11 Monitorando hosts e redes com netstat

O netstat (Network statistic) é uma aplicação comum a todos os sisteamas operacionais, utilizada para monitorar a rede e as interfaces de comunicação para obter principalmente informações sobre as conexões, tabelas de roteamento, estatísticas de interface e conexões mascaradas.

É muito útil para análise de rede para descobrir conexões tanto da rede, dos seus usários quanto de tentativas de intrusão. O netstat é uma ferramenta que faz parte de praticamente todas as distribuições Linux.

O uso básico do comando é simples e apresenta as conexões existentes no host. Quando omitido o endereço do host, subebtende-se que é o hosto local. As diretrizes são:

netstat : executa o utilitário de rede netstat;

-n : indica ao netstat para não resolver nomes;

-a : exibe todas as conexões existentes no computador.

$ netstat -n

```
(base) hk@hk:~$ netstat -n
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.1.103:60420     172.217.162.197:443     ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    34384    /run/user/1000/systemd/notify
unix  2      [ ]         DGRAM                    91496    /run/wpa_supplicant/wlo1
```

$ netstat -a -n

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:9050          0.0.0.0:*               LISTEN
tcp        0      0 192.168.1.103:60420     172.217.162.197:443     ESTABLISHED
tcp        0      0 192.168.1.103:59304     64.233.186.188:443      ESTABLISHED
tcp        0      0 192.168.1.103:53026     185.184.10.30:443       ESTABLISHED
tcp        0      0 192.168.1.103:43798     198.252.206.25:443      ESTABLISHED
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
```

11.1 Opções do netstat

A seguir algumas opções do netstat:

netstat -o : mostra há quanto tempo a conexão está estabelecida. Podeser combinado com “netstat -autno” e “netstat -axuo”;

netstat -i : mostra as informações de todas as interfaces que estão ativas e estatísticas de erros de entrada/saída, assim como estatística de tráfego;

netstat -c : mostra o momento exato que uma conexão é estabelecida ou o aumento de tráfego nas interfaces com as opções “netstat -ic” e ‘netstat -atnc”;

netstat -e : mostra um lista mais completa quando combinado com as outras opções como o “netstat -atne”, exibe as colunas: USER e INODE, que são o usuário que iniciou o processo que originou a abertura da porta e o INODE, que retrata a informação do nó da rede;

netstat -p : mostra o daemon (serviço) e o PID (identificador do processo) que estão ligados a cada porta;

netstat -s : mostra todas as estatísticas dos protocolos, quanto foi trafegado em cada protocolo. Pode ser combinado para exibir a estatística de um determinado protocolo: “netstat -st” e “netstat -su”.

11.2 Filtrando saídas com o netstat

O netstat permite que sejam usadas opções na filtragem da saída do comando.

Um exemplo seria a filtragem em busca de pacotes TCP usando a opção “-t”:

$ netstat -ant

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	127.0.0.1:3306	0.0.0.0:*	LISTEN
tcp6	0	0	:::80	:::*	LISTEN
tcp6	0	0	::1:631	:::*	LISTEN

Outro exemplo é buscar conexões realizadas no host permitindo saber quem, quando, onde e com fez uma conexão:

$ netstat -at

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	localhost:mysql	0.0.0.0:*	LISTEN
tcp	0	0	localhost:domain	0.0.0.0:*	LISTEN
tcp	0	0	localhost:ipp	0.0.0.0:*	LISTEN
tcp	1	0	hk:37954	banjo.canonical.co:http	CLOSE_WAIT
tcp6	0	0	ip6-localhost:ipp	[::]:*	LISTEN

Assim como filtrar pela busca de todas as conexões UDP e TCP:

$ netstat -tupan

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	127.0.0.1:3306	0.0.0.0:*	LISTEN	-
tcp	0	0	127.0.0.53:53	0.0.0.0:*	LISTEN	-
tcp	0	0	127.0.0.1:631	0.0.0.0:*	LISTEN	-
tcp	0	0	127.0.0.1:9050	0.0.0.0:*	LISTEN	-
tcp6	0	0	:::80	:::*	LISTEN	-
tcp6	0	0	::1:631	:::*	LISTEN	-

Todos os comandos do Linux para terem suas saídas filtradas pode utilizar o comando grep concatenado, por exemplo, para, no comando acima, filtrar as saídas para verificar se o MySQL está sendo executado ou não seria:

$ netstat -tupan | grep 3306

(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)

tcp 0 0 127.0.0.1:3306 0.0.0.0:* LISTEN -

Ou verificar se um sevidor web está sendo executado em um host-alvo:

$ netstat -tupan | grep 80

(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)

tcp 0 0 192.168.1.103:38080 172.217.173.97:443 ESTABLISHED 2544/chrome --type=

tcp 0 0 192.168.1.103:32980 68.67.160.132:443 ESTABLISHED 2544/chrome --type=

tcp6 0 0 :::80 :::* LISTEN -

udp 0 0 0.0.0.0:48072 0.0.0.0:* -