NAME

radium − argus record multiplexor

SYNOPSIS

radium [**options**] [**raoptions**]

COPYRIGHT

DESCRIPTION

Radium is a real-time Argus Record multiplexor that processes Argus records and Netflow records and outputs them to any number of client programs and files. **Radium** is a combination of the features of ra.1 and argus.8, supporting access for upto 128 client programs to argus records originating from remote data sources and/or local managed argus data files. Using **radium** you can construct complex distribution networks for collecting and processing argus data, and providing a single point of access to archived argus data.

Designed to run as a daemon, **radium** generally reads argus records directly from a remote argus, and writes the transaction status information to a log file or open socket connected to an **argus** client (such as **ra(1)**). **Radium** provides the same data access controls as argus.8, including remote filtering, source address based access control, indivual oriented strong authentication and confidentiality protection for the distributed data, using **SASL** and **tcp_wrapper** technology. Please refer to the INSTALL and README files for each distribution for a complete description.

Radium is normally configured from a system **/etc/radium.conf** configuration file, or from a configuration file either in the **$RADIUMHOME** directory, or specified on the command line.

RADIUM SPECIFIC OPTIONS

Radium, like all ra based clients, supports a number of **ra options** including remote data access, reading from multiple files and filtering of input argus records through a terminating filter expression. **radium(8)** specific options are:

OPTIONS

−B <addr>
Specify the bind interface address for remote access. Acceptable values are IP version 4 addresses. The default is to bind to INADDR_ANY address.

−d Run radium as a daemon. This will cause radium to do the things that Unix daemons do and return, if there were no errors, with radium running as a detached process.

−e <value>
Specify the source identifier for this **radium**. Acceptable values are numbers, hostnames or ip address.

−f <radium.conf>
Use *radium.conf* as a source of configuration information. Options set in this file override any other specification, and so this is the last word on option values. This file is read after the system /etc/radium.conf file is processed. See *radium.conf.5* for the configuration file format.

−O Turn off Berkeley Packet Filter optimizer. No reason to do this unless you think the optimizer generates bad code.

−p Override the persistent connection facility. **Radium** provides a fault tolerant feature for its remote argus data access facility. If the remote argus data source closes, **radium** will maintain its client connections, and attempt to reestablish its connection with remote source. This option overrides this behavior, causing **radium** to terminate if any of its remote sources closes.

−P <portnum>
Specifies the **<portnum>** for remote client connection. The default is to not support remote access. Setting the value to zero (0) will forceably turn off the facility.

−S <host[:port][//full/path/to/argus.data.file]> Attach to a specific remote *host* to receive argus records. Append an optional port specifier to attach to a port value other than the default 561. Without the

optional full pathname, **radium** will continuously transmit a stream of real-time flow records as they are received. With the optional filename, **radium** will open the argus datafile specified, and stream the contents, closing the connection with the file EOF.

−T threshold[smh] (secs)
Indicate that *radium* should correct the timestamps of received *argus* records, if they are out of sync by threshold secconds. Threshold can be specified with the extensions s, m, or h for seconds, minutes or hours. **−X** Clear existing radium configuration. This removes any initialization done prior to encountering this flag. Allows you to eliminate the effects of the */etc/radium.conf* file, or any radium.conf files that may have been loaded.

SIGNALS

Radium catches a number of **signal(3)** events. The three signals **SIGHUP**, **SIGINT**, and **SIGTERM** cause **radium** to exit, writing TIMEDOUT status records for all currently active transactions. The signal **SIGUSR1** will turn on **debug** reporting, and subsequent **SIGUSR1** signals, will increment the **debug-level**. The signal **SIGUSR2** will cause **radium** to turn off all **debug** reporting.

ENVIRONMENT

$RADIUMHOME - Radium Root directory
$RADIUMPATH - Radium.conf search path (/etc:$RADIUMHOME:$HOME)

FILES

/etc/radium.conf - radium daemon configuration file
/var/run/radium.#.#.pid - PID file

EXAMPLES

Run **radium** as a daemon, reading records from a remote host, using port 561, and writing all its transaction status reports to *output-file*. This is a typical mode.

radium -S remotehost:561 -d -e ‘hostname‘ -w *output-file*

Collect records from multiple argi, using port 561 on one and port 430 on the other, and make all of these records available to other programs on port 562.

radium -S host1:561 -S host2:430 -de ‘hostname‘ -P 562

Collect records from multiple Cisco Netflow sources, using the default port, and make the resulting argus records available on port 562.

radium -C -S host1 -S host2 -de ‘hostname‘ -P 562

Radium supports both input filtering and output filtering, and radium supports multiple output streams, each with their own independant filters.

If you are interested in distributing IP traffic only (input filter) and want to separate traffic into differing files based on traffic type, this simple example separates ICMP traffic from other traffic.

radium -w *file1* **"icmp" -w** *file2* **"not icmp" - ip**

Audit the network activity that is flowing between the two gateway routers, whose ethernet addresses are 00:08:03:2D:42:01 and 00:00:0C:18:29:F1. Make records available to other programs through port 430/tcp.

radium -S source -P 430 - ether host (0:8:3:2d:42:1 and 0:0:c:18:29:f1) &

Process argus records from a remote source only between 9am and 5pm every day and provide access to this stream on port 562.

radium -S remotehost -t 9-17 -P 562

AUTHORS

Carter Bullard (carter@qosient.com)

SEE ALSO

radium.conf(5), **argus**(8), **hosts_access**(5), **hosts_options**(5), **tcpd**(8), **tcpdump**(1)