Mikrotik събитие
за професионалисти, ентусиасти,
и всички, които имат желание да
се **забавляват!**

NetCamp

2022

Mikrotik Scripting работа с Log файлове. Примерен скрипт за откриване и блокиране на неоторизирани опити за влизане

с. Ягодина 08.2022

Да се запознаем

инж. Георги Анастасов

За мен! *Сертифициран мрежов специалист и консултант за продукти на* ***Mikrotik,*** *с опит в проектиране и изграждане на малки и средни компютърни мрежи, сървъри и системи за архивиране.*

WEB: www.steadypc.com
E-mail: office@steadypc.com
GSM: +359 878806291

Mikrotik Scripting работа с файлове

Съдържание

Mikrotik Log

System Log

Структура на Log

Големина, възможности, занулляване

01

Mikrotik Scripting работа с Log
Определяне на големината и изчистване

1. Определяне големината на Log.

❑ Определяне на броя редове.

```
/system logging action
 set 0 memory-lines=1000
```

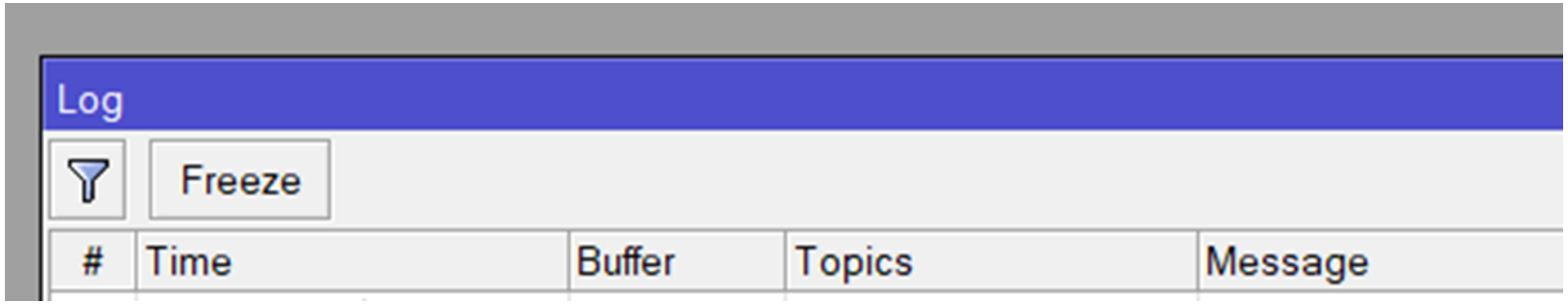
❑ Изчистване на Log

```
/system logging action
set 0 memory-lines=1
set 0 memory-lines=1000
```

Структура на Log съобщенията

2. Структура на Log съобщенията

#, Time, Buffer, Topics, Message



Структура на Log съобщенията

3. Запис и занулyване на Log.

log/ print file=currentlog.txt

Mikrotik Скриптове

02

Дефиниране на задачите
Проблеми

Mikrotik Scripting работа с Log

Дефиниране на задачата

1. Дефиниране на задачата.

- ❑ Дефиниране на броя грешни опити за влизане
  - За user error login – 3 неуспешни опита
  - За IPSec error login – 1 неуспешен опит

- ❑ Дефиниране на времеви интервал за обработка – 10мин, 1час, 1ден

- ❑ Дефиниране на честота на стартиране на скрипта

2. Проблеми

- ❑ Разлика във съобщенията за грешки в Ros v6 и Ros V7
- ❑ Възможни грешки при определяне на времевия интервал

03

Работа със стрингове

Синтаксис и основни операции

Mikrotik Scripting работа с Log

Работа със стрингове

1.Извличане на части от стринг с команда pick

:pick <var> <start>[<end>]

:put [:pick "abcde" 1 3] - извлича елемент от <start> включително до преди <end>

01234 Броенето започва от 0.

Резултат: bc

Намиране на фрагмент

2. Намиране на фрагмент в стринг с команда ~

find where message~"authentication failed"

Mikrotik Scripting работа с Log

Четене съдържанието на Log

3. Прочитане съдържанието на log и търсене на предварително дефинирани съобщения за грешка

```
/log
:foreach errorlogin in=[find where message~"login failure"] do={
```

Mikrotik Scripting работа с Log

Четене съдържанието на Log

3.1. Прочитане съдържанието на log и търсене на предварително дефинирани съобщения за грешка за текущия ден

```
/log
:foreach errorlogin in=[find where time>([/system clock get date]) message~"login failure"] do={
```

Четене съдържанието на Log

3.2. Прочитане съдържанието на log и търсене на предварително дефинирани съобщения за грешка за 10 минути назад във времето

```
/log
:foreach errorlogin in=[find where time>([/system clock get time] - 10min) message~"login failure"]
do={
```

Mikrotik Scripting работа с Log

Четене и запис в адресни листи

4. Реализиране на проверка за 3 грешни опита, чрез адресни листи.

- **Проверка за наличие на IP адрес в адресна листа**

```
:if ([:len [find where list=$blacklist and address=$ipsecannoying]] = 0) do={
```

- **Добавяне на IP адрес в адресна листа**

```
/ip firewall address-list add list=$blacklist address=$ipsecannoying timeout=1d
comment="$ipsecerrormsg"
```

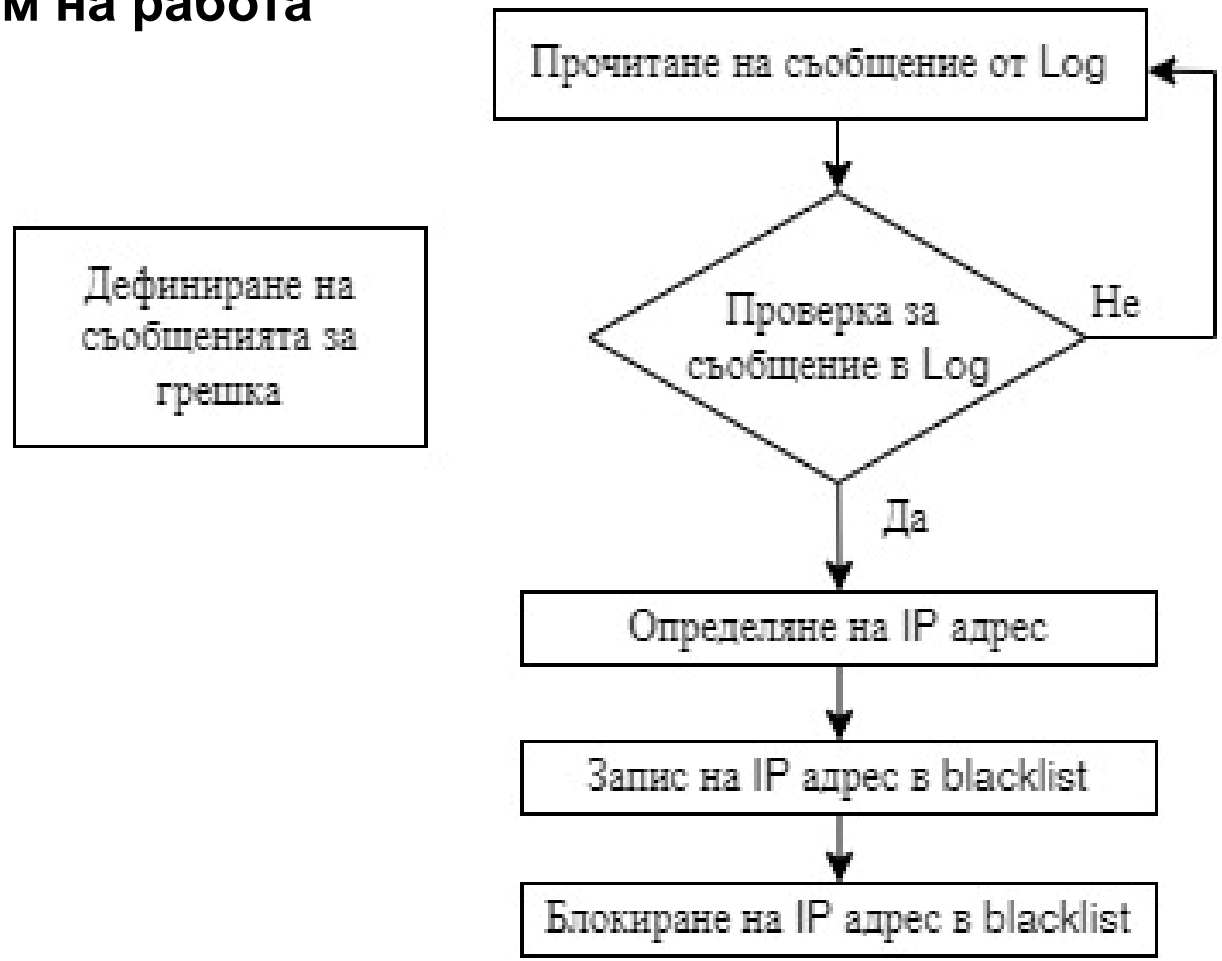
04

Откриване на user error login

Дефиниране на грешните съобщения.
Определяне на IP адреса в стринг.
Блокиране при 3 грешни опита

Mikrotik Scripting работа с Log
Дефиниране на грешните съобщения.

1. **Алгоритъм на работа**



Mikrotik Scripting работа с Log
Дефиниране на грешните съобщения.

2. Дефиниране на грешните опити user error login

"login failure for user x from x.x.x.x via service"

"login failure for user x from x.x.x.x via winbox"

"login failure for user x from x.x.x.x via romon network"

Mikrotik Scripting работа с Log

Намиране на грешните съобщения

3. Проверка за дефинираните фрази.

#Error message "login failure for user x from x.x.x.x via service"

/log
:global frommsg " from ";
:global viamsg   " via ";

[:pick $errormsg ([:find $errormsg $frommsg -1] + [:len $frommsg]) -> “login failure for user x from “

[:find $errormsg $viamsg -1] -> “ via service”

Mikrotik Scripting работа с Log
Ip АДРЕС

4. Определяне на IP адрес на досадника.

#Error message "login failure for user x from x.x.x.x via service"

```
/log
:global frommsg  " from ";
:global viamsg   " via ";

:foreach errorlogin in=[find where message~"login failure"] do={
    :local errormsg [get $errorlogin message]

:local ipannoying [:pick $errormsg ([:find $errormsg $frommsg -1] + [:len $frommsg]) [:find
$errormsg $viamsg -1]]
```

Mikrotik Scripting работа с Log

Работа с адресни листи

5. Блокиране чрез проверка в 3 адресни листи

```
:global blacklist "blacklist";

:global blacklist1 "errorlogin1";

:global blacklist2 "errorlogin2";
```

Mikrotik Scripting работа с Log

Работа с адресни листи

```
/ip firewall address-list
:if ([:len [find where list=$blacklist and address=$ipannoying]] = 0) do={
        :if (([:len [find where list=$blacklist2 and address=$ipannoying]] > 0) and ([:len [find
where list=$blacklist1 and address=$ipannoying]] > 0)) do={
                /ip firewall address-list add list=$blacklist address=$ipannoying
timeout=1d comment="$errormsg"
                }
        :if (([:len [find where list=$blacklist2 and address=$ipannoying]] = 0) and (/ip firewall
address-list [:len [find where list=$blacklist1 and address=$ipannoying]]) > 0) do={
                /ip firewall address-list add list=$blacklist2 address=$ipannoying
timeout=5m
                }
        :if ([:len [find where list=$blacklist1 and address=$ipannoying]] = 0) do={
                /ip firewall address-list add list=$blacklist1 address=$ipannoying
timeout=5m
                }
```

Откриване на IPSec error login

Дефиниране на грешните съобщения.
Определяне на IP адреса в стринг

05

Mikrotik Scripting работа с Log

Намиране на грешните съобщения

1.Дефиниране на грешните опити.

<192.168.0.21>: user steady authentication failed – грешна парола
<192.168.0.21>: user steady1 authentication failed – грешен потребител

192.168.0.21 parsing packet failed, possible cause: wrong password – грешен PSK или IKE2 вместо IKE1

phase1 negotiation failed due to time up 83.97.27.212[500]<=>192.168.0.21[500]
b9fa045d58fb47f9:814b7b92408980a8
– грешен PSK или IKE2 вместо IKE1

64.62.197.149 failed to get valid proposal.

Mikrotik Scripting работа с Log

Намиране на грешните съобщения и IP адреса

2.1. Определяне на IP адрес на досадника.

```
#IPSec "phase1 negotiation failed due to time up 83.97.27.212[500]<=>192.168.0.21[500]
b9fa045d58fb47f9:814b7b92408980a8 "

/log
:foreach erroripsec in=[find where message~"phase1 negotiation failed due to time up"] do={
   :local ipsecerrormsg [get $erroripsec message]
            #extract from => to the end
           :local ip1 [:pick $ipsecerrormsg [:find $ipsecerrormsg "=>"] [:len $ipsecerrormsg]]

            #Extract ftom beginning to [
           :local ipsecannoying [:pick $ip1 2 [:find $ip1 "["]]

           :put $ipsecannoying;
```

Mikrotik Scripting работа с Log

Намиране на грешните съобщения и IP адреса

2.2. Определяне на IP адрес на досадника.

```
#IPSec "<192.168.0.21>: user steady authentication failed"
# find ipsecannoying

/log
:foreach erroripsec in=[find where message~"authentication failed"] do={
    :local ipsecerrormsg [get $erroripsec message]
    :local ipsecannoying [:pick $ipsecerrormsg 1 [:find $ipsecerrormsg ">"]]
    :put $ipsecannoying;
```

Намиране на грешните съобщения и IP адреса

2.3. Определяне на IP адрес на досадника.

```
#IPSec "64.62.197.149 failed to get valid proposal. "
# find ipsecannoying
/log
:foreach erroripsec in=[find where message~"failed to get valid proposal"] do={
    :local ipsecerrormsg [get $erroripsec message]
    :local ipsecannoying [:pick $ipsecerrormsg 0 ([:find $ipsecerrormsg "failed"] -1)]
    :put $ipsecannoying;
```

Mikrotik Scripting работа с Log

Добавяне в адресна листа

3. Блокиране, чрез добавяне в адресна листа.

```
#Add ipsecannoying to blacklist

/ip firewall address-list
:if ([:len [find where list=$blacklist and address=$ipsecannoying]] = 0) do={
        /ip firewall address-list add list=$blacklist address=$ipsecannoying timeout=1d
        comment="$ipsecerrormsg"
        }
```

Скрипт за RoS v7

06

Scheduler.
Уведомяване на администратора.
Блокиране на IP адресите

Mikrotik Scripting работа с Log

Блокиране на IP адрес

1. **Блокиране на IP адресите в адресна листа blacklist**

Добавяне на скрипта в firewall RAW

```
/ip firewall raw
add action=drop chain=prerouting src-address-list=blacklist
```

Scheduler

2. Scheduler

Добавяне на скрипта в scheduler

/system scheduler add name=error-user-login on-event=error-user-login interval=1h

3. Динамична промяна на интервала в Scheduler

Алгоритъм на действие

- Прави се проверка на броя блокирани IP адреси в адресна листа **blacklist** с timeout по-малък от 23 часа.

- В зависимост от броя IP адреси се променя времевия интервал на стартиране на скрипта за проверка error-user-login
- Ако Log се запълва за по-малко от 30min интервала на стартиране става 1min

0-4бр. Interval=60min 5-20бр. Interval=30min >20бр. Interval=10min shortlog Interval=5min

Mikrotik Scripting работа с Log

Scheduler

3.1 Проверка на адресна листа blacklist за брой блокирани адреси

```
:global routerid [/system identity get name];
:global adminmail " admin@company.com ";
:local countip;
:set $countip 0;
:set $countip ([/ip firewall address-list print count where (list=blacklist and timeout<23h)])
```

3.2 Промяна на интервала на стартиране на скрипта

```
/system scheduler set name=error-user-login on-event=error-user-login interval=01:00:00
```

Mikrotik Scripting работа с Log

Scheduler

3.2 Промяна на интервала на стартиране на скрипта

```
:if ($countip<5) do={
/system scheduler set ([find where name=error-user-login]) interval=01:00:00
};

:if ($countip>=5 and $countip<=20 ) do={
/system scheduler set ([find where name=error-user-login]) interval=00:30:00
};

:if ($countip>21 ) do={
/system scheduler set ([find where name=error-user-login]) interval=00:10:00;
/tool e-mail send to=$adminmail subject="Error login attack detected body="$[/system clock
get date] Router $routerid more than 20 IP address has blacklisted"
};
```

Mikrotik Scripting работа с Log

Scheduler

3.2 Промяна на интервала на стартиране на скрипта 1минута при бързо запълващ се Log с 1000 реда и разлика между първо и последно съобщение по-малко от 30 минути.

```
:global shortlog 0;
:foreach i in=[/log find  time>([/system clock get time] - 30m) ] do={
:set shortlog ($shortlog + 1);
            };

:if ($ shortlog >998 ) do={
/system scheduler set ([find where name=error-user-login]) interval=00:05:00;
/tool e-mail send to=$adminmail subject="Log overflow" body="Router $routerid to much
router log events for short time";
};
```

Scheduler

3.3 Добавяне на динамичният скрипт в scheduler

```
/system scheduler add name=dynamic-scheduler-error-login on-event=dynamic-scheduler-error-login
interval=00:30:00
```

Notification

4. Изпращане на уведомление до администратора

-Конфигурирайте настройките на e-mail сървъра Tools -> Email за да получавате поща от рутера

##Send e-mail to admin that router blacklisted IP address

:global adminmail “admin@company.com";

/tool e-mail send to=$adminmail subject="Error login attack detected" body="$[/system clock get date] Router $routerid More than 20 IP address has blacklisted";

ВЪПРОСИ

Благодаря за вниманието!