAP, SNMP v1, community public
        SNMPv2-SMI::enterprises Enterprise Specific Trap (0) Uptime:
0:00:00.00
        NET-SNMP-EXAMPLES-MIB::netSnmpExampleHeartbeatNotification = INTEGER:
123456
```

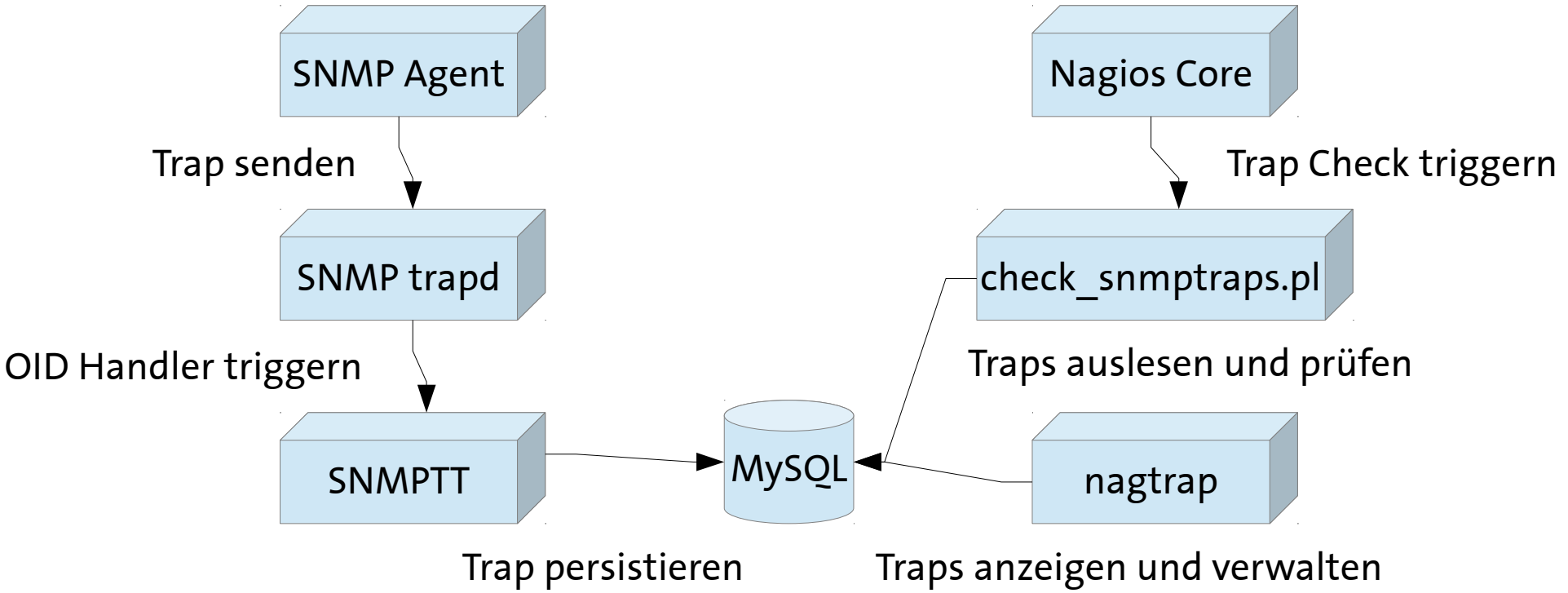
- SNMP Traps eignen sich hervorragend zum Applikations-Monitoring
- SNMP-API's sind für fast alle Programmiersprachen verfügbar
- Java: http://www.snmp4j.org/
- PHP: http://php.net/manual/de/book.snmp.php
- Python: http://pysnmp.sourceforge.net/
- Ruby: http://snmplib.rubyforge.org/

SNMP & Nagios

SNMP & Nagios – Philosophie

- Nagios kann SNMP auf zwei Arten lesen
  - Polling via Active Checks (was Nagios ohnehin meistens tut)
  - Checks via SNMP Traps (was interessanter ist)
- Beispiel in Nagios-Dokumentation hat Nachteile
  - Traps werden immer überschrieben, keine Historie
- Besser:
  - Verarbeitung via SNMPTT: http://www.snmptt.org/
  - Speichern in MySQL Datenbank
  - Nagios-Integration via NagTrap: http://sourceforge.net/projects/nagtrap/

The Big Picture



SNMPTT

- Übergabe an SNMPTT erfolgt über Trap Handler
- Dazu muss snmptrapd.conf angepasst werden:

```
# /etc/snmp/snmptrapd.conf

# allow community public
authCommunity log,execute,net public

# handle all traps via snmptt
traphandle default /usr/sbin/snmptthandler
```

- smnptt.ini: SNMPTT soll alle Traps entgegen nehmen:

```
# /etc/snmp/snmptt.ini

[Logging]
unknown_trap_log_enable = 1
unknown_trap_log_file = /var/log/snmptt/snmpttunknown.log
```

Verarbeiten von Traps mit SNMPTT - I

- Empfang einer Beispiel SNMP Trap mit Verarbeitung durch SNMPTT

```
2012-08-22 22:06:06 192.168.99.18(via UDP: [172.16.166.1]:53583-
>[172.16.166.129]:162) TRAP, SNMP v1, community public
        NET-SNMP-EXAMPLES-MIB::netSnmpExampleHeartbeatNotification Enterprise
Specific Trap (17) Uptime: 3 days, 10:01:04.69
        NET-SNMP-EXAMPLES-MIB::netSnmpExampleHeartbeatRate = INTEGER: 1234568
SNMPTTHANDLER started: Wed Aug 22 22:06:26 2012

s = 1345665986, usec = 747879
s_pad = 1345665986, usec_pad = 747879

Data received:

<UNKNOWN>

UDP: [172.16.166.1]:53583->[172.16.166.129]:162

DISMAN-EVENT-MIB::sysUpTimeInstance 3:10:01:04.69

SNMPv2-MIB::snmpTrapOID.0 NET-SNMP-EXAMPLES-
MIB::netSnmpExampleHeartbeatNotification.0.17

NET-SNMP-EXAMPLES-MIB::netSnmpExampleHeartbeatRate 1234568

SNMP-COMMUNITY-MIB::snmpTrapAddress.0 192.168.99.18

SNMP-COMMUNITY-MIB::snmpTrapCommunity.0 "public"

SNMPv2-MIB::snmpTrapEnterprise.0 NET-SNMP-EXAMPLES-
MIB::netSnmpExampleHeartbeatNotification
```

Verarbeiten von Traps mit SNMPTT - II

- SNMPTT soll Traps nach MySQL loggen

```
# /etc/snmp/snmptt.ini

...

[SQL]
db_translate_enterprise = 0
db_unknown_trap_format = '$-*'
sql_custom_columns = <<END
END

sql_custom_columns_unknown = <<END
END

mysql_dbi_enable = 1
mysql_dbi_host = localhost
mysql_dbi_port = 3306
mysql_dbi_database = snmptt
mysql_dbi_table = snmptt
mysql_dbi_table_unknown = snmptt_unknown
mysql_dbi_table_statistics = snmptt_statistics
mysql_dbi_username = snmptt
mysql_dbi_password = snmptt
mysql_ping_on_insert = 1
mysql_ping_interval = 300
```

SNMP Traps bei SNMPTT bekanntmachen - I

- MIB's können mit snmpttconvert übersetzt werden:

```
linux-dwoa:~ # snmpttconvertmib --in /usr/share/snmp/mibs/NET-SNMP-EXAMPLES-
MIB.txt --out /etc/snmp/snmptt.examples.conf


*****  Processing MIB file *****

snmptranslate version: NET-SNMP version: 5.7.1
severity: Normal

File to load is:        /usr/share/snmp/mibs/NET-SNMP-EXAMPLES-MIB.txt
File to APPEND TO:      /etc/snmp/snmptt.examples.conf

MIBS environment var:   /usr/share/snmp/mibs/NET-SNMP-EXAMPLES-MIB.txt
mib name: NET-SNMP-EXAMPLES-MIB


...


Done

Total translations:        1
Successful translations:   1
Failed translations:       0
```

SNMP Traps bei SNMPTT bekanntmachen - II

- Übersetzungen müssen von SNMPTT importiert werden:

```
# /etc/snmp/snmptt.ini

[General]
...

net_snmp_perl_enable = 1
net_snmp_perl_best_guess = 2
translate_log_trap_oid = 0
translate_value_oids = 1
translate_enterprise_oid_format = 1
translate_trap_oid_format = 1
translate_varname_oid_format = 1
translate_integers = 1

...

[TrapFiles]
snmptt_conf_files = <<END
/etc/snmp/snmptt.conf
/etc/snmp/snmptt.examples.conf
END
```

SNMP Traps bei SNMPTT bekanntmachen - III

- Die ursprüngliche MIB für netSnmpExampleHeartbeatRate

```
#  /usr/share/snmp/mibs/NET-SNMP-EXAMPLES-MIB.txt

NET-SNMP-EXAMPLES-MIB DEFINITIONS ::= BEGIN

--
-- Example MIB objects for agent module example implementations
--

IMPORTS
...

NetSnmpExamples  MODULE-IDENTITY
    LAST-UPDATED "200406150000Z"
    ORGANIZATION "www.net-snmp.org"
...

netSnmpExampleHeartbeatRate  OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "A simple integer object, to act as a payload for the
         netSnmpExampleHeartbeatNotification.  The value has
         no real meaning, but is nominally the interval (in
         seconds) between successive heartbeat notifications."
::= { netSnmpExampleNotificationObjects 1 }

...
```

SNMP Traps bei SNMPTT bekanntmachen - IV

- Übersetzung von NET-SNMP-EXAMPLES-MIB anpassen:

```
# /etc/snmp/snmptt.example.conf

#
#
#
#
MIB: NET-SNMP-EXAMPLES-MIB (file:/usr/share/snmp/mibs/NET-SNMP-EXAMPLES-
MIB.txt) converted on Thu Aug 23 12:16:36 2012 using snmpttconvertmib v1.3
#
#
#
EVENT  netSnmpExampleHeartbeatNotification .1.3.6.1.4.1.0.0 "Status Events" \
Critical
FORMAT An example notification, used to illustrate the $* \
SDESC
An example notification, used to illustrate the
definition and generation of trap and inform PDUs
(including the use of both standard and additional
varbinds in the notification payload).
This notification will typically be sent every
30 seconds, using the code found in the example module
agent/mibgroup/examples/notification.c
Variables:
  1: netSnmpExampleHeartbeatRate
EDESC
```

NagTrap konfigurieren

- check_snmptraps.pl muss sich mit MySQL verbinden können

```
#  /usr/lib/nagios/plugins/check_snmptrap.pl

...

# ==================== Database connect information ====================
my $dbHost = "localhost";
my $dbName = "snmptt";
my $dbUser = "snmptt";
my $dbPass = "snmptt";
my $dbTable = "snmptt";
my $dbTableUnknown = "snmptt_unknown";

...
```

Nagios Check prüfen

- check_snmptraps.pl Aufruf testen

```
linux-dwoa:~ # /usr/lib/nagios/plugins/check_snmptraps.pl -H 172.16.166.2 -r
CRITICAL - No warning Traps and 3 critical Traps in the database|'warning
trap'=0;;;; 'critical trap'=3;;;;


# Bestimmte Kategorie prüfen
linux-dwoa:~ # /usr/lib/nagios/plugins/check_snmptraps.pl -H 172.16.166.2 -r
-C 'Backup Fehler'
OK - No warning Traps and no critical traps in the database|'warning
trap'=0;;;; 'critical trap'=0;;;;

# Bestimmte OID prüfen
linux-dwoa:~ # /usr/lib/nagios/plugins/check_snmptraps.pl -H 172.16.166.2 -r
-O .1.3.6.1.4.1.0.0
CRITICAL - No warning Traps and 3 critical Traps in the database|'warning
trap'=0;;;; 'critical trap'=3;;;;

# Unbekannte Traps prüfen
linux-dwoa:~ # /usr/lib/nagios/plugins/check_snmptraps.pl -H 172.16.166.1 -r
-u
CRITICAL - 10 Unknown Traps|'Unknown trap='10;;;;
```

Literaturempfehlungen

- Net-SNMP: http://www.net-snmp.org/docs/
- SNMPTT: http://www.snmptt.org/docs/snmptt.shtml
- Nagios: http://nagios.sourceforge.net/docs/nagioscore/3/en/toc.html
- SNMP Traps verarbeiten: http://www.nagios-wiki.de/nagios/howtos/snmptt
- Evan McGinnis, David Perkins: Understanding SNMP Mibs http://www.amazon.de/Understanding-SNMP-Mibs-Evan-McGinnis/dp/0134377087/
- Douglas R. Mauro, Kevin J. Schmidt: Essential SNMP http://www.amazon.de/Essential-SNMP-System-Network-Administrators/dp/0596008406/

Viel Spaß noch auf der FrOSCon 2012!