NAME

ss - another utility to investigate sockets

SYNOPSIS

ss [*options*] *[FILTER]*

DESCRIPTION

ss is used to dump socket statistics. It allows showing information similar to *netstat*. It can display more TCP and state informations than other tools.

OPTIONS

When no option is used ss displays a list of open non-listening sockets (e.g. TCP/UNIX/UDP) that have established connection.

-h, --help
Show summary of options.

-V, --version
Output version information.

-H, --no-header
Suppress header line.

-n, --numeric
Do not try to resolve service names.

-r, --resolve
Try to resolve numeric address/ports.

-a, --all Display both listening and non-listening (for TCP this means established connections) sockets.

-l, --listening
Display only listening sockets (these are omitted by default).

-o, --options
Show timer information.

-e, --extended
Show detailed socket information

-m, --memory
Show socket memory usage.

-p, --processes
Show process using socket.

-i, --info
Show internal TCP information.

-K, --kill
Attempts to forcibly close sockets. This option displays sockets that are successfully closed and silently skips sockets that the kernel does not support closing. It supports IPv4 and IPv6 sockets only.

-s, --summary
Print summary statistics. This option does not parse socket lists obtaining summary from various sources. It is useful when amount of sockets is so huge that parsing /proc/net/tcp is painful.

-Z, --context
As the **-p** option but also shows process security context.

For netlink(7) sockets the initiating process context is displayed as follows:

1. If valid pid show the process context.

2. If destination is kernel (pid = 0) show kernel initial context.
3. If a unique identifier has been allocated by the kernel or netlink user, show context as "unavailable". This will generally indicate that a process has more than one netlink socket active.

-z, --contexts
As the **-Z** option but also shows the socket context. The socket context is taken from the associated inode and is not the actual socket context held by the kernel. Sockets are typically labeled with the context of the creating process, however the context shown will reflect any policy role, type and/or range transition rules applied, and is therefore a useful reference.

-N NSNAME, --net=NSNAME
Switch to the specified network namespace name.

-b, --bpf
Show socket BPF filters (only administrators are allowed to get these information).

-4, --ipv4
Display only IP version 4 sockets (alias for -f inet).

-6, --ipv6
Display only IP version 6 sockets (alias for -f inet6).

-0, --packet
Display PACKET sockets (alias for -f link).

-t, --tcp
Display TCP sockets.

-u, --udp
Display UDP sockets.

-d, --dccp
Display DCCP sockets.

-w, --raw
Display RAW sockets.

-x, --unix
Display Unix domain sockets (alias for -f unix).

-S, --sctp
Display SCTP sockets.

-f FAMILY, --family=FAMILY
Display sockets of type FAMILY. Currently the following families are supported: unix, inet, inet6, link, netlink.

-A QUERY, --query=QUERY, --socket=QUERY
List of socket tables to dump, separated by commas. The following identifiers are understood: all, inet, tcp, udp, raw, unix, packet, netlink, unix_dgram, unix_stream, unix_seqpacket, packet_raw, packet_dgram.

-D FILE, --diag=FILE
Do not display anything, just dump raw information about TCP sockets to FILE after applying filters. If FILE is - stdout is used.

-F FILE, --filter=FILE
Read filter information from FILE. Each line of FILE is interpreted like single command line option. If FILE is - stdin is used.

FILTER := [state STATE-FILTER] [EXPRESSION]
Please take a look at the official documentation (Debian package iproute-doc) for details regarding filters.

STATE-FILTER

STATE-FILTER allows to construct arbitrary set of states to match. Its syntax is sequence of keywords state and exclude followed by identifier of state.

Available identifiers are:

All standard TCP states: **established**, **syn-sent**, **syn-recv**, **fin-wait-1**, **fin-wait-2**, **time-wait**, **closed**, **close-wait**, **last-ack**, **listen** and **closing.**

all - for all the states

connected - all the states except for **listen** and **closed**

synchronized - all the **connected** states except for **syn-sent**

bucket - states, which are maintained as minisockets, i.e. **time-wait** and **syn-recv**

big - opposite to **bucket**

USAGE EXAMPLES

ss -t -a Display all TCP sockets.

ss -t -a -Z
Display all TCP sockets with process SELinux security contexts.

ss -u -a Display all UDP sockets.

ss -o state established '(dport = :ssh or sport = :ssh)'
Display all established ssh connections.

ss -x src /tmp/.X11-unix/*
Find all local processes connected to X server.

ss -o state fin-wait-1 '(sport = :http or sport = :https)' dst 193.233.7/24
List all the tcp sockets in state FIN-WAIT-1 for our apache to network 193.233.7/24 and look at their timers.

SEE ALSO

ip(8), **/usr/share/doc/iproute-doc/ss.html** (package iproutedoc)**,**
RFC 793 - https://tools.ietf.org/rfc/rfc793.txt (TCP states)

AUTHOR

ss was written by Alexey Kuznetsov, <kuznet@ms2.inr.ac.ru>.

This manual page was written by Michael Prokop <mika@grml.org> for the Debian project (but may be used by others).