Упражнения SNMP, часть I

Contents

1 Введение

1.1 Цели

- Install and learn to use the SNMP commands
- Explore and identify standard vs enterprise parts of the MIB tree
- Install vendor specific MIBs and use those with the SNMP commands

1.2 Замечания

- Команды, предваряемые “$” означают, что они должны быть выполнены с правами обычного пользователя – а не администратора.
- Команды, предваряемые “#” означают, что вы должны иметь права администратора.
- Команды с более специфичными подсказками (например “rtrX>” или “mysql>”) означают что вы выполняете их либо на удаленном оборудовании, либо в какой-то другой программе.

2 Установка клиента (менеджера)

Начните с установки набора инструментов net-snmp:

```
$ sudo apt-get install snmp
$ sudo apt-get install snmp-mibs-downloader
```

Вторая команда скачивает те стандартные MIBы от IETF и IANA, которые не включены по умолчанию.

Замечание: для того, чтобы это работало, вам необходимо включить источник “multiverse” в вашу конфигурацию APT, если вы используете Ubuntu 12.04 или 14.04. На этом семинаре это уже было сделано.

Теперь, отредактируйте файл /etc/snmp/snmp.conf:

```
$ sudo editor /etc/snmp/snmp.conf
```

Поменяйте эту строку:

```
mibs :
```

… так, что она выглядит как:

```
# mibs :
```

(Вы “закомментировали” пустую конфигурацию MIBов, которая говорит инструментам **не** загружать MIBы из каталога /usr/share/mibs/ автоматически)

3 Конфигурирование SNMP на вашем роутере

Для этого упражнения вы должны работать в группах. Выберите одного человека набирать на клавиатуре.

Если вы не уверены, в какой вы группе, обратитесь к диаграмме сети, расположенной на wiki для класса – посетите http://noc.ws.nsrc.org/ и нажмите на ссылку Network Diagram.

Теперь зайдите на ваш роутер:

```
$ ssh cisco@rtrN.ws.nsrc.org    (or "ssh cisco@10.10.N.254")

username: cisco
password: <CLASS PASSWORD>

rtrN> enable
Password: <CLASS PASSWORD>
rtrN# configure terminal            (conf t)
```

Теперь нам нужно добавить список контроля доступа для доступа к SNMP, активировать SNMP, назначить SNMP пароль для доступа “только для чтения”, и сказать роутеру чтобы он сохранял SNMP-информацию между перезагрузками. Это делается так:

```
rtrN(config)# access-list 99 permit 10.10.0.0 0.0.255.255
rtrN(config)# snmp-server community NetManage ro 99
rtrN(config)# snmp-server ifindex persist
```

Давайте выйдем из режима конфигурации и сохраним новую конфигурацию в постоянной памяти.

```
rtrN(config)# exit
rtrN# write memory                  (wr mem)
rtrN# exit                      (до тех пор пока вы не вернулись на pc)
```

Теперь посмотрим, работают ли наши изменения.

4 Тестирование SNMP

Чтобы проверить, что ваша конфигурация SNMP работает, запустить команду snmpstatus для каждого из следующих устройств

```
$ snmpstatus -c NetManage -v 2c <IP_ADDRESS>
```

Где это адрес одного из следующих устройств:

```
* Сервер NOC:                    10.10.0.250
* Роутер вашей группы:           10.10.N.254
* Магистральный маршрутизатор:   10.10.0.253
* Магистральный роутер:          10.10.0.254
* Точки доступа:                 10.10.0.251, 10.10.0.252
```

Что происходит если вы исползуете неправильный пароль (т.е. изменяте NetManage на что-то другое ?)

5 Траверс SNMP и OIDы

Теперь, вы будете использовать команду snmpwalk, являющегося частью инструментария SNMP, для перечисления таблиц, связанных с OIDами, перечисленными ниже, на каждом из устройств вы использовали выше:

```
.1.3.6.1.2.1.2.2.1.2
.1.3.6.1.2.1.31.1.1.1.18
.1.3.6.1.4.1.9.9.13.1
.1.3.6.1.2.1.25.2.3.1
.1.3.6.1.2.1.25.4.2.1
```

Вы сделаете это используя две разные формы команді snmpwalk:

```
$ snmpwalk -c NetManage -v 2c <IP_ADDRESS> <OID>
```

и

```
$ snmpwalk -On -c NetManage -v 2c <IP_ADDRESS> <OID>
```

… где OID – один из OIDов перечисленных выше: .1.3.6…

… где IP_ADDRESS может быть роутером вашей группы…

Замечание: параметр -On включает числовой вывод, т.е. отключает трансляцию OIDов в имена из MIBа.

Для этих OIDов:

a) Все ли устройства отвечают?
b) Заметили ли вы что-нибудь важное об OIDах в выводе?

6 Конфигурирование snmpd на вашем PC

Для этого упражнения ваша группа должна проверить, что сервис snmpd запущен и отвечает на запросы на всех машинах вашей группы. Вначале разрешите snmpd на вашей машине, потом проверьте, отвечает ли она, потом проверьте каждую машину других членов вашей группы.

- Установите SNMP-агента (программу-демона)

```
$ sudo apt-get install snmpd
```

- Конфигурирование.

Мы сохраним конфигурацию по умолчанию, и создадим нашу собственную:

```
$ cd /etc/snmp
$ sudo mv snmpd.conf snmpd.conf.dist
$ sudo editor snmpd.conf
```

Потом, скопируйте следующее:

```
#  Listen for connections on all interfaces (both IPv4 *and* IPv6)
agentAddress udp:161,udp6:[::1]:161

# Configure Read-Only community and restrict who can connect
rocommunity NetManage  10.10.0.0/16
rocommunity NetManage  127.0.0.1

# Information about this host
sysLocation    NSRC Network Management Workshop
sysContact     sysadm@pcX.ws.nsrc.org

# Which OSI layers are active in this host
# (Application + End-to-End layers)
sysServices    72

# Include proprietary dskTable MIB (in addition to hrStorageTable)
includeAllDisks  10%
```

Теперь сохраните файл и выйдите из редактора.

- Перезапустите snmpd

```
$ sudo service snmpd restart
```

6.1 Проверьте, что snmpd работает:

```
$ snmpstatus -c NetManage -v 2c localhost
```

Что вы наблюдаете?

6.2 Протестируйте ваших соседей

Убедитесь, что вы можете проверять snmpstatus на других серверах вашей группы:

```
$ snmpstatus -c NetManage -v 2c pcN.ws.nsrc.org
```

Например, для группы 5, вам следует проверить:

* pc17.ws.nsrc.org
* pc18.ws.nsrc.org
* pc19.ws.nsrc.org
* pc20.ws.nsrc.org

7 Добавление MIBов

Вспомните, когда вы запустили:

```
$ snmpwalk -c NetManage -v 2c 10.10.X.254  .1.3.6.1.4.1.9.9.13.1
```

Если вы обратили внимание, SNMP-клиент (snmpwalk) не мог проинтерпретировать все OIDы, которые вернул SNMP агент:

```
SNMPv2-SMI::enterprises.9.9.13.1.3.1.2.1 = STRING: "chassis"
SNMPv2-SMI::enterprises.9.9.13.1.3.1.6.1 = INTEGER: 1
```

Что такое 9.9.13.1.3.1 ?

Для расшифровки этой информации, нам нужно скачать дополнительные MIBы:

Мы будем использовать следующие MIBы (не скачивайте их пока!):

MIBы CISCO

```
ftp://ftp.cisco.com/pub/mibs/v2/CISCO-SMI.my
ftp://ftp.cisco.com/pub/mibs/v2/CISCO-ENVMON-MIB.my
```

Для удобства, мы сделали локальное зеркало здесь: http://noc.ws.nsrc.org/mibs/

Скачайте их теперь, как показано ниже:

```
$ sudo apt-get install wget
$ cd /usr/share/mibs
$ sudo mkdir cisco
$ cd cisco

$ sudo wget http://noc.ws.nsrc.org/downloads/mibs/CISCO-ENVMON-MIB.my
$ sudo wget http://noc.ws.nsrc.org/downloads/mibs/CISCO-SMI.my
```

Теперь нам нужно сказать инструментарию snmp, что у нас появились новые MIBы и что он должен их подгружать. Поэтому, отредактируйте файл /etc/snmp/snmp.conf, и добавьте следующие две строчки:

```
mibdirs +/usr/share/mibs/cisco
mibs +CISCO-ENVMON-MIB:CISCO-SMI
```

Сохраните файл, выйдите из редактора.

Теперь, снова выполните:

```
$ snmpwalk -c NetManage -v 2c 10.10.X.254  .1.3.6.1.4.1.9.9.13.1
```

Что вы увидели?

8 Траверс SNMP – остаток MIB-II

Используйте snmpwalk для опрашивания других устройств (роутеров, маршрутизаторов, серверов) в сети 10.10.0.X.

Обратите внимание на типы информации, которую вы можете получить.

```
$ snmpwalk -c NetManage -v 2c 10.10.0.X ifDescr
$ snmpwalk -c NetManage -v 2c 10.10.0.X ifAlias
$ snmpwalk -c NetManage -v 2c 10.10.0.X ifTable | less
$ snmpwalk -c NetManage -v 2c 10.10.0.X ifXTable | less
$ snmpwalk -c NetManage -v 2c 10.10.0.X ifOperStatus
$ snmpwalk -c NetManage -v 2c 10.10.0.X ifAdminStatus
$ snmpwalk -c NetManage -v 2c 10.10.0.X if
```

(Не забудьте, используя less, пробел пролистывает страницу вперед, b – страницу назад, и q – выход)

Видите ли вы разницу между ifTable и ifXTable?

Как вы думаете, в чем разница между ifOperStatus и ifAdminStatus? Можете ли вы представить себе ситуацию, когда эта разница может быть полезна?

9 Поиграемся еще с MIBами и OIDами

- Используйте SNMP для нахождения:

a. запущенных процессов на сервере соседа (hrSWRun)
b. свободного места на диске на сервере соседа (hrStorage)
c. интерфейсов на сервере соседа (ifIndex, ifDescr)

Можете ли вы использовать короткие имена для траверса этих таблиц?

- Поэкспериментируйте с командой snmptranslate, например:

```
$ snmptranslate .1.3.6.1.4.1.9.9.13.1
```

- Попробуйте это с различными OIDами