

NAME

raevent – read **argus(8)** event data.

COPYRIGHT

Copyright (c) 2000-2012 QoSient. All rights reserved.

SYNOPSIS

raevent [**raoptions**] [- **filter-expression**]

DESCRIPTION

Raevent reads **argus(8)** data from either *stdin*, an *argus-file*, or from a remote argus data source, filters the records it encounters based on an optional *filter-expression* and either prints the contents of the **argus(5)** records that it encounters to **stdout** or appends them into an **argus(5)** datafile.

OPTIONS

Raevent, like all ra based clients, supports a number of **ra options** including filtering of input argus records through a terminating filter expression. See **ra(1)** for a complete description of **ra options**.

EXAMPLE INVOCATION

```
% raevent -S localhost
```

```
event[874]=
2010/02/09.09:21:19.971182:srcid=192.168.0.68:prog:/usr/local/bin/ralsof
<ArgusEvent>
  <ArgusEventData>
    COMMAND  PID  USER  FD  TYPE  DEVICE  SIZE/OFF  NODE NAME
    SystemUIS 787 carter 11u IPv4 0x17ec2054 0t0 UDP *: *
    SystemUIS 787 carter 13u IPv4 0x185a28ec 0t0 UDP *: *
    AppleVNCs 798 carter 9u IPv6 0x172905c0 0t0 TCP *:5900 (LISTEN)
    Mail 817 carter 13u IPv4 0x18f73b1c 0t0 TCP 192.168.0.68:64540->17.148.16.45:993 (ESTABLISHED)
    Mail 817 carter 18u IPv4 0x20a15274 0t0 TCP 192.168.0.68:64542->17.148.16.45:993 (ESTABLISHED)
    Mail 817 carter 20u IPv4 0x172942d4 0t0 TCP 192.168.0.68:64541->17.148.16.45:993 (CLOSED)
    Mail 817 carter 21u IPv4 0x207f1a8c 0t0 TCP 192.168.0.68:64554->17.148.16.45:993 (ESTABLISHED)
    Mail 817 carter 26u IPv4 0x207fbb4c 0t0 TCP 192.168.0.68:64546->216.92.197.167:993 (ESTABLISHED)
    Mail 817 carter 29u IPv4 0x19e8d6b0 0t0 TCP 192.168.0.68:64547->216.92.197.167:993 (ESTABLISHED)
    Mail 817 carter 31u IPv4 0x207fb740 0t0 TCP 192.168.0.68:64548->216.92.197.167:993 (ESTABLISHED)
    Mail 817 carter 32u IPv4 0x20801abc 0t0 TCP 192.168.0.68:53902->216.92.197.167:993 (ESTABLISHED)
    Mail 817 carter 35u IPv4 0x19e8fbbc 0t0 TCP 192.168.0.68:50245->17.250.248.77:80 (CLOSED)
    Mail 817 carter 37u IPv4 0x207f5b4c 0t0 TCP 192.168.0.68:59403->216.75.197.71:80 (CLOSE_WAIT)
    Mail 817 carter 40u IPv4 0x19e8eef8 0t0 TCP 192.168.0.68:53903->216.75.197.71:80 (CLOSE_WAIT)
    Mail 817 carter 43u IPv4 0x20alc2d4 0t0 TCP 192.168.0.68:53913->208.59.201.100:80 (ESTABLISHED)
    Mail 817 carter 46u IPv4 0x20802aec 0t0 TCP 192.168.0.68:59408->208.59.201.100:80 (ESTABLISHED)
    Mail 817 carter 50u IPv4 0x207f92d4 0t0 TCP 192.168.0.68:53916->208.59.201.100:80 (ESTABLISHED)
    Microsoft 822 carter 5u IPv4 0x20a23740 0t0 TCP 192.168.0.68:53597->207.46.170.10:80 (CLOSED)
    iChatAgen 830 carter 6u IPv4 0x185a2734 0t0 UDP 127.0.0.1:52122->127.0.0.1:52122
    iChatAgen 830 carter 11u IPv4 0x20803f28 0t0 TCP 192.168.0.68:65360->205.188.3.5:5190 (ESTABLISHED)
    FileSyncA 838 carter 15u IPv4 0x20alcaec 0t0 TCP 192.168.0.68:57148->17.250.248.123:80 (CLOSED)
    aosnotify 843 carter 5u IPv4 0x20ald710 0t0 TCP 192.168.0.68:56355->17.250.248.83:5223 (ESTABLISHED)
    rasqline 27492 carter 5u IPv4 0x20a16abc 0t0 TCP 192.168.0.68:57166->192.168.0.82:561 (ESTABLISHED)
    Safari 37870 carter 18u IPv4 0x20a1e740 0t0 TCP 192.168.0.68:56792->198.145.117.112:80 (CLOSE_WAIT)
    Safari 37870 carter 33u IPv4 0x20800a8c 0t0 TCP 192.168.0.68:54690->69.192.29.115:443 (CLOSE_WAIT)
    iTunes 91271 carter 22u IPv4 0x2080b710 0t0 TCP *:3689 (LISTEN)
    iTunes 91271 carter 23u IPv6 0x172916d0 0t0 TCP *:3689 (LISTEN)
  </ArgusEventData>
</ArgusEvent>
```

Consider **raevent** as a proof of concept program for demonstrating the ArgusEvent system.

AUTHORS

Carter Bullard (carter@qosient.com).

SEE ALSO

ra(1), **rarc(5)**, **argus(8)**