adesso business. people. technology.

SNMP Applied

Sicheres Anwendungs-Monitoring mit SNMP

Gerrit Beine <gerrit.beine@adesso.de>

09.05.2014

Short run

- Konfiguration und Anwendung von Net-SNMP
- SNMPv3 mit Net-SNMP
- TLS/DTLS mit Net-SNMP

adesso business. people. technology.

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 OIDs (snmptranslate)
- Daemon zum Empfangen von SNMP Traps (snmptrapd)
- Daemon als SNMP Agent (snmpd)
- C- und Perl-APIs
- 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)

# listen on all interfaces
agentAddress udp:161
# 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 192.168.79.0/24
```

- Abfrage des snmpd erfolgt via snmpwalk

```
~$ snmpwalk -c public -v1 snmp.dev
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
...
```

Das Problem:
Das ist alles total unsicher!

Schwächen von SNMPv1 und SNMPv2c

- Autorisierung erfolgt über die IP-Adresse
- Authentifizierung erfolgt über Community
- Einschränkungen der Community gelten jeweils pro IP-Adresse
- Übertragung erfolgt unverschlüsselt
- Standard-Protokoll UDP sicher Datenübertragung nicht ab

Net-SNMP für SNMPv3 konfigurieren I

- Benutzer anlegen

```
~$ /etc/init.d/snmpd stop
~$ net-snmp-config --create-snmpv3-user -a "secretpw" snmpUser
~$ /etc/init.d/snmpd start
```

- Minimale Konfiguration für SNMPv3

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

# listen on all interfaces
agentAddress udp:161
```

```
# /usr/share/snmp/snmpd.conf !! :-(
# Via `net-snmp-config` erzeugt

rwuser snmpUser
```

Net-SNMP für SNMPv3 konfigurieren II

- Minimale Konfiguration für SNMPv3

```
# /var/lib/net-snmp/snmpd.conf (openSUSE)
# /var/lib/snmp/snmpd.conf (Debian)

##############################################################################
# STOP STOP STOP STOP STOP STOP STOP STOP STOP
#
#          **** DO NOT EDIT THIS FILE ****
#
# STOP STOP STOP STOP STOP STOP STOP STOP STOP
##############################################################################
...
```

- Abfrage testen (unverschlüsselt und verschlüsselt)

```
~$ snmpget -v 3 -u snmpUser -l authNoPriv -a MD5 -A secretpw \
 snmp.dev sysUpTime.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (8805) 0:01:28.05
```

```
~$ snmpget -v 3 -u snmpUser -l authPriv -a MD5 -A secretpw \
 -x DES -X secretpw snmp.dev sysUpTime.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (9835) 0:01:38.35
```

Benutzer hinzufügen I

- Neue Benutzer benötigen einen Template-User
- Benutzer hinzufügen mit snmpusm
- Danach unbedingt das Passwort ändern

```
~$ snmpusm -v 3 -u snmpUser -l authNoPriv -a MD5 -A secretpw \
 snmp.dev create gbeine snmpUser
User successfully created.
```

```
~$ snmpget -v 3 -u gbeine -l authNoPriv -a MD5 -A secretpw \
 snmp.dev sysUpTime.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (11303) 0:01:53.03
```

```
~$ snmpusm -v 3 -u gbeine -l authPriv -a MD5 -A secretpw \
 -x DES -X secretpw snmp.dev passwd secretpw strenggeheim
SNMPv3 Key(s) successfully changed.
```

```
~$ snmpget -v 3 -u gbeine -l authNoPriv -a MD5 -A strenggeheim \
 snmp.dev sysUpTime.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (5871) 0:00:58.71
```

- Achtung: Neue Benutzer und Passwortänderungen sind zwar sofort verfügbar, aber noch nicht persistiert!

Benutzer hinzufügen II

- Benutzer in Konfiguration eintragen und SNMP neu starten

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

# listen on all interfaces
agentAddress udp:161

# new user
rwuser gbeine
```

- Abfrage testen (unverschlüsselt und verschlüsselt)

```
# /var/lib/net-snmp/snmpd.conf (openSUSE)
# /var/lib/snmp/snmpd.conf (Debian)
# ...
usmUser 1 3 0x80001f88804162a72b6c8c205300000000 "gbeine" "gbeine" NULL \
 .1.3.6.1.6.3.10.1.1.2 0x0a32bdbfcc9830326f7a6353a4fef86e \
 .1.3.6.1.6.3.10.1.2.2 0x0a32bdb
```

http://www.net-snmp.org/docs/man/snmpd.conf.html:
„It is recommended you use the net-snmp-config command to do this“

Luxus auf Client-Seite

- Aufruf mit SNMPv3 wird recht kompliziert

```
~$ snmpget -v 3 -u snmpUser -l authPriv -a MD5 -A secretpw \
 -x DES -X secretpw snmp.dev sysUpTime.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (9835) 0:01:38.35
```

- Client Konfiguration für snmpget, snmpwalk, snmpset, ...

```
# ~/.snmp/snmp.conf

defSecurityName gbeine
defSecurityLevel authPriv
defAuthType MD5
defAuthPassphrase strenggeheim
defPrivType DES
defPrivPassphrase strenggeheim
defVersion 3
```

- Danach schon deutlich einfacher

```
~$ snmpget snmp.dev sysUpTime.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (5871) 0:00:58.71
```

Sicherheit erhöhen

- Verschlüsselung auf Seite des Servers erzwingen:

```
# /etc/snmp/snmpd.conf
# ...
rwuser gbeine priv
```

- Danach ist `-l authNoPriv` auf Client-Seite nicht mehr möglich :-)
- Passwort durch Diffie-Hellman-Keys ersetzen:

```
~$ snmpusm snmp.dev changekey gbeine
new auth key: 0x0404e48a606a7dc5ce0fe23d83257f91
new priv key: 0x092d15bea5298a286911692b28a9fc64
SNMPv3 Key(s) successfully changed.
```

- Client Konfiguration anpassen:

```
# ~/.snmp/snmp.conf

defSecurityName gbeine
defSecurityLevel authPriv
defVersion 3
defAuthLocalizedKey 0x0404e48a606a7dc5ce0fe23d83257f91
defPrivLocalizedKey 0x092d15bea5298a286911692b28a9fc64
```

Zugriffsbeschränkungen

- Zugriff von Usern oder Communities auf OIDs beschränken

```
# /etc/snmp/snmpd.conf
# ...
rwuser gbeine priv .1.3.6.1.2.1.1
# alternativ etwas besser lesbar
# rwuser gbeine priv system
```

- Lese-/Schreibzugriff pro Benutzer festgelegt
- Zugriff für jeden Benutzer auf Subtree der OID eingeschränkt
- Lösung dazu ist VACM (SNMPv3 View Based Access Control)

SNMPv3 VACM

- Zugriff von Usern oder Communities auf OIDs beschränken

```
# /etc/snmp/snmpd.conf
# ...
rwuser gbeine priv -V basic

view basic included system
view basic included interfaces
```

- View können OID-Subtree ein- und ausschließen
- Mehrere Einträge mit gleichem Namen werden zusammengefasst
- Weitere Einschränkungen möglich mit com2sec, group, access

Verbesserungen gegenüber SNMPv1 und SNMPv2c

- Authentifizierung erfolgt über Benutzer-Account
- Übertragung kann mit persönlichen Credentials verschlüsselt werden
- Verschlüsselung durch Server erzwungen
- Credentials durch sichere Diffie-Hellman-Keys ausgetauscht
- Beschränkung der Benutzer auf Teilbäume des MIB-Tree
- Festlegung von Lese-/Schreibrechten auf OID-Ebene

adesso business. people. technology.

Net-SNMP mit DTLS/TLS

Net-SNMP mit DTLS/TLS

- Net-SNMP beherrscht sowohl UDP als auch TCP
- Dank OpenSSL kann TLS und Datagram TLS (DTLS) verwendet werden
- Net-SNMP bringt eigene Tools zur Verwaltung von Zertifikaten mit
- Verfügbar ab Net-SNMP 5.6
- Debian liefert Net-SNMP 5.4 (zu alt)
- openSUSE liefert Net-SNMP 5.7, leider ohne DTLS/TLS Support
- Rebuild notwendig mit folgenden Optionen:

```
~$ ./configure .. \
 --with-security-modules=tsm \
 --with-transports=TLSTCP,DTLSUDP
```

Zertifikate erstellen

- Certificate Authority zum Signieren von Zertifikaten

```
~$ net-snmp-cert genca -I -n ca.snmp.dev
CA Generated:
  ca-certs/ca.snmp.dev.crt
  private/ca.snmp.dev.key
```

- Server-Zertifikat erstellen (wichtig ist `-t snmpd`)

```
~$ net-snmp-cert gencsr -I -t snmpd -n snmp.dev
Certificate Signing Request Generated:
  newcerts/snmpd.csr
  private/snmpd.key
```

- Client-Zertifikat erstellen (wichtig ist `-n gbeine`)

```
~$ net-snmp-cert gencsr -I -t manager -n gbeine
Certificate Signing Request Generated:
  newcerts/manager.csr
  private/manager.key
```

- Zertifikate signieren

```
~$ net-snmp-cert signcsr -I --with-ca ca.snmp.dev --csr snmpd
~$ net-snmp-cert signcsr -I --with-ca ca.snmp.dev --csr manager
```

Konfiguration des Servers für DTLS

- Fingerprint der Zertifikate auslesen

```
~$ net-snmp-cert showcerts --fingerprint
/etc/snmp/tls:

certs/manager.crt:
SHA1
Fingerprint=50:43:06:3E:5A:94:2C:51:3D:8B:32:81:68:B4:D3:BB:97:B2:9C:C4

certs/snmpd.crt:
SHA1
Fingerprint=78:11:C4:BE:D2:79:D6:00:4C:E0:0E:BC:0A:95:3B:92:1E:D3:26:41
```

- Konfiguration anpassen

```
# /etc/snmp/snmpd.conf
# ...

# listen on all interfaces
agentAddress udp:161, dtlsudp:10161

# certificate for user gbeine
certSecName 10 \
50:43:06:3E:5A:94:2C:51:3D:8B:32:81:68:B4:D3:BB:97:B2:9C:C4 --cn
```

Konfiguration auf Client-Seite

- SNMPv3 über DTLS (ohne Client-Konfiguration)

```
~$ snmpget -v 3 --defSecurityModel=tsm -u gbeine -l authPriv \
-T our_identity=50:43:06:3E:5A:94:2C:51:3D:8B:32:81:68:B4:D3:BB:97:B2:9C:C4 \
-T their_identity=78:11:C4:BE:D2:79:D6:00:4C:E0:0E:BC:0A:95:3B:92:1E:D3:26:41 \
dtlsudp:localhost:10161 sysUpTime.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (120) 0:00:01.20
```

- Client Konfiguration für snmpget, snmpwalk, snmpset, ...

```
# ~/.snmp/snmp.conf

defSecurityLevel authPriv
defVersion 3
defSecurityModel tsm
localCert 50:43:06:3E:5A:94:2C:51:3D:8B:32:81:68:B4:D3:BB:97:B2:9C:C4
peerCert 78:11:C4:BE:D2:79:D6:00:4C:E0:0E:BC:0A:95:3B:92:1E:D3:26:41
```

- SNMPv3 über DTLS (mit Client-Konfiguration)

```
~$ snmpget dtlsudp:localhost:10161 sysUpTime.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (120) 0:00:01.20
```

adesso business. people. technology.

Weiterführendes

Literaturempfehlungen

- Net-SNMP: http://www.net-snmp.org/docs/
- SNMP4J: http://www.snmp4j.org/
- 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/

adesso business. people. technology.

Viel Spaß noch auf dem LinuxTag 2014!

info@adesso.de
www.adesso.de