

NAME

audisp-remote – plugin for remote logging

SYNOPSIS

audisp-remote

DESCRIPTION

audisp-remote is a plugin for the audit event dispatcher that performs remote logging to an aggregate logging server. When the plugin is sent **SIGUSR1**, it writes a state report to **remote.state**.

TIPS

If you are aggregating multiple machines, you should edit `auditd.conf` to set the `name_format` to something meaningful and the `log_format` to enriched. This way you can tell where the event came from and have the user name and groups resolved locally before it is sent off of the machine.

SIGNALS**SIGUSR1**

Causes the audisp-remote program to write a state report to **remote.state** in **/run/audit**. The *suspend* flag tells whether or not logging has been suspended. The *remote_ended* flag tells if the connection was broken by the server saying it can't log events. The *transport_ok* flag tells whether or not the connection to the remote server is healthy. The *queue_length* tells how many records are enqueued to be sent to the remote server. The *max_queued_length* shows the peak queue length since startup. The report also records glibc memory consumption when available.

SIGUSR2

Causes the audisp-remote program to resume logging if it were suspended due to an error.

FILES

`/etc/audit/audisp-remote.conf` `/etc/audit/plugins.d/au-remote.conf` `/etc/audit/auditd.conf` `/run/audit/remote.state`

SEE ALSO

auditd.conf(8), **auditd-plugins(5)**, **audisp-remote.conf(5)**.

AUTHOR

Steve Grubb