iftopd软件

用户手册、FAQ及版本日志

目录

[1概述 2](#_Toc435110096)

[2安装使用环境 2](#_Toc435110097)

[3使用介绍和FAQ 2](#_Toc435110098)

[3.1软件的安装和卸载说明 2](#_Toc435110099)

[3.2 iftopd软件打开 3](#_Toc435110100)

[3.3 iftopd软件的重启 3](#_Toc435110101)

[3.4查看iftopd的状态 3](#_Toc435110102)

[3.5 iftopd软件的关闭 3](#_Toc435110103)

[3.6查看和设置系统负载阀值（方法二） 4](#_Toc435110104)

[3.7查看进程列表信息 4](#_Toc435110105)

[3.8iftopd软件关闭 4](#_Toc435110106)

[4版本记录（ CHANGELOG） 5](#_Toc435110107)

[4.1 V1.0 2015](#_Toc435110108)*[-](#_Toc435110108)*[09-23 5](#_Toc435110108)

[4.2 V1.1 5](#_Toc435110109)

# 1概述

改进iftop工具，使其能够在后台运行，监控每条网络连接的上下行平均速度，并将该信息，以日志保存，用于后续分析。

# 2安装使用环境

操作系统 ：CentOS 6.5 x86\_64

内核版本 ：Linux-3.12.6

定制ISO ：

CentOS-6.5-x86\_64-Custom-v1.3.iso

系统版本号：CentOS release 6.5 (Custom v1.3)

注：安装是需要确保系统中已经安装了libpcap和libcurses等，运行是需要连接的库，否则，不能正常运行。若iftop可以运行，则本软件(iftopd),完全可以正常运行。

# 3使用介绍和FAQ

## 3.1软件的安装和卸载说明

* 安装：rpm -ivh iftopd-1.1-1.el6\_3.12.6\_iso\_v1.0.x86\_64.rpm
* 卸载：rpm -e iftopd
* 参数说明

**\*start** : service iftopd start 启动iftopd 。

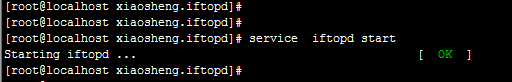
**\*restrt** : service iftopd restart 重启iftopd 。

**\*stop** : service iftopd stop关闭iftopd（卸载前务必先关闭iftopd）。

**\*status**: service iftopd status 查看iftopd当前的运行状态 。

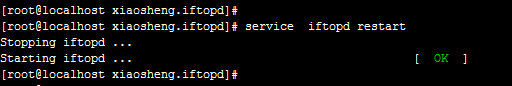
## 3.2 iftopd软件打开

* service iftopd start



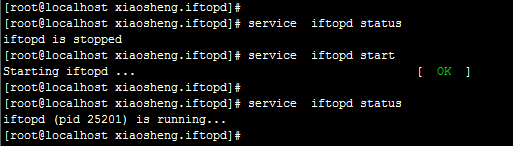
## 3.3 iftopd软件的重启

* service iftopd restart



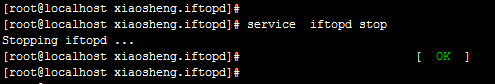
## 3.4查看iftopd的状态

* service iftopd status



## 3.5 iftopd软件的关闭

* service iftopd stop



## 3.6 配置文件的说明和使用（.iftopdc）

iftopd 配置文件名： .iftopdc，是一个放在根目录下的隐藏文件，故 配置文件必须放在 /root 目录先下。配置由用户自己来添加，若没有配置文件，iftopd按照默认参数启动。

在配置文件中，每行一个配置指令，配置指令是名称和数值对，例如，下面的指令用来设置网卡：interface: eth0。

配置文件中配置说明：

* interface: eth0

指定网卡

* promiscuous: (yes|no)

把网卡设置为“混杂模式”，默认是no。

* num-lines:500

输出前500条连接上下行速度输出前500条连接上下行速度，默认就是前500条。

* interval-seconds-time:1

采集数据信息的时间间隔，单位是秒，默认是1秒。

* speed-second-time:1

显示平均下载速度的单位选择，1--代表按每秒（/s） 来显示速度，2--代表按每分钟（/min）来显示速度，默认。在将该值设置为按每分钟来显示时，最好设置时间间隔值大于30秒。

* filter-code:bpf

用来选择要记录的数据包。因为只记录IP包，所以默认的规则就是：（bfp) and ip ，其中bfp是bfp格式的过滤代码。例子1：filter-code:ip host 149.20.4.69 只处理来自149.20.4.69 数据， 例子2：如果bpf为：icmp，则相当于 icmp and ip ，则就只抓取icmp的数据连接。

## 3.7 关于记录文件的说明（iftopd.log）

数据存储在记录文件iftopd.log文件里，该文件存储于/var/log/ 目录下，有iftopd启动后自动创建。

记录的内容如下图：

date : 记录的日期

time: 记录 的时间

num ：记录编号， 按照total 的大小排序

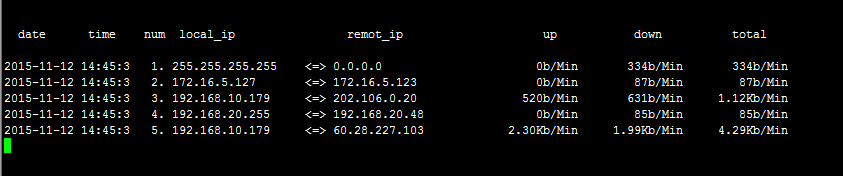
local\_ip ： 源ip

remot\_ip ：目的ip

up ： 上行速度

down ： 下行速度

total：上下行速度之和



## 3.8注意事项

* 在iftopd的配置文件中，其它未定义配置说明，禁止根据iftop的规则来使用。

# 4版本记录（ CHANGELOG）

* **4.2 V1.1 2015-11-18**

iftopd-1.1 ，对外测试发布的第一版本。

* **4.1 V1.0 2015-10-30**

iftopd-1.0，没有对外发布。