Сетевое управление и мониторинг

Contents

1 Введение

1.1 Цели

- Научиться использовать syslog-ng для управления логами.

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 Упражнения

Найдите студента, использующего тот же роутер, что и вы сами. Соберитесь в группу и выполните следующее упражнение вместе. Выберите одного человека в группе, который будет работать с роутером – остальные должны помочь ему с конфигурированием.

3 Настройте ваш виртуальный роутер отправлять сообщения syslog на ваш сервер:

Роутеры могут отправлять сообщения syslog в несколько мест, так что один роутер может отправлять сообщения на 4 или даже 5 машин. Следовательно, нам нужно настроить роутер посылать сообщения на каждую виртуальную машину в группе.

Зайдите на групповой роутер через SSH и сделайте следующее:

```
$ ssh cisco@10.10.X.254
rtrX> enable
rtrX# config terminal
```

Повторите следующую команду “logging 10.10.X.Y” для каждой машины в группе. То есть, если вы в группе 6 и вы используете машины 21, 22, 23, и 24, повторите команду четыре раза, указывая IP каждой машины (10.10.6.21, 10.10.6.22, и так далее).

```
rtrX(config)# logging 10.10.X.Y
...
rtrX(config)# logging facility local0
rtrX(config)# logging userinfo
rtrX(config)# exit
rtrX# write memory
```

Теперь выполните show logging, чтобы увидеть сводку конфигурации логирования.

```
rtrX# show logging
```

Выйдите с роутера (exit)

```
rtrX# exit
```

Теперь роутер будет отправлять UDP пакеты SYSLOG на ваши виртуальные машины на порт 514. Чтобы это проверить, зайдите на вашу виртуальную машину и сделайте следующее:

```
$ sudo -s
# apt-get install tcpdump        (не беспокойтесь, если он уже установлен)
# tcpdump -s0 -nv -i eth0 port 514
```

Затем, пусть один человек из группы опять зайдет на роутер и наберет:

```
$ ssh cisco@10.10.X.254
rtrX> enable
rtrX# config terminal
(config)# exit
rtrX> exit
```

На вашей машине, вы должны увидеть вывод TCPDUMPa. Он будет выглядеть примерно так:

```
08:01:12.154604 IP (tos 0x0, ttl 255, id 11, offset 0, flags [none], proto UDP (17), length 138)
    10.10.9.254.57429 > 10.10.9.36.514: SYSLOG, length: 110
    Facility local0 (16), Severity notice (5)
   Msg: 23: *Feb 19 08:01:10.855: %SYS-5-PRIV_AUTH_PASS: Privilege level set to 15 by cisco on vty0 (10.10.0.
08:01:15.519881 IP (tos 0x0, ttl 255, id 12, offset 0, flags [none], proto UDP (17), length 130)
    10.10.9.254.57429 > 10.10.9.36.514: SYSLOG, length: 102
    Facility local0 (16), Severity notice (5)
   Msg: 24: *Feb 19 08:01:14.215: %SYS-5-CONFIG_I: Configured from console by cisco on vty0 (10.10.0.117)
```

Теперь вы можете настроить програму логирования на вашей машине так, чтобы она получала эту информацию, и записывала ее в новый набор файлов.

4 Установка syslog-ng

Эти упражнения делаются с правами администратора. Если вы еще не получили прав администратора, наберите

```
$ sudo -s
```

Затем:

```
# apt-get update
# apt-get install syslog-ng syslog-ng-core
```

5 Отредактируйте /etc/syslog-ng/syslog-ng.conf

Найдите строки:

```
source s_src {
       system();
       internal();
};
```

и измените их на:

```
source s_src {
       system();
       internal();
       udp();
};
```

Сохраните файл и выйдите из редактора.

Теперь, создайте новый раздел конфигурации для наших сетевых логов:

```
# cd /etc/syslog-ng/conf.d/
# editor 10-network.conf
```

Скопируйте в этот файл следующее:

```
    filter f_routers { facility(local0); };

    log {
            source(s_src);
```

```
        filter(f_routers);
        destination(routers);
};

destination routers {
file("/var/log/network/$YEAR/$MONTH/$DAY/$HOST-$YEAR-$MONTH-$DAY-$HOUR.log"
 owner(root) group(root) perm(0644) dir_perm(0755) create_dirs(yes)
 template("$YEAR $DATE $HOST $MSG\n"));
};
```

Сохраните файл и выйдите из редактора.

6 Создайте каталог /var/log/network/

```
# mkdir /var/log/network/
```

7 Перезапустите syslog-ng:

```
# service syslog-ng restart
```

8 Проверьте syslog

Чтобы убедиться, что все работает, зайдите опять на роутер, и запустите какие-нибудь команды конфигурирования, потом уйдите с роутера. Например:

```
# ssh cisco@10.10.X.254
rtrX> enable
rtrX# config terminal
rtrX(config)# exit
rtrX> exit
```

Убедитесь, что вы вышли с роутера – если слишком много людей логинятся на роутер и не выходят, другие не могут получить доступ к роутеру.

9 Посмотрите, появились ли сообщения на вашей машине в каталоге /var/log/network/20XX/…/

```
$ cd /var/log/network
```

```
$ ls
$ cd 20XX
$ ls
... this will show you the directory for the month
... cd into this directory
$ ls
... repeat for the next level (the day of the month)
$ ls
```

Вы можете просмотреть получившийся файл логов при помощи таких программ как less, more, cat, tail, и других…

10 Поиск проблем

Если файлы не появляются в дереве каталогов /var/log/network, то тогда следует попробовать деактивировать/активировать интерфейс Loopback на роутере (в режиме конфигурации), а именно:

```
$ ssh cisco@rtrX

rtrX> enable
rtrX# conf t
rtrX(config)# interface Loopback 999
rtrX(config-if)# shutdown
```

подождите несколько секунд, затем:

```
rtrX(config-if)# no shutdown
```

Затем выполните exit, и сохраните конфигурацию (write mem):

```
rtrX(config-if)# exit
rtrX(config)# exit
rtrX# write memory
rtr1# exit
```

Проверьте логи в /var/log/network

```
# cd /var/log/network
# ls
```

…посмотрите в подкаталогах

Все еще нет логов?

Попробуйте выполнить следующую команду локально (на виртуальной машине):

```
# logger -p local0.info "Hello World\!"
```

Если файл все еще не был создан в подкаталоге */var/log/network*, проверьте вашу конфигурацию на предмет опечаток. Не забудьте перезапускать сервис syslog-ng каждый раз, когда вы меняете его настройки.

Какие другие команды вы можете выполнить на роутере (БУДЬТЕ ОСТОРОЖНЫ!), которые приведут к отправке сообщений syslog? Вы можете попробовать зайти на роутер и ввести неверный пароль для enable.

Не забывайте выполнять команду ls в каталоге логов, чтобы увидеть, когда и если там появится новый лог-файл.