

Автоматизация добавления новых хостов в МО (bash, nmap)

Типичная ситуация которая возникает при запуске в эксплуатацию NOC - добавление новых объектов МО в SA когда объектов в нём нет и автоматическое добавление замонтированного оборудования в процессе эксплуатации сети.

Я не умею программировать, поэтому задачу решал "в лоб" с использованием подручных инструментов:

1. nmap
2. bash
3. команды `./noc csv-import sa.managedobject`

у NOC есть возможность из консоли импорта специально сформированного csv файла с информацией о объектах МО. Основная цель скрипта - сформировать этот файл и передать его на импорт в систему.

Алгоритм действий такой:

1. считать из параметров скрипта сканируемый диапазон IP
2. передать их `nmap` и вывести результат сканирования в файл.
3. построчно прочитать данный файл и провести проверку через `rsqf`, есть ли такой IP в объектах МО
4. если объекта нет - вывести в текстовый файл специально сформированную строку
5. сформированный `.cvs` файл передать на импорт в NOC и отправить на почту для информирования

Обратите внимание на пути:

1. nok установлен в `/opt/noc`
2. `BASEDIR` -
3. `NMAPBIN` `nmap`

В качестве параметра скрипту передются ДВА диапазона для сканирования и параметр `scan`. При наличии параметра `scan` удаляются результаты предыдущей работы скрипта, если параметра нет - то скрипт работает с уже полученными данными. В директорию складывается архив хостов которые были добавлены.



запуск

```
$ mkdir data
```

```
$ ./cron.sh scan
```

```
.....
```

```
# ls -l
```

```
cron.sh
```

```
hostsscan.txt
```

```
networkscan.txt
```

```
out.hostsadd.txt
```

```
out.hostsbd.txt
```

```
out.hostsscan.txt
```

```
result.hostsadd.csv
```

После работы скрипта получают файлы:

- `hostsscan.txt` - файл с результатами сканирования сети *NMAP*
- `networkscan.txt` - список подсетей для сканирования в формате который понимаем `nmap`
- `out.hostsadd.txt` - файл со списком хостов которых нет в МО
- `out.hostsbd.txt` - файл со списком хостов которые ЕСТЬ в МО
- `out.hostsscan.txt` - файл с результатами сканирования сети *NMAP*

- result.hostsadd.csv - результат работы скрипта готовый для импорта через `./noc csv-import sa.managedobject`



```
#!/bin/bash

# set -e ?

# todo
# 1. сделать работу скрипта без сканирования сети. только генерацию по файлу от предыдущего скана. при этом не удалять файл скана
# 2. отправка результата по почте для оценки админом.
# 3. переделка на сканирование telnet\ssh а не пропинговкой.
# 4. добавление найденных устройств в бд.
# nmap -sP -iL networkscan.txt
export LANG="ru_RU.UTF-8"
export LOCALE="ru_RU"

BASEDIR=/opt/scripts/discoverynet

# проверяем или по телнету или по пингу.
# по пингу должно быть быстрее /16

NMAPBIN="/usr/bin/nmap -sP -n -iL $BASEDIR/networkscan.txt -oG $BASEDIR/out.hostsscan.txt"
# NMAPBIN="/usr/bin/nmap -sP -oG \"$BASEDIR/out.hostsscan.txt\""

echo $NMAPBIN

# заносим параметры по default для формирования csv файла
#name=address
is_managed="True"
administrative_domain="default"

segment="ALL"
activator="activatormain"
collector=""
profile_name="Generic.Host"
object_profile="default"
description=""
auth_profile=""
scheme="0"
address=""
port=""
user="admin"
password="admin"
super_password="admin"
remote_path=""
trap_source_ip=""
trap_community=""
snmp_ro="public"
snmp_rw="public"
vc_domain=""
vrf=""
termination_group=""
service_terminator=""
shape="Cisco/router"
config_filter_rule=""
config_diff_filter_rule=""
config_validation_rule=""
max_scripts="5"
tags="autoadd"

headcsv="name,is_managed,administrative_domain,segment,activator,collector,profile_name,object_profile,description,auth_profile,scheme,
address,port,user,password,super_password,remote_path,trap_source_ip,trap_community,snmp_ro,snmp_rw,vc_domain,vrf,termination_group,
service_terminator,shape,config_filter_rule,config_diff_filter_rule,config_validation_rule,max_scripts,tags"
```

```

# выполняем сканирование сети.
# в качестве параметра берём диапазон переданный из консоли.
if [ "$1" = "scan" ]
then
# очищаем вывод от предыдущего запуска
cd $BASEDIR && rm result* out*

# сканируем сеть
$NMAPBIN
fi

# читаем построчно получившийся файл и начинаем формировать файл для загрузки в бд.

while read -r line

do
profile_name="Generic.Host"
object_profile="default"
trap_source_ip=""
snmpcheckresult=""
name=$line
# echo $name
address='echo $line | grep Host | grep "Status: Up" | awk '{print $2}'"

# проверяем что вывод ненулевой и проверяем есть ли оно в бд
if [ -n "$address" ]
then
$BASEDIR/sql.sh $address &

fi
echo -e "\n\n"
done < $BASEDIR/out.hostsscan.txt

# проверяем есть ли новые хосты. если есть то отправляем почту и добавляем в бд
# склеиваем CVS из "шапки" и "тела"

sleep 60

if [ -a $BASEDIR/out.hostsadd.txt ]
then
echo $headcvsv > $BASEDIR/result.hostsadd.csv
cat out.hostsadd.txt >> $BASEDIR/result.hostsadd.csv

# удаляем из БД дубликаты
/opt/scripts/maintenance.fix/cron.sh

# добавление хостов.
cd /opt/noc && ./noc csv-import sa.managedobject -r skip -v 3 $BASEDIR/result.hostsadd.csv
RETVAL=$?

if [ $RETVAL -ne 0 ]
then
echo "error import"
/bin/mail -S sendcharsets=utf-8 -s "Ошибка импорта данных" -a $BASEDIR/result.hostsadd.csv root@example.com < $BASEDIR/result.
hostsadd.csv
fi

# отправка почты
/bin/mail -S sendcharsets=utf-8 -s "Найденный новые хосты СПД" -a $BASEDIR/result.hostsadd.csv root@example.com < $BASEDIR
/result.hostsadd.csv
fi

# переносим файл в архив.

mv $BASEDIR/result.hostsadd.csv $BASEDIR/data/ /bin/date +%Y\%m\%d'.csv

```



sql.sh

```
#!/bin/bash
```

```
export LANG="ru_RU.UTF-8"
```

```
export LOCALE="ru_RU"
```

```
BASEDIR=/opt/scripts/discoverynet
```

```
# заносим параметры по default для формирования csv файла
```

```
#name=address
```

```
is_managed="True"
```

```
administrative_domain="default"
```

```
activator="activatormain"
```

```
collector=""
```

```
profile_name="Generic.Host"
```

```
object_profile="default"
```

```
description=""
```

```
auth_profile=""
```

```
scheme="0"
```

```
address=""
```

```
port=""
```

```
user="admin"
```

```
password="admin"
```

```
super_password="admin"
```

```
remote_path=""
```

```
trap_source_ip=""
```

```
trap_community=""
```

```
snmp_ro="public"
```

```
snmp_rw="public"
```

```
vc_domain=""
```

```
vrf=""
```

```
termination_group=""
```

```
service_terminator=""
```

```
shape="Cisco/router"
```

```
config_filter_rule=""
```

```
config_diff_filter_rule=""
```

```
config_validation_rule=""
```

```
max_scripts="5"
```

```
tags="autoadd"
```

```
headcvs="name,is_managed,administrative_domain,segment,activator,collector,profile_name,object_profile,description,auth_profile,scheme,  
address,port,user,password,super_password,remote_path,trap_source_ip,trap_community,snmp_ro,snmp_rw,vc_domain,vrf,termination_group,  
service_terminator,shape,config_filter_rule,config_diff_filter_rule,config_validation_rule,max_scripts,tags"
```

```
address=$1
```

```
SQLQUERY="SELECT address FROM sa_managedobject where address = '$address' and name not like 'wiping-%' limit 1 ;"
```

```
SQLRESULT=`echo $SQLQUERY | psql -U noc --dbname noc -X -A -t -q --no-align`
```

```
# Проверяем БД доступна
```

```
RETVAL=$?
```

```
if [ $RETVAL -eq 1 ]
```

```
then
```

```
echo "Postgress DOWN"
```

```
exit
```

```
fi
```

```
if [ -n "$SQLRESULT" -a $RETVAL -eq 0 ]
```

```
then
```

```
# хост присутствует в БД и надо проверять для него SNMP для обновления данных
```

```
echo -e $SQLRESULT "есть в БД"
```

```
# выводим адресс в файл
```

```
echo -e $address >> $BASEDIR/out.hostsbd.txt
```

```
else
```

```
echo -e $SQLRESULT "нет в БД"
```

```
# по параметрам default заполняет строку нужными значениями
```

```
# выводим в файл out.hostsadd.txt так как данного хоста нету в БД
```

```
# ADDROW="$address,True,default,activatormain,,Huawei.VRP,huawei.ftb,с.Анрай_ул.Новобозарная_13_Ал.Гай ЦАТС.,0,$address,0,admin,admin,admin,,,$address,,,,,,,,,Cisco/router,,,,,5,"
```

```
# необходимо чтобы нормально работал пинг.
```

```
# $trap_source_ip = "$address"
```

```
ADDROW="$address,$is_managed,$administrative_domain,$segment,$activator,$collector,$profile_name,$object_profile,$description,$auth_profile,$scheme,$address,$port,$user,$password,$super_password,$remote_path,$address,$trap_community,$snmp_ro,$snmp_rw,$vc_domain,$vrf,$termination_group,$service_terminator,$shape,$config_filter_rule,$config_diff_filter_rule,$config_validation_rule,$max_scripts,$tags"
```

```
echo -e $ADDROW >> $BASEDIR/out.hostsadd.txt
```

```
fi
```

у меня скрипт запускается каждую ночь по расписанию в *cron*:

```
0 21 * * * /opt/scripts/discoverynet/cron.sh scan >/dev/null 2>&1
```

- [Autoadd new devices in microservices](#)
- [Мониторинг активаторов и дисковери](#)
- [Обновление полей name, snmp_ro, object_profiles в МО с использованием snmp \(bash, snmp \) \(добавлен код для микросервисов\)](#)
- [График задач дискавери](#)
- [Удаление зависших задач](#)