نصب nTop-3.4 بر روی لینوکس fedora core 13

برای نصب ntop باید دستور

```
./autogen
```

را در ترمینال وارد کرد.در صورت نصب نبودن libpcap با خطای زیر مواجه میشویم :

```
checking for pcap_lookupdev in -lpcap... no
        *** FATAL ERROR ***
 It looks that you don't have the libpcap distribution installed.
 Download, compile and, optionally, install it.
 When finished please re-run this program.
 You can download the latest source tarball at http://www.tcpdump.org/
configure: error:  The LBL Packet Capture Library, libpcap, was not found!
```

برای رفع این خطا باید libpcap را نصب نمود. برای نصب libpcap دستورات زیر را به ترتیب اجرا میکنیم :

```
./configure
make
make install
```

در بعضی از مواقع بعد از نصب libpcap دوباره خطای قبلی گزارش میشود که در این صورت باید tcpdump نیز نصب شود.

بعد از نصب libpcap اگر دوباره اقدام به نصب ntop بکنیم ، در صورت نصب نبودنrrdtool با خطای زیر مواجه میشویم :

```
configure: error: Unable to find RRD at /usr/local/rrdtool: please use --with-rrd-home=DIR
```

برای رفع این مشکل باید آدرس جایی را که rrdtool در آن نصب شده است را به عنوان پارامتر در هنگام نصب وارد کنیم. و در صورت عدم نصب باید آن را نصب کنیم. برای نصب rrdtool دستورات زیر را اجرا میکنیم :

```
./configure
make
make install
```

rrdtool به صورت پیشفرض در آدرس /opt/rrdtool-V که V نمایانگر نسخه نصب شده از rrdtool است. در هنگام نصب ntop باید به عنوان پارامتر ارسال شود.

Ntop برای اجرا شدن نیازمند GeoIp است. در صورت عدم نصب خطای زیر در هنگام نصب ntop پیش میآید.

```
checking for GeoIP_record_by_ipnum in -lGeoIP... no
Please install GeoIP (http://www.maxmind.com/)
```

این نسخه از ntop دارای پایگاه داده مورد نیاز برای geoip میباشد و باید api های مورد نیاز برای کار با آنها را نصب کنیم. این برنامه را میتوان از آدرس زیر دریافت کرد:

```
http://geolite.maxmind.com/download/geoip/api/c/
```

برای نصب این کتابخانه دستورات زیر را استفاده میکنیم:

```
./configure
make
make check
make install
```

بعد از نصب GeoIP میتوان اقدام به نصب ntop نمود. برای نصب دستورات زیر را اجرا میکنیم

```
./autogen –with-rrd-home=/opt/rrdtool-(version)
make
make install
```

در هنگام نصب ntop باید host ما متصل به اینترنت باشد تا بتواند کتابخانه ettercap را دریافت و نصب کند.

کار با ntop

ایجاد کاربر ntop

با دستور زیر میتوان کاربر جدیدی برای کار با ntop ایجاد کرد:

```
useradd -M -s /sbin/nologin -r ntop
```

با سویچ M– برای کاربر دایرکتوری home ساخته نمیشود

با سویچ s– محیط shell کاری لینوکس برای کاریر معرفی میشود.

با عبارت /sbin/nologin، کاربر ایجاد شده امکان دسترسی به shell را نخواهد داشت.

تغییر دسترسی های پوشه ها

برای کاربر ایجاد شده باید دسترسی به پوشه کاری مورد نیازش را بدهیم.

```
chown ntop:root /usr/local/var/ntop/
chown ntop:ntop /usr/local/share/ntop/
```

ایجاد کلمه رمز برای کاربر ntop

برای اینکه کاربر ntop قادر به کار باشد باید برای او کلمه رمز تعریف شود.
برای تعریف کلمه رمز از دستور زیر استفاده میشود:

```
Ntop -A
```

خروجی زیر برای دستور بالا نمایان میشود، که باید کلمه رمز را برای کاربر وارد کنیم:

```
Mon Jul 28 03:38:34 2008  NOTE: Interface merge enabled by default
Mon Jul 28 03:38:34 2008  Initializing gdbm databases

ntop startup - waiting for user response!

Please enter the password for the admin user:
Please enter the password again:
Mon Jul 28 03:38:42 2008  Admin user password has been set
```

آغاز به کار ntop

در این مرحله میتوان ntop را برای کار فعال کرد.

```
/usr/local/bin/ntop -d -L -u ntop -P /usr/local/var/ntop --skip-version-check --use-syslog=daemon
```

در صورت استفاده از چند کارت شبکه، دستور زیر وارد میشود:

```
/usr/local/bin/ntop -i "eth0,eth1" -d -L -u ntop -P /usr/local/var/ntop --skip-version-check --use-
syslog=daemon
```

خروجی شبیه مورد زیر در صورت اجرای درست نمایش داده خواهد شد:

```
Mon Jul 28 03:42:19 2008  NOTE: Interface merge enabled by default
Mon Jul 28 03:42:19 2008  Initializing gdbm databases
```

- **-i "eth0,eth1"** : Specifies the network interface or interfaces to be used by ntop for network monitoring. Here you are monitoring eth0 and eth1.
  - -i “eth0,eth1” :مشخص کردن کارت شبکه که ntop از آنها برای مونیتور کردن شبکه استفاده میکند
  - -d : اجرای ntop به صورت یک سرویس
  - -L :فرستادن همه log ها به system log(/var/log/messages) در عوض نمایش در صفحه نمایش
  - -u ntop : آغاز کردن ntop با کاربر ntop
  - -P /usr/local/var/ntop :مشخص کردن آدرسی که ntop دیتابیس خود را نگه میدارد.
  - --skip-version-check :غیر فعال کردن کنترل اینکه نسخه در حال اجرا آخرین نسخه است.
  - --use-syslog=deamon :فعال سازی استفاده از syslog deamon

مشاده وضعیت ترافیک

به صورت پیشفرض ntop در پورت شماره 3000 به حالت listen است، کا میتوان با یک مرورگر وضعبت آن را مشاهده کرد.

```
http://localhost:3000/
OR
http://server-ip:3000/
```

باز کردن پورت3000 در iptable

در بعضی از موارد پورت ۳۰۰۰ توسط firewall بسته میباشد که باید برای کار با ntop باز شود، برای این منظور باید در فایل های کانفیگ iptable تغییراتی دهیم. فایل کانفیگ iptable در آدرس

```
/etc/sysconfig/iptables
```

قرار دارد. برای باز کردن پورت ۳۰۰۰ ، خط زیر را به آن اضافه میکنیم:

```
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 3000 -j ACCEP
```

برای اعمال تغییرات باید فایروال را restart کنیم.

```
service iptables restart
```

توقف ntop

برای توقف کار ntop از دستور زیر استفاده میشود

```
Killall ntop
```

نوشته شده توسط: حامد شیخلو