SNMP

SNMP (англ. - Simple Network Management Protocol — простой протокол сетевого управления) — стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP. К поддерживающим SNMP устройствам относятся маршрутизаторы, коммутаторы, серверы, рабочие станции, принтеры, модемные стойки и другие. Протокол обычно используется в системах сетевого управления для контроля подключённых к сети устройств на предмет условий, которые требуют внимания администратора. SNMP состоит из набора стандартов для сетевого управления, включая протокол прикладного уровня, схему баз данных и набор объектов данных.

Стенд

Две машины с установленной ОС Astra Linux 1.6 SE (Smolensk) x64.

1-ой машине присвоен ip адрес: 192.168.1.111

2-ой машине присвоен ip адрес: 192.168.1.112

1: Установка демона и утилит SNMP & SNMPD:

а) Установка SNMP на 1-ый сервер, который выступает в качестве менеджера:

```
$sudo apt-get update
$sudo apt-get install snmp
```

б) Установка SNMPD на 2-ой сервер, который выступает в качестве агента (опрашиваемого) :

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

2: Конфигурация:

а) менеджера SNMP:

Откройте файл /etc/snmp/snmp.conf:

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

Чтобы позволить менеджеру SNMP импортировать файлы MIB, следует закомментировать следующую строку:

```
#mibs :
```

После чего сохранить файл (Ctrl+O) и выйти из редактора nano (ctrl+X).

б) агента snmpd:

Откройте файл /etc/snmp/snmpd.conf

```
sudo nano /etc/snmp/snmpd.conf
```

Откорректируйте директиву agentAddress; на данный момент она поддерживает только соединения, исходящие с локального компьютера. Нужно закомментировать эту строку и раскомментировать следующую строку, что разрешает все соединения.

```
#  Listen for connections from the local system only

#agentAddress  udp:127.0.0.1:161

#  Listen for connections on all interfaces (both IPv4 *and* IPv6)

agentAddress udp:161,udp6:[::1]:161
```

⚠ Если не используется ipv6, следует также удалить udp6:[::1]:161

Далее в конфиге нужно создать пользователя %Имя_вашего_пользователя, который, который будет использоваться в качестве шаблона для создания обычных пользователей. Пакеты SNMP делают это путём клонирования параметров пользователей.

Создавая нового пользователя, укажите тип аутентификации (MD5 или SHA) и пароль (минимум 8 символов). Если вы планируете использовать при передаче данных защитное преобразование данных, вы также должны указать протокол преобразования (DES или AES) и пароль для него (по желанию). Если вы не выберете пароль для протокола преобразования, вместо него будет использоваться пароль аутентификации.

Для примера создадим пользователя "usertest", с паролем "temp_password", с MD5 типом аутентификации и протоколом преобразования DES. Для этого в конфигурационном файле snmpd.cfg запишем:

```
createUser usertest MD5 temp_password DES
```

Далее в конфигурационном файле, пользователю "usertest" следует указать уровень доступа:

rwuser - даёт право на чтение и запись.

rouser - даёт право только на чтение.

Для обязательного защитного преобразования используется параметр **priv** .

Чтобы ограничить пользователя определённой частью MIB, нужно указать OID высшего уровня, к которому пользователь должен иметь доступ.

```
rwuser usertest priv
```

Сохраните и закройте файл /etc/snmp/snmpd.cfg.

Перезапустите сервис snmpd:

```
sudo service snmpd restart
```

Посомтреть статус менеджера snmpd:

```
$sudo service snmpd status
```

```
u@snmpserv:~$ sudo service snmpd status
● snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
   Loaded: loaded (/lib/systemd/system/snmpd.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2018-09-21 10:56:51 MSK; 14s ago
  Process: 1311 ExecStartPre=/bin/mkdir -p /var/run/agentx (code=exited, status=0/SUCCESS)
 Main PID: 1314 (snmpd)
    Tasks: 1 (limit: 4915)
   CGroup: /system.slice/snmpd.service
           └─1314 /usr/sbin/snmpd -Lsd -Lf /dev/null -u Debian-snmp -g Debian-snmp -I -smux mteTrigger mteTriggerConf -f

сен 21 10:56:51 snmpserv systemd[1]: Starting Simple Network Management Protocol (SNMP) Daemon....
сен 21 10:56:51 snmpserv systemd[1]: Started Simple Network Management Protocol (SNMP) Daemon..
сен 21 10:56:51 snmpserv snmpd[1314]: Turning on AgentX master support.
сен 21 10:56:51 snmpserv snmpd[1314]: NET-SNMP version 5.7.3
```

3. Общая структура команд SNMP:

Утилита snmpusm применяется для управления пользователями SNMPv3.Три базовых операций SNMP - это snmpget, snmpset и snmpwalk. Их назначение понятно из названия: snmpget считывает значение оценки с помощью устройства, snmpset устанавливает значение параметра на устройство, snmpwalk считывает с устройства часть дерева MIB.

При работе с набором net-snmp используется несколько шаблонов для вызова команд.

Сначала нужно пройти аутентификацию и подключиться к демону SNMP. Для этого могут понадобиться следующие флаги:

- -v (version): задаёт версию SNMP-протокола.
- -c (community): определяет версию строки доступа .
- -u (user-name): указывает имя пользователя, которого нужно авторизовать. Чтобы пользователь имел право на чтение и изменение, он должен быть зарегистрирован в SNMP.
- -l (level): задаёт уровень безопасности для подключения. Можно использовать такие значения: noAuthNoPriv (без аутентификации), authNoPriv (аутентификация без защитного преобразования) и authPriv (аутентификация и защитное преобразование). Кроме того, указанный пользователь должен иметь доступ к выбранному уровню безопасности, иначе он не сможет подключиться.
- -a (protocol): определяет протокол аутентификации, MD5 или SHA. Это значение должно совпадать с информацией пользователя, указанной при его создании.
- -x (protocol): определяет протокол защитного преобразования, DES или AES. Это значение должно совпадать с информацией пользователя, указанной при его создании. Протокол защитного преобразования обязательно нужно указывать, если в настройках пользователя есть параметр priv.
- -A (passphrase): пароль для аутентификации пользователя.
- -X (passphrase): пароль защитного преобразования. Если вы не указали этот пароль, вместо него будет использоваться пароль для аутентификации. Это пароль обязательно нужно указывать, если в настройках пользователя есть параметр priv.

Теперь вы можете написать команду. Ваша команда может отличаться в зависимости от параметров пользователя. Общий синтаксис:

```
snmp_command -u _ -l authPriv -a MD5 -x DES -A _ -X __ ip_ ___
```

3a) Утилита snmpget - получение информации с удалённого хоста

К примеру, чтобы убедиться, что пользователь usertest доступен, нужно запустить на менеджере:

```
snmpget -u usertest -l authPriv -a MD5 -x DES -A temp_password -X temp_password 192.168.1.112 1.3.6.1.2.1.1.1.0

SNMPv2-MIB::sysDescr.0 = STRING: Linux snmpdtest 4.15.3-1-generic #astra14 SMP Tue Aug 7 13:57:30 UTC 2018
x86_64 GNU/Linux
```

1.3.6.1.2.1.1.1.0 – OID, . uname –a.

```
u@snmpserv:~$ sudo service snmpd status
● snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
   Loaded: loaded (/lib/systemd/system/snmpd.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2018-09-21 10:56:51 MSK; 12min ago
  Process: 1311 ExecStartPre=/bin/mkdir -p /var/run/agentx (code=exited, status=0/SUCCESS)
 Main PID: 1314 (snmpd)
    Tasks: 1 (limit: 4915)
   CGroup: /system.slice/snmpd.service
           └─1314 /usr/sbin/snmpd -Lsd -Lf /dev/null -u Debian-snmp -g Debian-snmp -I -smux mteTrigger mteTriggerConf -f

сен 21 10:56:51 snmpserv systemd[1]: Starting Simple Network Management Protocol (SNMP) Daemon....
сен 21 10:56:51 snmpserv systemd[1]: Started Simple Network Management Protocol (SNMP) Daemon..
сен 21 10:56:51 snmpserv snmpd[1314]: Turning on AgentX master support.
сен 21 10:56:51 snmpserv snmpd[1314]: NET-SNMP version 5.7.3
сен 21 10:57:00 snmpserv snmpd[1314]: Connection from UDP: [192.168.1.111]:32960->[192.168.1.112]:161
сен 21 10:57:00 snmpserv snmpd[1314]: Connection from UDP: [192.168.1.111]:32960->[192.168.1.112]:161
сен 21 11:06:35 snmpserv snmpd[1314]: Connection from UDP: [192.168.1.111]:47138->[192.168.1.112]:161
сен 21 11:06:35 snmpserv snmpd[1314]: Connection from UDP: [192.168.1.111]:47138->[192.168.1.112]:161
сен 21 11:09:00 snmpserv snmpd[1314]: Connection from UDP: [192.168.1.111]:33383->[192.168.1.112]:161
сен 21 11:09:00 snmpserv snmpd[1314]: Connection from UDP: [192.168.1.111]:33383->[192.168.1.112]:161
u@snmpserv:~$
```

3) snmpusm - SNMPv3

snmpusm. :

snmpusm ___ _ create _ _

С помощью шаблона (usertest) и флагов вы можете создать пользователя с необходимым уровнем привилегий.

```
snmpusm -u usertest -l authPriv -a MD5 -x DES -A temp_password -X temp_password 192.168.1.112 create newuser
usertest

User successfully created.
```

Теперь на удалённом сервере есть полностью готовый к работе пользователь newuser. Однако пока что он использует те же учётные данные, что и usertest. Для того, чтобы изменить пароль пользователя, следует выполнить аутентификацию как newuser и установить новый пароль (8 символов минимум).

```
snmpusm -u newuser -l authPriv -a MD5 -x DES -A temp_password -X temp_password 192.168.1.112 passwd
temp_password my_new_password

SNMPv3 Key(s) successfully changed.
```

newuser «my_new_password».